

Integrated Dell Remote Access Controller 8 (iDRAC8)

Guía del usuario versión 2.05.05.05



Notas, precauciones y avisos

-  **NOTA:** Una NOTA proporciona información importante que le ayuda a utilizar mejor su equipo.
-  **PRECAUCIÓN:** Una PRECAUCIÓN indica la posibilidad de daños en el hardware o la pérdida de datos, y le explica cómo evitar el problema.
-  **AVISO:** Un mensaje de AVISO indica el riesgo de daños materiales, lesiones corporales o incluso la muerte.

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

2014 - 12

Rev. A00

Tabla de contenido

1 Descripción general.....	17
Ventajas al utilizar iDRAC con Lifecycle Controller.....	17
Funciones clave	18
Novedades de esta versión.....	21
Cómo usar esta guía del usuario.....	21
Exploradores web compatibles.....	22
Administración de licencias	22
Tipos de licencias.....	22
Adquisición de licencias.....	22
Operaciones de licencia.....	22
Funciones con licencia en iDRAC8	24
Interfaces y protocolos para acceder a iDRAC.....	30
Información sobre puertos iDRAC.....	33
Otros documentos que podrían ser de utilidad.....	34
Referencia de medios sociales.....	35
Cómo ponerse en contacto con Dell.....	36
Acceso a documentos desde el sitio de asistencia de Dell.....	36
2 Inicio de sesión en iDRAC.....	38
Inicio de sesión en iDRAC como usuario local de Active Directory o usuario LDAP.....	38
Inicio de sesión en iDRAC mediante una tarjeta inteligente.....	39
Inicio de sesión en iDRAC como usuario local mediante una tarjeta inteligente.....	39
Inicio de sesión en iDRAC como usuario de Active Directory mediante una tarjeta inteligente.....	40
Inicio de sesión en iDRAC mediante inicio de sesión único	41
Inicio de sesión SSO de iDRAC mediante la interfaz web de iDRAC.....	41
Inicio de sesión SSO de iDRAC mediante la interfaz web de CMC.....	41
Acceso a iDRAC mediante RACADM remoto.....	41
Validación del certificado de CA para usar RACADM remoto en Linux.....	42
Acceso a iDRAC mediante RACADM local.....	42
Acceso a iDRAC mediante RACADM de firmware.....	42
Acceso a iDRAC mediante SMCLP.....	42
Inicio de sesión en iDRAC mediante la autenticación de clave pública.....	42
Varias sesiones iDRAC.....	43
Cambio de la contraseña de inicio de sesión predeterminada.....	43
Cambio de la contraseña de inicio de sesión predeterminada mediante la interfaz web.....	44
Cambio de la contraseña de inicio de sesión predeterminada mediante RACADM.....	44

Cambio de la contraseña de inicio de sesión predeterminada mediante la utilidad de configuración de iDRAC.....	44
Activación o desactivación del mensaje de advertencia de contraseña predeterminada	45
Activación o desactivación del mensaje de advertencia de contraseña predeterminada mediante la interfaz web.....	45
Activación o desactivación del mensaje de advertencia para cambiar la contraseña de inicio de sesión predeterminada mediante RACADM.....	45

3 Configuración de Managed System y Management Station..... 46

Configuración de la dirección IP de iDRAC.....	46
Configuración de la IP de iDRAC mediante la utilidad de configuración de iDRAC.....	47
Configuración de la IP de iDRAC mediante la interfaz web de CMC.....	50
Activación del descubrimiento automático.....	51
Configuración de servidores y componentes del servidor mediante la configuración automática.....	52
Cómo usar contraseñas de algoritmos hash para obtener una mayor seguridad.....	56
Configuración de Management Station.....	57
Acceso a iDRAC de manera remota.....	58
Configuración de Managed System.....	58
Modificación de la configuración de la cuenta de administrador local.....	58
Configuración de la ubicación de Managed System.....	59
Optimización del rendimiento y el consumo de alimentación del sistema.....	59
Configuración de exploradores web compatibles.....	66
Cómo agregar iDRAC a la lista de dominios de confianza.....	68
Desactivación de la función de lista blanca en Firefox.....	68
Visualización de las versiones traducidas de la interfaz web.....	69
Actualización del firmware de dispositivos.....	69
Descarga del firmware de dispositivos.....	71
Actualización del firmware mediante la interfaz web de iDRAC.....	72
Actualización del firmware de dispositivos mediante RACADM.....	76
Programación de actualizaciones automáticas del firmware	77
Actualización del firmware mediante la interfaz web de CMC.....	78
Actualización del firmware mediante DUP.....	79
Actualización del firmware mediante RACADM remoto.....	79
Actualización del firmware mediante Lifecycle Controller Remote Services.....	79
Actualización del firmware del CMC desde el iDRAC.....	80
Visualización y administración de actualizaciones preconfiguradas.....	80
Visualización y administración de actualizaciones preconfiguradas mediante la interfaz web de iDRAC.....	81
Visualización y administración de actualizaciones preconfiguradas mediante RACADM.....	81
Reversión del firmware del dispositivo.....	81
Reversión del firmware mediante la interfaz web de iDRAC.....	82

Reversión del firmware mediante la interfaz web de CMC.....	83
Reversión del firmware mediante RACADM.....	83
Reversión del firmware mediante Lifecycle Controller.....	83
Reversión del firmware mediante Lifecycle Controller Remote Services.....	83
Recuperación de iDRAC.....	83
Uso del servidor TFTP.....	84
Copia de seguridad del perfil del servidor.....	84
Cómo hacer una copia de seguridad del perfil del servidor mediante la interfaz web de iDRAC.....	85
Copia de seguridad del perfil del servidor mediante RACADM.....	85
Programación de la copia de seguridad automática del perfil del servidor.....	85
Importación del perfil del servidor.....	87
Importación del perfil del servidor mediante la interfaz web de iDRAC.....	87
Importación del perfil del servidor mediante RACADM.....	88
Secuencia de operaciones de restauración.....	88
Supervisión de iDRAC mediante otras herramientas de administración del sistema.....	88

4 Configuración de iDRAC..... 89

Visualización de la información de iDRAC.....	90
Visualización de la información de iDRAC mediante la interfaz web.....	90
Visualización de la información de iDRAC mediante RACADM.....	90
Modificación de la configuración de red.....	90
Modificación de la configuración de red mediante la interfaz web.....	91
Modificación de la configuración de red mediante RACADM local.....	91
Configuración del filtrado de IP.....	92
Configuración de servicios.....	94
Configuración de servicios mediante la interfaz web.....	94
Configuración de servicios mediante RACADM.....	94
Activación o desactivación de la redirección de HTTPs.....	95
Uso del cliente de VNC Client para administrar el servidor remoto.....	95
Configuración del servidor VNC mediante la interfaz web del iDRAC.....	96
Configuración del servidor VNC mediante RACADM.....	96
Configuración del visor VNC sin Cifrado SSL.....	97
Configuración del visor VNC sin Cifrado SSL.....	97
Configuración del panel frontal.....	97
Configuración de los valores de LCD.....	98
Configuración del valor LED del Id. del sistema.....	99
Configuración de zona horaria y NTP.....	99
Configuración de zona horaria y NTP mediante la interfaz web de iDRAC.....	99
Configuración de zona horaria y NTP mediante RACADM.....	100
Configuración del primer dispositivo de inicio.....	100
Configuración del primer dispositivo de inicio mediante la interfaz web.....	100

Configuración del primer dispositivo de inicio mediante RACADM.....	101
Configuración del primer dispositivo de inicio mediante la consola virtual.....	101
Activación de la pantalla de último bloqueo.....	101
Activación o desactivación del paso del sistema operativo a iDRAC.....	102
Tarjetas admitidas para el paso del sistema operativo al iDRAC	103
Sistemas operativos admitidos para la NIC de USB.....	103
Activación o desactivación del paso del sistema operativo a iDRAC mediante la interfaz web.....	105
Activación o desactivación del paso del sistema operativo a iDRAC mediante RACADM.....	106
Activación o desactivación del paso del sistema operativo a iDRAC mediante la utilidad de configuración de iDRAC.....	106
Obtención de certificados.....	106
Certificados de servidor SSL.....	107
Generación de una nueva solicitud de firma de certificado.....	109
Carga del certificado del servidor.....	109
Visualización del certificado del servidor.....	110
Carga del certificado de firma personalizado.....	111
Descarga del certificado de firma del certificado SSL personalizado	112
Eliminación del certificado de firma del certificado SSL personalizado.....	112
Configuración de varios iDRAC mediante RACADM.....	112
Creación de un archivo de configuración de iDRAC.....	113
Reglas de análisis.....	114
Modificación de la dirección IP de iDRAC.....	115
Desactivación del acceso para modificar los valores de configuración de iDRAC en el sistema host.....	116

5 Visualización de la información de iDRAC y el sistema administrado.... 117

Visualización de la condición y las propiedades de Managed System.....	117
Visualización del inventario del sistema.....	117
Visualización de la información del sensor.....	119
Supervisión del índice de rendimiento de CPU, memoria y módulos de E/S.....	121
Supervisión del índice de rendimiento de CPU, memoria y módulos de E/S mediante la interfaz web.....	122
Supervisión del índice de rendimiento de CPU, memoria y módulos de E/S mediante RACADM.....	122
Consulta del sistema para verificar el cumplimiento de aire fresco.....	123
Visualización de los datos históricos de temperatura.....	123
Visualización de los datos históricos de temperatura mediante la interfaz web de iDRAC.....	124
Visualización de datos históricos de temperatura mediante RACADM.....	124
Configuración del umbral de advertencia para la temperatura de entrada.....	124
Visualización de interfaces de red disponibles en el sistema operativo host.....	125

Visualización de interfaces de red disponibles en el sistema operativo host mediante la interfaz web.....	125
Visualización de interfaces de red disponibles en el sistema operativo host mediante RACADM.....	126
Visualización de las conexiones de red Fabric de la tarjeta mezzanine FlexAdress.....	126
Visualización o terminación de sesiones iDRAC.....	127
Terminación de las sesiones de iDRAC mediante la interfaz web.....	127
Terminación de las sesiones de iDRAC mediante RACADM.....	127

6 Configuración de la comunicación de iDRAC..... 128

Comunicación con iDRAC a través de una conexión serie mediante un cable DB9.....	129
Configuración del BIOS para la conexión serie.....	130
Activación de la conexión serie RAC.....	130
Activación de los modos básicos y de terminal de la conexión serie básica IPMI.....	131
Cambio entre la comunicación en serie RAC y la consola de comunicación en serie mediante el cable DB9.....	133
Cambio de una consola de comunicación en serie a la comunicación en serie RAC.....	133
Cambio de una comunicación en serie RAC a consola de comunicación en serie.....	133
Comunicación con iDRAC mediante IPMI SOL.....	134
Configuración del BIOS para la conexión serie.....	134
Configuración de iDRAC para usar SOL.....	135
Activación del protocolo compatible.....	136
Comunicación con iDRAC mediante IPMI en la LAN.....	140
Configuración de IPMI en la LAN mediante la interfaz web.....	140
Configuración de IPMI en la LAN mediante la utilidad de configuración de iDRAC.....	140
Configuración de IPMI en la LAN mediante RACADM.....	141
Activación o desactivación de RACADM remoto.....	141
Activación o desactivación de RACADM remoto mediante la interfaz web.....	141
Activación o desactivación de RACADM remoto mediante RACADM.....	141
Desactivación de RACADM local.....	142
Activación de IPMI en Managed System.....	142
Configuración de Linux para la consola de comunicación en serie durante el inicio.....	142
Activación del inicio de sesión en la consola virtual después del inicio.....	143
Esquemas de criptografía SSH compatibles.....	143
Uso de la autenticación de clave pública para SSH.....	144

7 Configuración de cuentas de usuario y privilegios..... 148

Configuración de usuarios locales.....	148
Configuración de usuarios locales mediante la interfaz web de iDRAC.....	148
Configuración de los usuarios locales mediante RACADM.....	149
Configuración de usuarios de Active Directory.....	151
Prerrequisitos del uso de la autenticación de Active Directory para iDRAC.....	153

Mecanismos de autenticación compatibles de Active Directory.....	155
Descripción general del esquema estándar de Active Directory.....	155
Configuración del esquema estándar de Active Directory.....	157
Descripción general del esquema extendido de Active Directory.....	160
Configuración del esquema extendido de Active Directory.....	163
Prueba de la configuración de Active Directory.....	173
Configuración de los usuarios LDAP genéricos.....	174
Configuración del servicio de directorio de LDAP genérico mediante la interfaz basada en web de iDRAC.....	174
Configuración del servicio de directorio LDAP genérico mediante RACADM.....	175
Prueba de la configuración del servicio de directorio de LDAP.....	175

8 Configuración de iDRAC para inicio de sesión único o inicio de sesión mediante tarjeta inteligente..... 177

Prerrequisitos para el inicio de sesión único de Active Directory o el inicio de sesión mediante tarjeta inteligente.....	177
Registro de iDRAC como equipo en el dominio raíz de Active Directory.....	178
Generación del archivo Keytab de Kerberos.....	178
Creación de objetos de Active Directory y establecimiento de privilegios.....	179
Configuración del explorador para activar el inicio de sesión único de Active Directory.....	179
Configuración del inicio de sesión SSO de iDRAC para usuarios de Active Directory.....	180
Configuración del inicio de sesión SSO de iDRAC para usuarios de Active Directory mediante la interfaz web.....	180
Configuración del inicio de sesión SSO de iDRAC para usuarios de Active Directory mediante RACADM.....	180
Configuración del inicio de sesión mediante tarjeta inteligente de iDRAC para usuarios locales.....	181
Carga del certificado de usuario de tarjeta inteligente.....	181
Carga del certificado de CA de confianza para tarjeta inteligente.....	181
Configuración del inicio de sesión mediante tarjeta inteligente de iDRAC para usuarios de Active Directory.....	182
Activación o desactivación del inicio de sesión mediante tarjeta inteligente.....	183
Activación o desactivación del inicio de sesión mediante tarjeta inteligente utilizando la interfaz web.....	183
Activación o desactivación del inicio de sesión mediante tarjeta inteligente utilizando RACADM.....	183
Activación o desactivación del inicio de sesión mediante tarjeta inteligente mediante la utilidad de configuración de iDRAC.....	184

9 Configuración de iDRAC para enviar alertas..... 185

Activación o desactivación de alertas.....	185
Activación o desactivación de alertas mediante la interfaz web.....	186

Activación o desactivación de alertas mediante RACADM.....	186
Activación o desactivación de alertas mediante la utilidad de configuración de iDRAC.....	186
Filtrado de alertas	186
Filtrado de alertas mediante la interfaz web de iDRAC.....	186
Filtrado de alertas mediante RACADM.....	187
Configuración de alertas de suceso.....	187
Configuración de alertas de suceso mediante la interfaz web.....	187
Configuración de alertas de suceso mediante RACADM.....	188
Configuración de suceso de periodicidad de alertas.....	188
Configuración de sucesos de periodicidad de alertas mediante la interfaz web de iDRAC....	188
Configuración de sucesos de periodicidad de alertas mediante RACADM.....	188
Configuración de acciones del suceso.....	188
Configuración de acciones del suceso mediante la interfaz web.....	189
Configuración de acciones del suceso mediante RACADM.....	189
Configuración de alertas por correo electrónico, capturas SNMP o capturas IPMI.....	189
Configuración de destinos de alerta IP.....	190
Configuración de los valores de alertas por correo electrónico.....	191
Configuración de sucesos de WS.....	194
Id. de mensaje de alertas.....	194
10 Administración de registros.....	198
Visualización del registro de sucesos del sistema.....	198
Visualización del registro de sucesos del sistema mediante la interfaz web.....	198
Visualización del registro de sucesos del sistema mediante RACADM.....	199
Visualización del registro de sucesos del sistema mediante la utilidad de configuración de iDRAC.....	199
Visualización del registro de Lifecycle	199
Visualización del registro de Lifecycle mediante la interfaz web.....	200
Visualización del registro de Lifecycle mediante RACADM.....	200
Exportación de los registros de Lifecycle Controller.....	200
Exportación de los registros de Lifecycle Controller mediante la interfaz web.....	201
Exportación de los registros de Lifecycle Controller mediante RACADM.....	201
Adición de notas de trabajo.....	201
Configuración del registro del sistema remoto.....	201
Configuración del registro del sistema remoto mediante la interfaz web.....	202
Configuración del registro del sistema remoto mediante RACADM.....	202
11 Supervisión y administración de la alimentación.....	203
Supervisión de la alimentación.....	203
Supervisión de la alimentación mediante la interfaz web.....	204
Supervisión de la alimentación mediante RACADM.....	204
Configuración del umbral de advertencia para consumo de alimentación.....	204

Configuración del umbral de advertencia para consumo de alimentación mediante la interfaz web.....	204
Ejecución de las operaciones de control de alimentación.....	205
Ejecución de las operaciones de control de alimentación mediante la interfaz web.....	205
Ejecución de las operaciones de control de alimentación mediante RACADM.....	205
Límites de alimentación.....	205
Límites de alimentación en servidores Blade.....	205
Visualización y configuración de la política de límites de alimentación.....	206
Configuración de las opciones de suministro de energía.....	207
Configuración de las opciones de suministro de energía mediante la interfaz web.....	208
Configuración de las opciones de suministro de energía mediante RACADM.....	208
Configuración de las opciones de suministro de energía mediante la utilidad de configuración de iDRAC.....	209
Activación o desactivación del botón de encendido.....	209

12 Inventario, supervisión y configuración de dispositivos de red..... 210

Inventario y supervisión de dispositivos de red.....	210
Supervisión de dispositivos de red mediante la interfaz web.....	210
Supervisión de dispositivos de red mediante RACADM.....	210
Inventario y supervisión de dispositivos HBA FC.....	211
Supervisión de dispositivos HBA FC mediante la interfaz web.....	211
Supervisión de dispositivos HBA FC mediante RACADM.....	211
Configuración dinámica de las direcciones virtuales, del iniciador y del destino de almacenamiento.....	211
Tarjetas admitidas para la optimización de la identidad de E/S.....	212
Versión del BIOS admitida para la optimización de la identidad de E/S.....	213
Versiones del firmware de la NIC admitidas para la optimización de la identidad de E/S.....	213
Comportamiento del sistema para FlexAddress e identidad de E /S	214
Activación o desactivación de la optimización de la identidad de E/S.....	215
Configuración de la política de persistencia.....	216

13 Administración de dispositivos de almacenamiento.....220

Comprensión de los conceptos de RAID.....	222
¿Qué es RAID?.....	222
Organización del almacenamiento de datos para obtener disponibilidad y rendimiento.....	223
Elección de niveles RAID	224
Comparación de rendimiento de niveles RAID.....	231
Controladoras admitidas.....	233
Controladoras RAID admitidas.....	233
Controladoras no RAID admitidas.....	233
Gabinetes admitidos.....	233
Resumen de funciones admitidas para Storage Devices (Dispositivos de almacenamiento).....	233

Inventario y supervisión de dispositivos de almacenamiento.....	236
Supervisión de dispositivos de almacenamiento mediante la interfaz web.....	237
Supervisión de dispositivos de almacenamiento mediante RACADM.....	237
Supervisión de plano posterior mediante la utilidad de configuración de iDRAC.....	237
Visualización de la topología de un dispositivo de almacenamiento.....	237
Administración de discos físicos.....	238
Asignación o desasignación de un disco físico como repuesto dinámico global.....	238
Convertir a disco RAID.....	239
Convertir a disco no RAID.....	240
Administración de discos virtuales.....	240
Creación de discos virtuales.....	240
Edición de políticas de caché de discos virtuales.....	242
Eliminación de discos virtuales.....	243
Revisión de congruencia en el disco virtual.....	244
Inicialización de discos virtuales.....	244
Cifrado de discos virtuales.....	245
Asignación o desasignación de repuestos dinámicos dedicados.....	246
Administración de discos virtuales mediante la interfaz web.....	246
Administración de discos virtuales mediante RACADM.....	247
Administración de controladoras.....	247
Configuración de las propiedades de la controladora.....	248
Importación o importación automática de la configuración ajena.....	251
Borrar configuración ajena.....	253
Restablecimiento de la configuración de la controladora.....	254
Operaciones con adaptadores HBA SAS de 12 Gbps.....	254
Supervisión de análisis de falla predictiva en unidades.....	255
Operaciones de la controladora en modo no RAID (HBA).....	255
Ejecución de trabajos de configuración de RAID en varias controladoras de almacenamiento.....	256
Administración de SSD PCIe.....	256
Inventario y supervisión de SSD PCIe.....	257
Preparar para quitar una unidad SSD PCIe.....	257
Borrado de datos de un dispositivo SSD PCIe.....	259
Administración de gabinetes o planos posteriores.....	260
Configuración del modo de plano posterior.....	261
Visualización de ranuras universales.....	263
Configuración de modo de SGPIO.....	264
Elección de modo de operación para aplicar configuración.....	265
Elección del modo de operación mediante la interfaz web.....	265
Elección del modo de operación mediante RACADM.....	266
Visualización y aplicación de operaciones pendientes.....	266

Visualización, aplicación o eliminación de operaciones pendientes mediante la interfaz web.....	266
Visualización y aplicación de operaciones pendientes mediante RACADM.....	267
Situaciones de almacenamiento: situaciones de aplicación de la operación.....	267
Caso 1: se seleccionó una operación de aplicación (Aplicar ahora, En el siguiente reinicio, o A la hora programada) y no hay operaciones pendientes existentes	
Caso 2: se seleccionó una operación de aplicación (Aplicar ahora, En el siguiente reinicio o A la hora programada) y existen operaciones pendientes	
Caso 3: se seleccionó Agregar a operaciones pendientes y no existen operaciones pendientes	
Caso 4: se seleccionó Agregar a operaciones pendientes y no existen operaciones pendientes anteriores.....	267
Forma de hacer parpadear o dejar de hacer parpadear LED de componentes.....	269
Forma de hacer parpadear o dejar de hacer parpadear LED de componentes mediante la interfaz web.....	269
Blinking or Unblinking Component LEDs Using RACADM.....	270

14 Configuración y uso de la consola virtual.....271

Resoluciones de pantalla y velocidades de actualización admitidas.....	271
Configuración de exploradores web para usar la consola virtual.....	272
Configuración de exploradores web para usar el complemento Java.....	273
Configuración de IE para usar el complemento ActiveX.....	273
Importación de certificados de CA a Management Station.....	275
Configuración de la consola virtual.....	276
Configuración de la consola virtual mediante la interfaz web.....	276
Configuración de la consola virtual mediante RACADM.....	276
Vista previa de la consola virtual.....	277
Inicio de la consola virtual.....	277
Inicio de la consola virtual mediante la interfaz web.....	278
Inicio de la consola virtual mediante URL.....	278
Desactivación de mensajes de advertencia mientras se inicia la consola virtual o los medios virtuales mediante el complemento de Java o ActiveX.....	279
Uso del visor de la consola virtual.....	279
Sincronización de los punteros del mouse	280
Pulsación de teclas a través de la consola virtual.....	281

15 Administración de medios virtuales.....285

Unidades y dispositivos compatibles.....	286
Configuración de medios virtuales.....	286
Configuración de medios virtuales mediante la interfaz web de iDRAC.....	286
Configuración de medios virtuales mediante RACADM.....	287
Configuración de medios virtuales mediante la utilidad de configuración de iDRAC.....	287
Estado de medios conectados y respuesta del sistema.....	287
Acceso a medios virtuales.....	288

Inicio de medios virtuales mediante la consola virtual.....	288
Inicio de medios virtuales sin usar la consola virtual.....	289
Adición de imágenes de medios virtuales.....	289
Visualización de los detalles del dispositivo virtual.....	290
Restablecimiento de USB.....	290
Asignación de la unidad virtual.....	290
Anulación de la asignación de la unidad virtual.....	292
Configuración del orden de inicio a través del BIOS.....	292
Activación del inicio único para medios virtuales.....	293
16 Instalación y uso de la utilidad de VMCLI.....	294
Instalación de VMCLI.....	294
Ejecución de la utilidad de VMCLI.....	294
Sintaxis de VMCLI.....	295
Comandos de VMCLI para acceder a los medios virtuales	295
Opciones de shell del sistema operativo de VMCLI	296
17 Administración de la tarjeta vFlash SD.....	297
Configuración de la tarjeta vFlash SD.....	297
Visualización de las propiedades de la tarjeta vFlash SD.....	298
Activación o desactivación de la funcionalidad vFlash.....	298
Inicialización de la tarjeta vFlash SD.....	299
Obtención del último estado mediante RACADM.....	300
Administración de las particiones vFlash.....	301
Creación de una partición vacía.....	301
Creación de una partición mediante un archivo de imagen.....	302
Formateo de una partición.....	303
Visualización de las particiones disponibles.....	304
Modificación de una partición.....	304
Conexión o desconexión de particiones.....	305
Eliminación de las particiones existentes.....	306
Descarga del contenido de una partición.....	307
Inicio de una partición.....	308
18 Uso de SMCLP.....	309
Capacidades de System Management mediante SMCLP.....	309
Ejecución de los comandos SMCLP.....	310
Sintaxis SMCLP de iDRAC.....	310
Navegación en el espacio de direcciones de MAP.....	313
Uso de Show Verb.....	314
Uso de la opción -display.....	314
Uso de la opción -level.....	314

Uso de la opción -output.....	314
Ejemplos de uso.....	314
Administración de la alimentación del servidor.....	315
Administración de SEL.....	315
Navegación en MAP del destino.....	317
19 Uso del módulo de servicio del iDRAC	318
Instalación del módulo de servicio del iDRAC.....	318
Sistemas operativos admitidos para el módulo de servicio de iDRAC.....	318
Funciones de supervisión del módulo de servicio del iDRAC	319
Información sobre el sistema operativo	319
Replicar registros de Lifecycle en el registro del sistema operativo	319
Opciones de recuperación automática del sistema	320
Proveedores del Instrumental de administración de Windows	320
Coexistencia de OpenManage Server Administrator y módulo de servicio del iDRAC	321
Uso del módulo de servicio del iDRAC desde la interfaz web del iDRAC.....	322
Uso del módulo de servicio del iDRAC desde RACADM.....	322
20 Uso de un puerto USB para la administración del servidor	323
Acceso a la interfaz de iDRAC por medio de la conexión USB directa.....	323
Configuración de iDRAC mediante el perfil de configuración del servidor en un dispositivo USB.....	324
Configuración de los valores de puerto de administración USB.....	324
Importación de un perfil de configuración del servidor desde un dispositivo USB	327
21 Uso de la sincronización rápida de iDRAC.....	330
Configuración de la sincronización rápida de iDRAC.....	331
Configuración de los ajustes de sincronización rápida de iDRAC mediante la interfaz web..	331
Configuración de los valores de sincronización rápida de iDRAC mediante RACADM.....	331
Configuración de los valores de sincronización rápida del iDRAC mediante la utilidad de configuración de iDRAC.....	332
Uso de dispositivos móviles para ver información de iDRAC.....	332
22 Implementación de los sistemas operativos.....	333
Implementación del sistema operativo mediante VMCLI	333
Implementación del sistema operativo mediante recurso compartido de archivos remotos.....	335
Administración de recursos compartidos de archivos remotos.....	335
Configuración de recursos compartidos de archivos remotos mediante la interfaz web.....	336
Configuración de recursos compartidos de archivos remotos mediante RACADM.....	337
Implementación del sistema operativo mediante medios virtuales.....	338
Instalación del sistema operativo desde varios discos.....	339
Implementación del sistema operativo incorporado en la tarjeta SD.....	339

Activación del módulo SD y la redundancia del BIOS.....	339
23 Solución de problemas de Managed System mediante iDRAC.....	341
Uso de la consola de diagnósticos.....	341
Programación del diagnóstico automatizado remoto.....	342
Programación de diagnóstico automatizado remoto mediante RACADM.....	343
Visualización de los códigos de la POST.....	343
Visualización de videos de captura de inicio y bloqueo.....	343
Configuración de los valores de captura de video.....	344
Visualización de registros.....	344
Visualización de la pantalla de último bloqueo del sistema.....	344
Visualización del estado del panel frontal.....	344
Visualización del estado del LCD del panel frontal del sistema.....	345
Visualización del estado del LED del panel frontal del sistema.....	345
Indicadores de problemas del hardware.....	346
Visualización de la condición del sistema.....	346
Generación de un informe de asistencia técnica.....	347
Generación de un informe de asistencia técnica de forma automática.....	348
Generación de informe de asistencia técnica de forma manual.....	349
Consulta de la pantalla de estado del servidor en busca de mensajes de error.....	351
Reinicio de iDRAC.....	351
Reinicio de iDRAC mediante la interfaz web de iDRAC.....	351
Reinicio de iDRAC mediante RACADM.....	351
Borrado de datos del sistema y del usuario.....	351
Restablecimiento de iDRAC a los valores predeterminados de fábrica.....	352
Restablecimiento de iDRAC a los valores predeterminados de fábrica mediante la interfaz web de iDRAC.....	352
Restablecimiento de iDRAC a los valores predeterminados de fábrica mediante la utilidad de configuración de iDRAC.....	353
24 Preguntas frecuentes.....	354
Registro de sucesos del sistema.....	354
Seguridad de la red.....	355
Active Directory.....	355
Inicio de sesión único.....	358
Inicio de sesión mediante tarjeta inteligente.....	359
Consola virtual.....	360
Medios virtuales.....	364
Tarjeta vFlash SD.....	366
Autenticación SNMP.....	367
Dispositivos de almacenamiento.....	367
iDRAC Service Module.....	367

RACADM.....	369
Varios.....	371

25 Situación de uso..... 374

Solución de problemas de un Managed System inaccesible.....	374
Obtención de la información del sistema y evaluación de la condición del sistema.....	375
Establecimiento de alertas y configuración de alertas por correo electrónico.....	375
Visualización y exportación del registro de Lifecycle y el registro de sucesos del sistema.....	375
Interfaces para actualizar el firmware de iDRAC.....	376
Realización de un apagado ordenado del sistema.....	376
Creación de una nueva cuenta de usuario de administrador.....	376
Inicio de la consola remota de servidores y montaje de una unidad USB.....	376
Instalación del sistema operativo básico conectado a los medios virtuales y los recursos compartidos de archivos remotos.....	377
Administración de la densidad de bastidor.....	377
Instalación de una nueva licencia electrónica.....	377
Aplicación de valores de configuración de la identidad de E/S para varias tarjetas de red en un reinicio del sistema host individual	377

Descripción general

Integrated Dell Remote Access Controller (iDRAC) está diseñado para mejorar la productividad de los administradores de servidor y mejorar la disponibilidad global de los servidores de Dell. iDRAC alerta a los administradores sobre los problemas de servidor, les ayuda a realizar tareas de administración de servidor remota y reduce la necesidad de obtener acceso físico al servidor.

iDRAC con tecnología de Lifecycle Controller forma parte de una solución de centro de datos más grande que ayuda a que las aplicaciones empresariales críticas y las cargas de trabajo estén disponibles en todo momento. La tecnología permite a los administradores implementar, supervisar, administrar, configurar, actualizar y buscar y solucionar problemas de los servidores de Dell desde cualquier ubicación. Esto lo hace independientemente del sistema operativo o la presencia o el estado del hipervisor.

Varios productos funcionan conjuntamente con iDRAC y Lifecycle Controller para simplificar y agilizar las operaciones de TI, como por ejemplo:

- Dell Management plug-in for VMware vCenter
- Dell Repository Manager
- Dell Management Packs para Microsoft System Center Operations Manager (SCOM) y Microsoft System Center Configuration Manager (SCCM)
- BMC Bladelogic
- Dell OpenManage Essentials
- Dell OpenManage Power Center

iDRAC está disponible en las variantes siguientes:

- Basic Management con IPMI (disponible de manera predeterminada para los servidores serie 200 a 500)
- iDRAC Express (disponible de manera predeterminada para todos los servidores tipo bastidor y torre serie 600 y superiores, y para todos los servidores blade)
- iDRAC Enterprise (disponible en todos los modelos de servidores)

Para obtener más información, consulte *iDRAC Overview and Feature Guide* (Guía de información general y funciones de iDRAC), disponible en dell.com/support/manuals.

Ventajas al utilizar iDRAC con Lifecycle Controller

Entre las ventajas se incluyen las siguientes:

- Mayor disponibilidad: notificación temprana de fallas potenciales o reales que ayudan a evitar una falla de servidor o reducir el tiempo de recuperación después de una falla.

- Productividad mejorada y menor costo total de propiedad (TCO): la extensión del alcance que tienen los administradores a un mayor número de servidores remotos puede mejorar la productividad del personal de TI mientras se reducen los costos operativos, tales como los viajes.
- Entorno seguro: al proporciona acceso seguro a servidores remotos, los administradores pueden realizar funciones críticas de administración mientras conservan la seguridad del servidor y la red.
- Mejor administración incorporada a través de Lifecycle Controller: Lifecycle Controller proporciona capacidades de implementación y servicios simplificados a través de la GUI de Lifecycle Controller para la implementación local y las interfaces de servicios remotos (WS-Management) para la implementación remota incorporada con Dell OpenManage Essentials y consolas de asociados.

Para obtener más información acerca de la GUI de Lifecycle Controller, consulte *Lifecycle Controller User's Guide* (Guía del usuario de Dell LifeCycle Controller) y para obtener información sobre los servicios remotos, consulte *Lifecycle Controller Remote Services User's Guide* (Guía del usuario de Lifecycle Controller Remote Services) disponible en dell.com/support/manuals.

Funciones clave

Entre las funciones clave del iDRAC se incluye lo siguiente:

- ✍ **NOTA:** Algunas de las funciones solamente están disponibles con la licencia iDRAC Enterprise. Para obtener información sobre las funciones disponibles para una licencia, consulte [Administración de licencias](#).

Inventario y supervisión

- Visualización de la condición del servidor administrado
- Realización de inventarios y supervisión de los adaptadores de red y del subsistema de almacenamiento (PERC y almacenamiento conectado directamente) sin la intervención de agentes del sistema operativo
- Visualización y exportación del inventario del sistema
- Visualización de la información del sensor, como la temperatura, el voltaje y la intrusión
- Supervisión del estado de CPU, de la limitación automática del procesador y de la falla predictiva
- Visualización de la información de memoria
- Supervisión y control del uso de la alimentación
- Compatibilidad con SNMPv3 GET
- Servidores Blade: inicio de la interfaz web de Chassis Management Controller (CMC), visualización de la información CMC y direcciones WWN/MAC.

- ✍ **NOTA:** CMC proporciona acceso a iDRAC a través del panel LCD del chasis M1000E y conexiones de la consola local. Para obtener más información, consulte la *Guía de usuario de Chassis Management Controller* disponible en dell.com/support/manuals.

- Visualización de las interfaces de red disponibles en los sistemas operativos host
- Ver el inventario, supervisar la información y configurar las opciones básicas del iDRAC con la función de sincronización rápida del iDRAC y un dispositivo móvil.

Implementación

- Administración de las particiones de tarjeta vFlash SD
- Configuración de los valores de visualización del panel frontal
- Administración de la configuración de red del iDRAC
- Configuración y uso de la consola virtual y los medios virtuales

- Implementación de sistemas operativos mediante recursos compartidos de archivos remotos, medios virtuales y VMCLI
- Activación del descubrimiento automático
- Realice la configuración del servidor con la función de perfil XML de exportación o importación a través de RACADM y WS-MAN. Para obtener más información, consulte la *Guía de inicio rápido de Lifecycle Controller Remote Services*.
- Configuración de la política de persistencia de las direcciones virtuales, del iniciador y los destinos de almacenamiento
- Configuración remota de los dispositivos de almacenamiento conectados al sistema durante el tiempo de ejecución
- Realice las siguientes operaciones para los dispositivos de almacenamiento:
 - Discos físicos: asignar o desasignar discos físicos como repuestos dinámicos globales.
 - Discos virtuales:
 - * Crear discos virtuales.
 - * Editar las políticas de la caché de los discos virtuales.
 - * Ejecutar una revisión de congruencia en el disco virtual.
 - * Inicializar discos virtuales.
 - * Cifrar discos virtuales.
 - * Asignar o desasignar repuestos dinámicos dedicados.
 - * Eliminar discos virtuales.
 - Controladoras:
 - * Configurar propiedades de la controladora.
 - * Importar o importar automáticamente configuración ajena.
 - * Borrar configuración ajena.
 - * Restablecer configuración de la controladora.
 - * Crear o cambiar claves de seguridad.
 - Dispositivos SSD PCIe:
 - * Realizar un inventario y supervisar de forma remota la condición de los dispositivos SSD PCIe en el servidor
 - * Preparar para quitar SSD PCIe.
 - * Borrar los datos de manera segura.
 - Establecer el modo de plano posterior (modo unificado o dividido)
 - Hacer parpadear o dejar de hacer parpadear LED de componentes.
 - Aplicar la configuración del dispositivo inmediatamente, en el siguiente reinicio del sistema, en un tiempo programado o como una operación pendiente que se aplicará en un lote como parte de un único trabajo

Actualizar

- Administración de licencias del iDRAC
- Actualización del BIOS y firmware de dispositivos para dispositivos compatibles con Lifecycle Controller.
- Actualización o reversión del firmware de Lifecycle Controller y del firmware del iDRAC por medio de una única imagen de firmware
- Administración de actualizaciones preconfiguradas
- Creación de copia de seguridad y restauración del perfil del servidor.

- Acceder a la interfaz de iDRAC a través de una conexión USB directa.
- Configuración de iDRAC mediante perfiles de configuración del servidor en el dispositivo USB.

Mantenimiento y solución de problemas

- Operaciones relacionadas con la alimentación y supervisión del consumo de alimentación
- Optimización del rendimiento del sistema y del consumo de alimentación mediante la modificación de la configuración térmica
- Independencia de Server Administrator para la generación de alertas.
- Registro de datos de sucesos: registro de Lifecycle y de RAC.
- Establecimiento de alertas por correo electrónico, alertas IPMI, registros del sistema remoto, registros de sucesos de WS y capturas SNMP (v1, v2c y v3) para sucesos y notificación mejorada de alertas por correo electrónico.
- Captura de la última imagen de bloqueo del sistema.
- Visualización de vídeos de captura de inicio y bloqueo.
- Supervisión y generación de alerta fuera de banda del índice de rendimiento de la CPU, la memoria y los módulos de E/S.
- Configuración del umbral de advertencia para la temperatura de entrada y el consumo de alimentación.
- Utilice el módulo de servicio de iDRAC para:
 - Ver información sobre el sistema operativo (SO).
 - Replicar los registros de Lifecycle Controller en los registros del sistema operativo.
 - Opciones de recuperación automática del sistema.
 - Relleno de datos del instrumental de administración de Windows (WMI).
 - Integración con el informe de asistencia técnica. Esto se aplica únicamente si se ha instalado el módulo de servicio de iDRAC versión 2.0 o posterior. Para obtener más información, consulte [Generación de un informe de asistencia técnica](#).
 - Preparar para quitar un SSD PCIe NVMe. Para obtener más información, consulte [Preparación para quitar SSD PCIe](#).
- Genere el informe de asistencia técnica de las siguientes maneras:
 - Automática: el uso del módulo de servicio del iDRAC que automáticamente invoca la herramienta OS Collector.
 - Manual: mediante la herramienta OS Collector.

Conectividad segura

Proteger el acceso a recursos de red críticos es una prioridad. iDRAC implementa una variedad de funciones de seguridad, entre ellas las siguientes:

- Certificado de firma personalizado para el certificado de capa de sockets seguros (SSL).
- Actualizaciones de firmware firmadas.
- Autenticación de usuarios a través de Microsoft Active Directory, servicio de directorio del protocolo ligero de acceso a directorios (LDAP) genérico o contraseñas e identificaciones de usuario administrados de manera local.
- Autenticación de factor doble mediante la función de inicio de sesión mediante tarjeta inteligente. La autenticación de factor doble se basa en la tarjeta inteligente física y el PIN correspondiente.
- Inicio de sesión único y autenticación de clave pública.
- Autorización basada en roles con el fin de configurar privilegios específicos para cada usuario.

- Autenticación SNMPv3 para cuentas de usuario almacenadas localmente en el iDRAC; esta opción es la recomendada, pero está desactivada de forma predeterminada.
- Configuración de la identificación y contraseña del usuario.
- Modificación de la contraseña de inicio de sesión predeterminada.
- Configuración de las contraseñas de usuario y las contraseñas del BIOS mediante un formato de algoritmo hash unidireccional para una mayor seguridad.
- Interfaces web y SMCLP 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 configurables (para HTTP, HTTPS, SSH, Telnet, consola virtual y medios virtuales).
 - ✎ **NOTA:** Telnet no admite el cifrado SSL y está desactivado de manera predeterminada.
- Shell seguro (SSH), que utiliza una capa cifrada de transporte para brindar una 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 limitado de direcciones IP para clientes que se conectan al iDRAC.
- Adaptador Gigabit Ethernet dedicado en servidores tipo bastidor y torre disponible (es posible que se necesite hardware adicional).

Novedades de esta versión

- Compatibilidad con los siguientes sistemas PowerEdge:
 - PowerEdge T430
 - PowerEdge R530
 - PowerEdge R430
 - PowerEdge M630
 - PowerEdge FC630
- Configuración de valores de actualización del firmware del CMC para realizar la actualización del firmware del CMC y sus componentes compartidos desde el iDRAC. Esto se aplica a los chasis FX2/ FX2s
- Actualización a la lista de funciones sujetas a licencia.
- Compatibilidad para nombre de dominio DNS en las capturas SNMP.

Cómo usar esta guía del usuario

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

- Interfaz web de iDRAC: aquí se proporciona solo la información relacionada con la tarea. Para obtener información sobre los campos y las opciones, consulte la *Ayuda en línea de iDRAC*, a la que puede acceder desde la interfaz web.
- RACADM: Aquí se proporciona el comando u objeto RACADM que debe usar. Para obtener más información, consulte la *Guía de referencia de línea de comandos RACADM* disponible en **dell.com/support/manuals**.
- Utilidad de configuración de iDRAC: aquí se proporciona solo la información relacionada con la tarea. Para obtener más información sobre los campos y las opciones, consulte la *Ayuda en línea de la utilidad de configuración de iDRAC*, a la que puede acceder cuando hace clic en **Ayuda** en la interfaz gráfica de usuario de configuración del iDRAC (presione <F2> durante el inicio y luego haga clic en **Configuración de iDRAC** en la página **Menú principal de configuración del sistema**).

Exploradores web compatibles

iDRAC es compatible con los siguientes exploradores:

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari

Para ver la lista de versiones, consulte las *Notas de publicación de iDRAC8*, disponibles en dell.com/support/manuals.

Administración de licencias

Las funciones de iDRAC están disponibles según la licencia adquirida (Basic Management, iDRAC Express o iDRAC Enterprise). Solo las funciones con licencia están disponibles en la interfaces que permiten configurar o utilizar iDRAC. Por ejemplo, la interfaz web de iDRAC, RACADM, WS-MAN, OpenManage Server Administrator, etc. Algunas funciones, como NIC dedicada o vFlash requieren tarjetas de puerto de iDRAC, que son componentes opcionales para servidores de la serie 200-500.

La funcionalidad de actualización del firmware y administración de licencias de iDRAC está disponible a través de la interfaz web de iDRAC y RACADM.

Tipos de licencias

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

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


Adquisición de licencias

Utilice cualquiera de los métodos siguientes para adquirir licencias:

- Correo electrónico: la licencia se adjunta a un correo electrónico que se envía después de solicitarlo desde el centro de asistencia técnica.
- Portal de autoservicio: hay un vínculo a un portal de autoservicio disponible en iDRAC. Haga clic en este vínculo para abrir el portal de autoservicio de licencias en Internet. Actualmente, se puede usar el portal de autoservicio de licencias para recuperar licencias adquiridas con el servidor. Debe ponerse en contacto con el representante de ventas o de asistencia técnica para comprar una licencia de actualización o una nueva. Para obtener más información, consulte la ayuda en línea correspondiente a la página del portal de autoservicio.
- Punto de venta: la licencia se adquiere al realizar un pedido de un sistema.


Operaciones de licencia

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


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

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

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

 **NOTA:** Para algunas funciones, su activación requiere un reinicio del sistema.

- Exportar: exporte la licencia instalada en un dispositivo de almacenamiento externo como copia de seguridad o para reinstalarla después de reemplazar la placa base parcial o completamente. El nombre de archivo y el formato de la licencia exportada es **<EntitlementID>.xml**.
- Eliminar: elimine la licencia asignada a un componente cuando este no esté presente. Una vez eliminada la licencia, ya no se almacenará en iDRAC y se activarán las funciones del producto base.
- Reemplazar: reemplace la licencia para extender una licencia de evaluación, cambiar un tipo de licencia (tal como una licencia de evaluación por una licencia adquirida) o extender una licencia caducada.
 - Una licencia de evaluación se puede reemplazar con una licencia de evaluación actualizada o con una licencia adquirida.
 - Una licencia adquirida se puede reemplazar con una licencia actualizada o con una licencia ampliada.
- Más información: obtenga más información acerca de la licencia instalada o las licencias disponibles para un componente instalado en el servidor.

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

Para realizar una implementación de licencias de uno a varios, puede utilizar Dell License Manager. Para obtener más información, consulte *Dell License Manager User's Guide* (Guía del usuario de Dell License Manager) disponible en dell.com/support/manuals.

Importación de la licencia después de reemplazar la placa base

Puede utilizar la herramienta de instalación local de la licencia iDRAC Enterprise si reemplazó recientemente la placa base y necesita volver a instalar localmente (sin conectividad de red) la licencia iDRAC Enterprise y activar la NIC dedicada. Esta utilidad permite instalar una licencia iDRAC Enterprise de prueba por 30 días y restablecer el iDRAC para cambiar de la NIC compartida a la NIC dedicada.

Para obtener más información acerca de esta utilidad y descargar la herramienta, haga clic [aquí](#).

Estado o condición del componente de licencia y operaciones disponibles

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

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

Estado o condición de la licencia o el componente	Importar	Exportar	Eliminar	Reemplazar	Más información
Inicio de sesión no de administrador	No	No	No	No	Sí
Licencia activa	Sí	Sí	Sí	Sí	Sí
Licencia caducada	No	Sí	Sí	Sí	Sí
Licencia instalada pero falta el componente	No	Sí	Sí	No	Sí

 **NOTA:** En la interfaz web de iDRAC, en la página **Licencias**, expanda el dispositivo para ver la opción **Reemplazar** en el menú desplegable.

Administración de licencias mediante la interfaz web de iDRAC

Para administrar licencias mediante la interfaz web de iDRAC, vaya a **Descripción general ServidorLicencias**.

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

Administración de licencias mediante RACADM

Para administrar licencias mediante RACADM, utilice el subcomando **license**. Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8), disponible en dell.com/support/manuals.

Funciones con licencia en iDRAC8

En la siguiente tabla se proporcionan las funciones de iDRAC8 activadas según la licencia adquirida.

Función	iDRAC8 Basic	iDRAC8 Express	iDRAC8 Express para servidores blade	iDRAC8 Enterprise
Interfaces/estándares				
IPMI 2.0	Sí	Sí	Sí	Sí
DCMI 1.5	Sí	Sí	Sí	Sí
Interfaz gráfica web del usuario	Sí	Sí	Sí	Sí

Función	iDRAC8 Basic	iDRAC8 Express	iDRAC8 Express para servidores blade	iDRAC8 Enterprise
Línea de comandos racadm (local/remota)	Sí	Sí	Sí	Sí
SMASH-CLP (solo SSH)	Sí	Sí	Sí	Sí
Telnet	Sí	Sí	Sí	Sí
SSH	Sí	Sí	Sí	Sí
WSMAN	Sí	Sí	Sí	Sí
Protocolo de tiempo de la red	No	Sí	Sí	Sí
Conectividad				
NIC compartido	Sí	Sí	N/A	Sí ¹
NIC dedicado ²	Sí	Sí	Sí	Sí ²
Etiquetado VLAN	Sí	Sí	Sí	Sí
IPv4	Sí	Sí	Sí	Sí
IPv6	Sí	Sí	Sí	Sí
DHCP	Sí	Sí	Sí	Sí
DNS dinámico	Sí	Sí	Sí	Sí
Paso a través del sistema operativo	Sí	Sí	Sí	Sí
USB del panel frontal	Sí	Sí	Sí	Sí
Seguridad				
Autoridad basada en roles	Sí	Sí	Sí	Sí
Usuarios locales	Sí	Sí	Sí	Sí
Cifrado SSL	Sí	Sí	Sí	Sí
Bloqueo de IP	No	Sí	Sí	Sí
Servicios de directorio (AD, LDAP)	No	No	No	Sí

Función	iDRAC8 Basic	iDRAC8 Express	iDRAC8 Express para servidores blade	iDRAC8 Enterprise
Autenticación de dos factores (tarjeta inteligente)	No	No	No	Sí
Inicio de sesión único (Kerberos)	No	No	No	Sí
Autenticación de PK (para SSH)	No	Sí	Sí	Sí
Presencia remota				
Control de alimentación	Sí	Sí	Sí	Sí
Control de inicio	Sí	Sí	Sí	Sí
Comunicación en serie en la LAN	Sí	Sí	Sí	Sí
Medios virtuales	No	No	Sí	Sí
Carpetas virtuales	No	No	No	Sí
Recurso compartido de archivos remotos	No	No	No	Sí
Consola virtual	No	No	Sí	Sí
Conexión VNC al sistema operativo	No	No	No	Sí
Control de calidad/ancho de banda	No	No	Sí	Sí
Colaboración de consola virtual (hasta seis usuarios en simultáneo)	No	No	No	Sí
Chat de consola virtual	No	No	No	Sí
Particiones de flash virtual	No	No	No	Sí ^{2,3}
Alimentación y elementos térmicos				
Encendido automático tras la pérdida	Sí	Sí	Sí	Sí
Medidor de alimentación en tiempo real	Sí	Sí	Sí	Sí

Función	iDRAC8 Basic	iDRAC8 Express	iDRAC8 Express para servidores blade	iDRAC8 Enterprise
Umbrales de alimentación y alertas (incluye espacio)	No	Sí	Sí	Sí
Gráficos de alimentación en tiempo real	No	Sí	Sí	Sí
Contadores de datos históricos de alimentación	No	Sí	Sí	Sí
Límites de alimentación	No	No	No	Sí
Integración de Power Center	No	No	No	Sí
Supervisión de la temperatura	Sí	Sí	Sí	Sí
Gráficos de temperatura	No	Sí	Sí	Sí
Supervisión de la condición				
Supervisión completa sin agentes	Sí	Sí	Sí	Sí
Supervisión predictiva de fallas	Sí	Sí	Sí	Sí
SNMPv1 y v2 y v3 (capturas y obtenciones)	Sí	Sí	Sí	Sí
Alertas de correo electrónico	No	Sí	Sí	Sí
Umbrales configurables	Sí	Sí	Sí	Sí
Supervisión de ventiladores	Sí	Sí	Sí	Sí
Supervisión de suministros de energía	Sí	Sí	Sí	Sí
Supervisión de memoria	Sí	Sí	Sí	Sí
Supervisión de CPU	Sí	Sí	Sí	Sí
Supervisión de RAID	Sí	Sí	Sí	Sí
Supervisión de NIC	Sí	Sí	Sí	Sí

Función	iDRAC8 Basic	iDRAC8 Express	iDRAC8 Express para servidores blade	iDRAC8 Enterprise
Supervisión de discos duros (gabinete)	Sí	Sí	Sí	Sí
Supervisión de rendimiento fuera de banda	No	No	No	Sí
Actualizar				
Actualización remota sin agentes	Sí	Sí	Sí	Sí
Herramientas de actualización incorporadas	Sí	Sí	Sí	Sí
Sincronización con un repositorio (actualizaciones programadas)	No	No	No	Sí
Actualización automática	No	No	No	Sí
Implementación y configuración				
Herramientas incorporadas de implementación del sistema operativo	Sí	Sí	Sí	Sí
Herramientas de configuración incorporadas (Utilidad de configuración del iDRAC)	Sí	Sí	Sí	Sí
Asistentes de configuración incorporados (asistentes de Lifecycle Controller)	Sí	Sí	Sí	Sí
Descubrimiento automático	No	Sí	Sí	Sí
Implementación remota del sistema operativo	No	Sí	Sí	Sí
Paquete incorporado de controladores	Sí	Sí	Sí	Sí
Configuración completa del inventario	Sí	Sí	Sí	Sí

Función	iDRAC8 Basic	iDRAC8 Express	iDRAC8 Express para servidores blade	iDRAC8 Enterprise
Exportación de inventario	Sí	Sí	Sí	Sí
Configuración remota	Sí	Sí	Sí	Sí
Configuración sin intervención	No	No	No	Sí
Retiro/reasignación del sistema	Sí	Sí	Sí	Sí
Diagnóstico, servicio y registro				
Herramientas de diagnóstico incorporadas	Sí	Sí	Sí	Sí
Reemplazo de piezas	No	Sí	Sí	Sí
Copia de seguridad de la configuración del servidor	No	No	No	Sí
Restauración de la configuración del servidor	Sí	Sí	Sí	Sí
Easy Restore (configuración del sistema)	Sí	Sí	Sí	Sí
LED/LCD de condición	Sí	Sí	Sí	Sí
Sincronización rápida (requiere bisel de NFC)	Sí	Sí	N/A	Sí
iDRAC directo (puerto de administración de USB frontal)	Sí	Sí	Sí	Sí
Módulo de servicio del iDRAC (iSM)	Sí	Sí	Sí	Sí
Informe de asistencia técnica incorporado	Sí	Sí	Sí	Sí
Captura de pantalla de bloqueo	No	Sí	Sí	Sí
Captura de video de bloqueo	No	No	No	Sí

Función	iDRAC8 Basic	iDRAC8 Express	iDRAC8 Express para servidores blade	iDRAC8 Enterprise
Captura de inicio	No	No	No	Sí
Restablecimiento manual del iDRAC	Sí	Sí	Sí	Sí
NMI virtual	Sí	Sí	Sí	Sí
Vigilancia del sistema operativo	Sí	Sí	Sí	Sí
Informe de condición incorporado	Sí	Sí	Sí	Sí
Registro de sucesos del sistema	Sí	Sí	Sí	Sí
Registro de Lifecycle	Sí	Sí	Sí	Sí
Notas de trabajo	Sí	Sí	Sí	Sí
Syslog remoto	No	No	No	Sí
Administración de licencias	Sí	Sí	Sí	Sí

[1] No disponible con servidores blade.

[2] Los servidores tipo bastidor y torre serie 500 e inferiores requieren una tarjeta de hardware para activar esta función. Este hardware se ofrece a un costo adicional.

[3] Requiere medios de la tarjeta SD vFlash.

Interfaces y protocolos para acceder a iDRAC

En la siguiente tabla se enumeran las interfaces para acceder a iDRAC.





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

Tabla 2. Interfaces y protocolos para acceder a iDRAC

Interfaz o protocolo	Descripción
Utilidad iDRAC Settings (Configuración de iDRAC)	Utilice la utilidad de configuración de iDRAC para realizar operaciones previas al sistema operativo. Posee un conjunto de funciones disponibles en la interfaz web de iDRAC, además de otras funciones.

Interfaz o protocolo	Descripción
Interfaz web del iDRAC	<p>Para acceder a la interfaz de configuración de iDRAC, presione <F2> durante el inicio y haga clic en Configuración de iDRAC en la página Menú principal de configuración del sistema.</p> <p>Utilice la interfaz web de iDRAC para administrar iDRAC y controlar el sistema administrado. El explorador se conecta al servidor web a través del puerto HTTPS. Los flujos de datos se cifran mediante SSL de 128 bits para proporcionar privacidad e integridad. Todas las conexiones al puerto HTTP se redireccionan a HTTPS. Los administradores pueden cargar su propio certificado SSL a través de un proceso de generación de SSL CSR para proteger el servidor web. Los puertos HTTP y HTTPS se pueden cambiar y el acceso de usuario se basa en los privilegios de usuario.</p>
RACADM	<p>Use esta utilidad de línea de comandos para realizar la administración de iDRAC y del servidor. Puede utilizar RACADM de manera local y remota.</p> <ul style="list-style-type: none"> • La interfaz de línea de comandos RACADM local se ejecuta en los sistemas administrados que tengan instalado Server Administrator. RACADM local se comunica con iDRAC a través de su interfaz de host IPMI dentro de banda. Dado que está instalado en el sistema administrado local, los usuarios deben iniciar sesión en el sistema operativo para ejecutar esta utilidad. Un usuario debe disponer de privilegios de administrador completo para utilizar esta utilidad. • El RACADM remoto es una utilidad cliente que se ejecuta en una estación de trabajo. Utiliza la interfaz de red fuera de banda para ejecutar los comandos RACADM en los sistemas administrados y utiliza el canal HTTPS. La opción -r ejecuta el comando RACADM sobre una red. • El RACADM de firmware no es accesible al iniciar sesión en iDRAC mediante SSH o Telnet. Puede ejecutar los comandos de RACADM de firmware sin especificar la dirección IP, el nombre de usuario o la contraseña de iDRAC. • No debe especificar la dirección IP, el nombre de usuario o la contraseña de iDRAC para ejecutar los comandos de RACADM de firmware. Después de entrar en el símbolo del sistema de RACADM, puede ejecutar directamente los comandos sin el prefijo racadm.
Panel LCD de servidor/panel LCD de chasis	<p>Utilice la pantalla LCD en el panel frontal del servidor para realizar lo siguiente:</p> <ul style="list-style-type: none"> • Ver alertas, la dirección IP o MAC de iDRAC, las cadenas programables del usuario • Configurar DHCP • Configurar la dirección IP de iDRAC <p>Para servidores Blade, la pantalla LCD se encuentra en el panel anterior del chasis y se comparte entre todos los servidores Blade.</p> <p>Para restablecer iDRAC sin reiniciar el servidor, mantenga presionado el botón Identificación del sistema  durante 16 segundos.</p>
Interfaz web del CMC	<p>Además de supervisar y administrar el chasis, utilice la interfaz web de CMC para realizar lo siguiente:</p> <ul style="list-style-type: none"> • Ver el estado de un sistema administrado • Actualizar el firmware del iDRAC • Establecer la configuración de red de iDRAC • Iniciar sesión en la interfaz web de iDRAC • Iniciar, detener o restablecer el sistema administrado

Interfaz o protocolo	Descripción
Lifecycle Controller	<ul style="list-style-type: none"> • Actualizar el BIOS, PERC y otros adaptadores de red compatibles <p>Utilice Lifecycle Controller para realizar las configuraciones de iDRAC. Para acceder a Lifecycle Controller, presione <F10> durante el inicio y vaya a Configuración del sistema → Configuración avanzada de hardware → Configuración de iDRAC. Para obtener más información, consulte <i>Lifecycle Controller User's Guide</i> (Guía del usuario de Dell Lifecycle Controller), disponible en dell.com/support/manuals.</p>
Telnet	<p>Utilice Telnet para acceder a iDRAC, donde puede ejecutar comandos RACADM y SMCLP. Para obtener información detallada acerca de RACADM, consulte <i>iDRAC8 RACADM Command Line Interface Reference Guide</i> (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8), disponible en dell.com/support/manuals. Para obtener información acerca de SMCLP, consulte Uso de SMCLP.</p> <p> NOTA: Telnet no es un protocolo seguro y está desactivado de manera predeterminada. Telnet transmite todos los datos, incluidas las contraseñas, en texto sin formato. Al transmitir información confidencial, utilice la interfaz SSH.</p>
SSH	<p>Utilice SSH para ejecutar comandos RACADM y SMCLP. SSH proporciona las mismas capacidades que la consola Telnet, pero utiliza una capa de transporte cifrado para mayor seguridad. En iDRAC, el servicio SSH está activado de manera predeterminada pero se puede desactivar. iDRAC solo admite SSH versión 2 con DSA y el algoritmo de clave de host RSA. Al encender iDRAC por primera vez, se genera una clave de host única DSA de 1024 bits y RDA de 1024 bits.</p>
IPMITool	<p>Utilice IPMITool para acceder a las funciones de administración básicas del sistema remoto a través de iDRAC. La interfaz incluye IPMI local, IPMI en la LAN, IPMI en comunicación en serie y comunicación en serie en la LAN. Para obtener más información acerca de IPMITool, consulte <i>Dell OpenManage Baseboard Management Controller Utilities User's Guide</i> (Guía del usuario de las utilidades de la controladora de administración de la placa base de Dell OpenManage), disponible en dell.com/support/manuals.</p> <p> NOTA: No se admite IPMI versión 1.5.</p>
VMCLI	<p>Utilice la interfaz de línea de comandos de medios virtuales (VMCLI) para acceder a medios virtuales a través de la estación de trabajo e implementar sistemas operativos en varios sistemas administrados.</p>
SMCLP	<p>Utilice el protocolo de línea de comandos de Server Management Workgroup (SMCLP) para realizar tareas de administración de sistemas. Esto está disponible a través de SSH o Telnet. Para obtener más información acerca de SMCLP, consulte Uso de SMCLP.</p>
WS-MAN	<p>Los servicios remotos LC se basan en el protocolo WS-Management para realizar tareas de administración de uno a varios sistemas. Debe utilizar el cliente WS-MAN como cliente WinRM (Windows) o cliente OpenWSMAN (Linux) para utilizar la funcionalidad Servicios remotos LC. También puede utilizar Power Shell y Python para crear secuencias de comandos para la interfaz WS-MAN.</p>

Interfaz o protocolo	Descripción
	<p>Web Services for Management (WS-Management) es un protocolo basado en SOAP que se utiliza para la administración de sistemas. iDRAC utiliza WS-Management para transmitir información de administración basada en el modelo común de información (CIM) de Distributed Management Task Force (DMTF). La información CIM define la semántica y los tipos de información que se pueden modificar en un sistema administrado. Los datos disponibles a través de WS-Management los proporciona la interfaz de instrumentación de iDRAC asignada a los perfiles DMTF y de extensión.</p> <p>Para obtener más información, consulte lo siguiente:</p> <ul style="list-style-type: none"> • Lifecycle Controller-Remote Services User's Guide (Guía del usuario de Lifecycle Controller Remote Services) disponible en dell.com/support/manuals. • Lifecycle Controller Integration Best Practices Guide (Guía de prácticas recomendadas para la integración de Lifecycle Controller) disponible en dell.com/support/manuals. • Página de Lifecycle Controller en Dell TechCenter: delltechcenter.com/page/Lifecycle+Controller • Centro de secuencias de comandos de Lifecycle Controller WS-Management: delltechcenter.com/page/Scripting+the+Dell+Lifecycle+Controller • MOF y perfiles: delltechcenter.com/page/DCIM.Library • Sitio web de DMTF: dmtf.org/standards/profiles/

Información sobre puertos iDRAC

Se requieren los siguientes puertos para acceder a iDRAC de forma remota por medio de firewalls. Estos son los puertos predeterminados que iDRAC utiliza en espera para las conexiones. De manera opcional, puede modificar la mayoría de los puertos. Para hacerlo, consulte [Configuración de servicios](#).

Tabla 3. Puertos que iDRAC utiliza en espera para las conexiones

Número de puerto	Función
22*	SSH
23*	Telnet
80*	HTTP
443*	HTTPS
623	RMCP/RMCP+
161*	SNMP
5900*	Teclado y redireccionamiento del mouse de la consola virtual, Medios virtuales, Carpetas virtuales y Uso compartido de archivos remotos
5901	VNC
	Cuando la función de VNC está activada, se abre el puerto 5901.

Número de puerto	Función
------------------	---------

* Puerto configurable

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

Tabla 4. Puertos que iDRAC utiliza como cliente

Número de puerto	Función
25*	SMTP
53	DNS
68	Dirección IP asignada por DHCP
69	TFTP
162*	Captura SNMP
445	Common Internet File System (Sistema de archivos de Internet común - CIFS)
636	LDAP sobre SSL (LDAPS)
2049	Network File System (Sistema de archivos de red - NFS)
123	Protocolo de hora de red (NTP)
3269	LDAPS para catálogo global (GC)

* Puerto configurable

Otros documentos que podrían ser de utilidad

Además de esta guía, los siguientes documentos que están 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 de iDRAC en su sistema.

- En la *Ayuda en línea de iDRAC* se proporciona información acerca de los campos disponibles en la interfaz web de iDRAC y sus descripciones. Puede acceder a la ayuda en línea después de instalar iDRAC.
- En *iDRAC8 RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8) se proporciona información acerca de los subcomandos RACADM, las interfaces admitidas y los grupos de bases de datos de propiedades y las definiciones de objetos de iDRAC.
- La *Tabla de compatibilidades de RACADM para iDRAC* incluye la lista de comandos y objetos que son aplicables para una determinada versión de iDRAC.
- En la *Systems Management Overview Guide* (Guía de información general de Systems Management) se proporciona información acerca de los distintos programas de software disponibles para realizar tareas de administración de sistemas.
- En *Dell Lifecycle Controller Graphical User Interface For 13th Generation Dell PowerEdge Servers User's Guide* (Guía del usuario de la interfaz gráfica de usuario de Dell Lifecycle Controller para

servidores Dell PowerEdge de 13.ª generación) se proporciona información sobre el uso de la interfaz gráfica de usuario (GUI) de Lifecycle Controller.

- En *Dell Lifecycle Controller Remote Services For 13th Generation Dell PowerEdge Servers Quick Start Guide* (Guía de inicio rápido de servicios remotos de Dell Lifecycle Controller para servidores Dell PowerEdge de 13.ª generación) se brinda una descripción general de las capacidades de los servicios remotos, información sobre cómo empezar a trabajar con los servicios remotos, API de Lifecycle Controller y referencias a varios recursos en Dell Tech Center.
- *Dell Remote Access Configurarlos Tool User's Guide* (Guía del usuario de la herramienta de configuración de Dell Remote Access) proporciona información sobre cómo utilizar la herramienta para descubrir las direcciones IP de iDRAC en la red, realizar actualizaciones del firmware de uno a varios y activar la configuración del directorio para las direcciones IP descubiertas.
- La *Matriz de compatibilidad de software de los 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.
- *iDRAC Service Module Installation Guide* (Guía de instalación del módulo de servicio del iDRAC) proporciona información para instalar el módulo de servicio del iDRAC.
- En la *Guía de instalación de Dell OpenManage Server Administrator* se incluyen instrucciones para ayudar a instalar Dell OpenManage Server Administrator.
- En la *Guía de instalación de Dell OpenManage Management Station Software* se incluyen instrucciones para ayudar a instalar este software que incluye la utilidad de administración de la placa base, herramientas de DRAC y el complemento de Active Directory.
- En la *Dell OpenManage Baseboard Management Controller Management Utilities User's Guide* (Guía del usuarios de las utilidades de administración de OpenManage Baseboard Management Controller) se incluye información acerca de la interfaz IPMI.
- Las *Notas de publicación* proporcionan actualizaciones de última hora relativas al sistema o a la documentación o material avanzado de consulta técnica destinado a técnicos o usuarios experimentados.
- En el *Glossary* (Glosario) se proporciona información acerca de los términos utilizados en este documento.

Están disponibles los siguientes documentos para proporcionar más información:

- En *iDRAC Overview and Feature Guide* (Guía de información general y funciones de iDRAC) se proporciona información sobre iDRAC, sus funciones sujetas a licencia y las opciones de actualización de licencias.
- Las instrucciones de seguridad incluidas con el sistema proporcionan información importante sobre la seguridad y las normativas. Para obtener más información sobre las normativas, consulte la página de inicio de cumplimiento normativo en dell.com/remotoconfiguración. Es posible que se incluya información de garantía en este documento o en un documento separado.
- En la *Guía de instalación en bastidor* incluida con la solución de bastidor se describe cómo instalar el sistema en un bastidor.
- En la *Guía de introducción* se ofrece una visión general sobre las funciones, la configuración y las especificaciones técnicas del sistema.
- El *Manual del propietario* proporciona información sobre las funciones del sistema y describe cómo solucionar problemas del sistema e instalar o sustituir componentes del sistema.

Enlaces relacionados

[Cómo ponerse en contacto con Dell](#)

[Acceso a documentos desde el sitio de asistencia de Dell](#)


Referencia de medios sociales

Para conocer más sobre el producto y las mejoras prácticas y obtener información sobre las soluciones y los servicios Dell, puede acceder a las plataformas de medios sociales tales como Dell TechCenter.

Puede acceder a blogs, foros, documentos, videos explicativos, etc. desde la página wiki del iDRAC en www.delltechcenter.com/idrac.

Para consultar documentos del iDRAC y otro firmware relacionado, visite www.dell.com/esmmanuals.

Cómo ponerse en contacto con Dell

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

Dell proporciona varias opciones de servicio y asistencia en línea o telefónica. Puesto que la disponibilidad varía en función del país y del producto, es posible que no pueda disponer de algunos servicios en su área. Si desea ponerse en contacto con Dell para tratar cuestiones relacionadas con las ventas, la asistencia técnica o el servicio de atención al cliente:

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

Acceso a documentos desde el sitio de asistencia de Dell


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

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

- Mediante los motores de búsqueda:
 - Escriba el nombre y la versión del documento en el cuadro buscar.

Inicio de sesión en iDRAC

Puede iniciar sesión en iDRAC como usuario de iDRAC, como usuario de Microsoft Active Directory o como usuario de protocolo ligero de acceso a directorios (LDAP). El nombre de usuario predeterminado y la contraseña correspondiente son root y calvin, respectivamente. También puede iniciar sesión mediante el inicio de sesión único (SSO) o tarjeta inteligente.

 **NOTA:** Debe disponer del privilegio Iniciar sesión en iDRAC para poder iniciar sesión en iDRAC.

Enlaces relacionados

[Inicio de sesión en iDRAC como usuario local de Active Directory o usuario LDAP](#)


[Inicio de sesión en iDRAC mediante una tarjeta inteligente](#)


[Inicio de sesión en iDRAC mediante inicio de sesión único](#)

[Cambio de la contraseña de inicio de sesión predeterminada](#)

Inicio de sesión en iDRAC como usuario local de Active Directory o usuario LDAP


Antes de iniciar sesión en iDRAC mediante la interfaz web, asegúrese de haber configurado un explorador web compatible y de haber creado una cuenta de usuario con los privilegios necesarios.

 **NOTA:** El nombre de usuario *no* distingue mayúsculas y minúsculas para un usuario de Active Directory. La contraseña distingue mayúsculas y minúsculas para todos los usuarios.

 **NOTA:** Además de Active Directory, se admiten servicios de directorio basados en openLDAP, openDS, Novell eDir y Fedora.

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

1. Abra un explorador de web compatible.
2. En el campo **Dirección**, escriba `https://[iDRAC-IP-address]` y presione <Intro>.

 **NOTA:** Si se ha modificado el número de puerto HTTPS predeterminado (puerto 443), ingrese: `https://[iDRAC-IP-address]:[port-number]`, donde `[iDRAC-IP-address]` es la dirección IPv4 o IPv6 de iDRAC y `[port-number]` es el número de puerto HTTPS.

Se muestra la página **Inicio de sesión**.

3. Para un usuario local:
 - En los campos **Nombre de usuario** y **Contraseña**, introduzca el nombre de usuario y la contraseña de iDRAC.
 - En el menú desplegable **Dominio**, seleccione **Este iDRAC**.
4. Para un usuario de Active Directory, en los campos **Nombre de usuario** y **Contraseña**, introduzca el nombre de usuario y la contraseña de Active Directory. Si ha especificado el nombre de dominio como parte del nombre de usuario, seleccione **Este iDRAC** en el menú desplegable. El formato del nombre de usuario puede ser el siguiente: `<dominio>\<nombre de usuario>`, `<dominio>/<nombre de usuario>` o `<usuario>@<dominio>`.

Por ejemplo, dell.com\john_doe, o JOHN_DOE@DELL.COM.

Si el dominio no se especifica en el nombre de usuario, seleccione el dominio de Active Directory en el menú desplegable **Dominio**.

5. Para un usuario LDAP, en los campos **Nombre de usuario** y **Contraseña**, introduzca el nombre de usuario y la contraseña LDAP. Para el inicio de sesión no se necesita el dominio. De manera predeterminada, **Este iDRAC** está seleccionado en el menú desplegable.
6. Haga clic en **Enviar**. Ha iniciado sesión en iDRAC con los privilegios de usuario necesarios. Si inicia sesión con el privilegio de configuración de usuarios y las credenciales predeterminadas de la cuenta, y si está activada la función de advertencia de contraseña predeterminada, aparecerá la página **Advertencia de contraseña predeterminada** donde puede cambiar fácilmente la contraseña.

Enlaces relacionados

- [Configuración de cuentas de usuario y privilegios](#)
- [Cambio de la contraseña de inicio de sesión predeterminada](#)
- [Configuración de exploradores web compatibles](#)

Inicio de sesión en iDRAC mediante una tarjeta inteligente

Puede iniciar sesión en iDRAC mediante una tarjeta inteligente. Las tarjetas inteligentes proporcionan una autenticación de factor doble (TFA) y ofrecen dos niveles de seguridad:

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

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

Enlaces relacionados


- [Inicio de sesión en iDRAC como usuario local mediante una tarjeta inteligente](#)
- [Inicio de sesión en iDRAC como usuario de Active Directory mediante una tarjeta inteligente](#)

Inicio de sesión en iDRAC como usuario local mediante una tarjeta inteligente

Antes de iniciar sesión como usuario local mediante una tarjeta inteligente, asegúrese de hacer lo siguiente:


- Cargar el certificado de tarjeta inteligente del usuario y el certificado de CA de confianza en iDRAC
- Activar el inicio de sesión mediante tarjeta inteligente.

La interfaz web de iDRAC muestra la página de Inicio de sesión mediante tarjeta inteligente de todos los usuarios que fueron configurados para usar la tarjeta inteligente.


 **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.

Para iniciar sesión en iDRAC como usuario local mediante una tarjeta inteligente:

1. Acceda a la interfaz web de iDRAC mediante el vínculo `https://[IP address]`. Aparece la página **Inicio de sesión de iDRAC** en la que se le solicita insertar la tarjeta inteligente.

 **NOTA:** Si el número de puerto HTTPS predeterminado (puerto 443) se ha modificado, escriba: `https://[IP address]:[port number]`, donde `[IP address]` es la dirección IP de DRAC y `[port number]` es el número de puerto HTTPS.

2. Inserte la tarjeta inteligente en el lector y haga clic en **Iniciar sesión**.
Se muestra una petición para el PIN de la tarjeta inteligente. No es necesario especificar una contraseña.
3. Introduzca el PIN para los usuarios de tarjeta inteligente.
Ahora está conectado a iDRAC.

 **NOTA:** Si se trata de un usuario local para el que está activada la opción **Activar la revisión CRL para el inicio de sesión mediante tarjeta inteligente**, iDRAC intenta descargar la CRL y la comprueba en búsqueda del certificado del usuario. El inicio de sesión falla si el certificado se indica como revocado en la CRL o si la CRL no puede descargarse por algún motivo.

Enlaces relacionados

[Activación o desactivación del inicio de sesión mediante tarjeta inteligente](#)

[Configuración del inicio de sesión mediante tarjeta inteligente de iDRAC para usuarios locales](#)


Inicio de sesión en iDRAC como usuario de Active Directory mediante una tarjeta inteligente

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

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

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

1. Inicie sesión en iDRAC mediante el vínculo `https://[IP address]`.
Aparece la página **Inicio de sesión de iDRAC** en la que se le solicita insertar la tarjeta inteligente.

 **NOTA:** Si el número de puerto HTTPS predeterminado (puerto 443) se ha modificado, escriba: `https://[IP address]:[port number]` donde, `[IP address]` es la dirección IP de DRAC y `[port number]` es el número de puerto HTTPS.

2. Inserte la tarjeta inteligente y haga clic en **Iniciar sesión**.
Aparece la página **PIN**.
3. Introduzca el PIN y haga clic en **Enviar**.
Ha iniciado sesión en iDRAC con sus credenciales de Active Directory.

 **NOTA:**

Si el usuario de la tarjeta inteligente está presente en Active Directory, no es necesario introducir una contraseña de Active Directory.

Enlaces relacionados

[Activación o desactivación del inicio de sesión mediante tarjeta inteligente](#)

[Configuración del inicio de sesión mediante tarjeta inteligente de iDRAC para usuarios de Active Directory](#)

Inicio de sesión en iDRAC mediante inicio de sesión único

Cuando está activado el inicio de sesión único (SSO), puede iniciar sesión en iDRAC sin introducir las credenciales de autenticación de usuario del dominio, como nombre de usuario y contraseña.

Enlaces relacionados

[Configuración del inicio de sesión SSO de iDRAC para usuarios de Active Directory](#)


Inicio de sesión SSO de iDRAC mediante la interfaz web de iDRAC

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

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

Para iniciar sesión en iDRAC mediante la interfaz web:

1. Inicie sesión en la estación de administración mediante una cuenta de Active Directory válida.
2. En un explorador web, escriba `https://[FQDN address]`

 **NOTA:** Si el número de puerto HTTPS predeterminado (puerto 443) se ha modificado, escriba: `https://[FQDN address]:[port number]` donde, `[FQDN address]` es el nombre iDRAC FQDN (`iDRACdnsname.domain.name`) y `[port number]` es el número de puerto HTTPS.

 **NOTA:** Si usa la dirección IP en lugar de FQDN, falla SSO.

Iniciará sesión en iDRAC con los privilegios adecuados de Microsoft Active Directory y las credenciales almacenadas en la caché del sistema operativo en el momento de iniciar sesión con una cuenta de Active Directory válida.

Inicio de sesión SSO de iDRAC mediante la interfaz web de CMC

Mediante la función SSO, puede iniciar la interfaz web de iDRAC desde la interfaz web de CMC. Un usuario de CMC tiene los privilegios de usuario de CMC al iniciar iDRAC desde CMC. Si la cuenta de usuario está presente en CMC y no en iDRAC, el usuario aún puede iniciar iDRAC desde CMC.

Si se desactiva la LAN de la red de iDRAC (LAN activada = No), SSO no estará disponible.

Si el servidor se quita del chasis, se cambia la dirección IP de iDRAC o hay un problema en la conexión de red de iDRAC, la opción para iniciar iDRAC estará desactivada en la interfaz web de CMC.


Para obtener más información, consulte *Chassis Management Controller User's Guide* (Guía del usuario de Chassis Management Controller) disponible en dell.com/support/manuals.

Acceso a iDRAC mediante RACADM remoto

Puede utilizar RACADM para acceder a iDRAC mediante la utilidad de configuración de RACADM.

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

Si la estación de trabajo no almacena el certificado SSL de iDRAC en su dispositivo de almacenamiento predeterminado, aparecerá un mensaje de advertencia al ejecutar el comando RACADM. No obstante, el comando se ejecuta correctamente.

 **NOTA:** El certificado de iDRAC es el que iDRAC envía al cliente RACADM para establecer la sesión segura. Este certificado lo emite la CA o es autofirmado. En cualquiera de los casos, si la estación de trabajo no reconoce la CA o la autoridad firmante, aparecerá un aviso.

Enlaces relacionados

[Validación del certificado de CA para usar RACADM remoto en Linux](#)

Validación del certificado de CA para usar RACADM remoto en Linux

Antes de ejecutar los comandos de RACADM remoto, valide el certificado de CA que se utiliza para las comunicaciones seguras.

Para validar el certificado para usar RACADM remoto:

1. Convierta el certificado en formato DER al formato PEM (mediante la herramienta de línea de comandos openssl):

```
openssl x509 -inform pem -in [yourdownloadedderformatcert.crt] -outform pem -out [outcertfileinpemformat.pem] -text
```
2. Busque la ubicación del conjunto de certificados de CA predeterminados en la estación de administración. Por ejemplo, para RHEL5 de 64 bits es **/etc/pki/tls/cert.pem**.
3. Agregue el certificado CA con formato PEM al certificado CA de la estación de administración. Por ejemplo, utilice el comando `cat` command: `- cat testcacert.pem >> cert.pem`
4. Genere y cargue el certificado de servidor en iDRAC.

Acceso a iDRAC mediante RACADM local

Para obtener información sobre la forma de acceder a iDRAC mediante RACADM local, consulte *iDRAC8 RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8), disponible en dell.com/support/manuals.

Acceso a iDRAC mediante RACADM de firmware

Puede utilizar las interfaces SSH o Telnet para acceder a iDRAC y ejecutar el firmware de RACADM. Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8), disponible en dell.com/support/manuals.

Acceso a iDRAC mediante SMCLP

SMCLP es el símbolo del sistema de línea de comandos predeterminado cuando inicia sesión en iDRAC mediante Telnet o SSH. Para obtener más información, consulte [Uso de SMCLP](#).

Inicio de sesión en iDRAC mediante la autenticación de clave pública

Puede iniciar sesión en iDRAC a través de SSH sin introducir ninguna contraseña. También puede enviar un único comando RACADM como un argumento de línea de comandos a la aplicación SSH. Las opciones de línea de comandos tienen un comportamiento similar a las de RACADM remoto, ya que la sesión termina una vez completado el comando.

Por ejemplo:

Inicio de sesión:

```
ssh username@<domain>
```

o

```
ssh username@<IP_address>
```

donde IP_address es la dirección IP de iDRAC.

Envío de comandos RACADM:

```
ssh username@<domain> racadm getversion
```

```
ssh username@<domain> racadm getsel
```

Enlaces relacionados

[Uso de la autenticación de clave pública para SSH](#)

Varias sesiones iDRAC

En la tabla siguiente se proporciona la lista de varias sesiones iDRAC posibles mediante las distintas interfaces.

Tabla 5. Varias sesiones iDRAC

Interfaz	Número de sesiones
Interfaz web del iDRAC	6
RACADM remoto	4
Firmware RACADM / SMCLP	SSH - 2 Telnet - 2 Serie - 1

Cambio de la contraseña de inicio de sesión predeterminada

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

- Inicia sesión en iDRAC con el privilegio Configurar usuario.
- Está activada la función de advertencia de contraseña predeterminada.
- Las credenciales para las cuentas actualmente configuradas son root/calvin.

También aparecerá un mensaje de advertencia al iniciar sesión en iDRAC con SSH, Telnet, RACADM remoto o la interfaz web. Para la interfaz web, SSH y Telnet, aparecerá un único mensaje de advertencia se muestra para cada sesión. Para RACADM remoto, el mensaje de advertencia aparecerá para cada comando.

Enlaces relacionados

[Activación o desactivación del mensaje de advertencia de contraseña predeterminada](#)

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

Cuando se conecta a la interfaz web de iDRAC, si aparece la página **Advertencia de contraseña predeterminada**, puede cambiar la contraseña. Para hacerlo, siga estos pasos:

1. Seleccione la opción **Cambiar contraseña predeterminada**.
2. En el campo **Contraseña nueva**, introduzca la contraseña nueva.
La cantidad máxima de caracteres para la contraseña es 20. Los caracteres están enmascarados. Se admiten los siguientes caracteres:
 - 0-9
 - A-Z
 - a-z
 - Caracteres especiales: +, &, ?, >, -, }, |, ,, !, (, ', ,, _[, ", @, #,), *, ;, \$,], /, \, %, =, <, :, {, |, \
3. En el campo **Confirmar contraseña**, introduzca nuevamente la contraseña.
4. Haga clic en **Continuar**. Se configura la contraseña nueva y queda conectado a iDRAC.



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

Para obtener información acerca de otros campos, consulte la *Ayuda en línea de iDRAC*.

Cambio de la contraseña de inicio de sesión predeterminada mediante RACADM

Para cambiar la contraseña, ejecute el siguiente comando RACADM:

```
racadm set iDRAC.Users.<index>.Password <Password>
```

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

Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8).

Cambio de la contraseña de inicio de sesión predeterminada mediante la utilidad de configuración de iDRAC

Para cambiar la contraseña de inicio de sesión predeterminada mediante la utilidad de configuración de iDRAC:

1. En la utilidad de configuración de iDRAC, vaya a **Configuración de usuario**.
Se muestra la página **Configuración de iDRAC - Configuración de usuario**.
2. En el campo **Cambiar contraseña**, introduzca la contraseña nueva.
3. Haga clic en **Atrás**, en **Terminar** y, a continuación, en **Sí**.
Los detalles se guardan.

Activación o desactivación del mensaje de advertencia de contraseña predeterminada

Es posible activar o desactivar el mensaje de advertencia de contraseña predeterminada. Para hacerlo, se debe contar con el privilegio de configuración de usuarios.

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

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

1. Vaya a **Descripción general** → **Configuración de iDRAC** → **Autenticación de usuarios** → **Usuarios locales**.

Se muestra la página **Users (Usuarios)**.

2. En la sección **Advertencia de contraseña predeterminada**, seleccione **Activar** y, a continuación, haga clic en **Aplicar** para activar la visualización de la página **Advertencia de contraseña predeterminada** al iniciar sesión en iDRAC. De lo contrario, seleccione **Desactivar**.


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

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

Para activar la visualización del mensaje de advertencia a fin de cambiar la contraseña de inicio de sesión predeterminada mediante RACADM, utilice el objeto `idrac.tuning.DefaultCredentialWarning`. Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8)*, disponible en dell.com/support/manuals.

Configuración de Managed System y Management Station

Para realizar administración de sistemas fuera de banda mediante iDRAC, debe configurar iDRAC para acceso remoto, configurar la estación de administración y el sistema administrado, y configurar los exploradores web compatibles.

 **NOTA:** En el caso de servidores Blade, instale los módulos de CMC y de E/S en el chasis e instale físicamente el sistema en el chasis antes de realizar las configuraciones.

iDRAC Express e iDRAC Enterprise se envían de fábrica con una dirección IP estática predeterminada. Sin embargo, Dell también ofrece dos opciones: detección automática, que le permite acceder al iDRAC y configurar su servidor en forma remota y DHCP:

- **Detección automática:** Utilice esta opción si tiene un servidor de aprovisionamiento instalado en el entorno del centro de datos. El servidor de aprovisionamiento administra y automatiza la implementación o actualización de un sistema operativo y aplicaciones a un servidor Dell PowerEdge. Si activa la detección automática, los servidores, luego del primer inicio, buscan un servidor de aprovisionamiento para controlar y comenzar el proceso de implementación o actualización automatizada.
- **DHCP:** utilice esta opción si tiene un servidor de protocolo de configuración dinámica de host (DHCP) instalado en el entorno del centro de datos. El servidor DHCP asigna automáticamente la dirección IP, la puerta de enlace y la máscara de subred para iDRAC.

Para activar Detección automática o DHCP coloque una orden en el servidor. Activar cualquiera de estas funciones no tiene costo. Solo es posible una configuración.

Enlaces relacionados

[Configuración de la dirección IP de iDRAC](#)

[Configuración de Managed System](#)

[Actualización del firmware de dispositivos](#)

[Reversión del firmware del dispositivo](#)

[Configuración de Management Station](#)

[Configuración de exploradores web compatibles](#)

Configuración de la dirección IP de iDRAC

Debe configurar las opciones de red iniciales en función de la infraestructura de red para activar la comunicación entrante y saliente con iDRAC. Puede configurar la dirección IP mediante una de las siguientes interfaces:

- Utilidad Configuración de iDRAC
- Lifecycle Controller (consulte la *Lifecycle Controller User's Guide* (Guía del usuario de Dell Lifecycle Controller))

- Dell Deployment Toolkit (consulte *Dell Deployment Toolkit User's Guide* (Guía del usuario de Dell Deployment Toolkit))
- Panel LCD del chasis o servidor (consulte el *Manual de propietario del hardware* del sistema)
 - ✎ **NOTA:** En el caso de los servidores blade, puede configurar las opciones de red mediante el panel LCD de chasis solo durante la configuración inicial de CMC. Una vez implementado el chasis, no es posible reconfigurar iDRAC mediante el panel LCD del chasis.
- Interfaz web de CMC (consulte la *Dell Chassis Management Controller Firmware User's Guide* (Guía del usuario del firmware de Dell Chassis Management Controller))

En el caso de los servidores tipo bastidor y torre, puede configurar la dirección IP o utilizar la dirección IP predeterminada de iDRAC (192.168.0.120) para configurar las opciones de red iniciales, incluida la configuración de DHCP o la dirección IP estática para iDRAC.

En el caso de los servidores blade, la interfaz de red de iDRAC está desactivada de manera predeterminada.

Después de configurar la dirección IP de iDRAC:

- Asegúrese de *cambiar el nombre de usuario y la contraseña predeterminados después de configurar la dirección IP de iDRAC.*
- Obtenga acceso a ella a través de cualquiera de las interfaces siguientes:
 - Interfaz web de iDRAC mediante un explorador compatible (Internet Explorer, Firefox, Chrome o Safari)
 - Shell seguro (SSH): requiere un cliente, tal como PuTTY en Windows. SSH está disponible de forma predeterminada en la mayoría de los sistemas Linux y, por tanto, no requiere cliente.
 - Telnet (debe estar activado, ya que esta desactivado de manera predeterminada).
 - IPMITool (utiliza el comando IPMI) o solicitud shell (requiere un instalador personalizado de Dell en Windows o Linux, disponible en el DVD *Documentación y herramientas de Systems Management* o dell.com/support).

Enlaces relacionados

[Configuración de la IP de iDRAC mediante la utilidad de configuración de iDRAC](#)

[Configuración de la IP de iDRAC mediante la interfaz web de CMC](#)

[Activación del descubrimiento automático](#)

[Configuración de servidores y componentes del servidor mediante la configuración automática](#)

Configuración de la IP de iDRAC mediante la utilidad de configuración de iDRAC

Para configurar la dirección IP de iDRAC:

1. Encienda el sistema administrado.
2. Presione <F2> durante la Power-on Self-test (Autoprueba de encendido - POST).
3. En la página **System Setup Main Menu (Menú principal de Configuración del sistema)**, haga clic en **iDRAC Settings (Configuración de iDRAC)**.
Aparece la página **Configuración de iDRAC**.
4. Haga clic en **Red**.
Aparecerá la página **Red**.
5. Especifique los valores siguientes:
 - Configuración de red


- Configuración común
 - Configuración de IPv4
 - Configuración de IPv6
 - Configuración de IPMI
 - Configuración de VLAN
6. Haga clic en **Atrás**, en **Terminar** y, a continuación, en **Sí**.
Se guarda la información de red y el sistema se reinicia.

Enlaces relacionados

- [Configuración de red](#)
- [Configuración común](#)
- [Configuración de IPv4](#)
- [Configuración de IPv6](#)
- [Configuración de IPMI](#)
- [Configuración de VLAN](#)

Configuración de red

Para configurar la configuración de red:


 **NOTA:** Para obtener información acerca de las opciones, consulte la *Ayuda en línea de la utilidad de configuración de iDRAC*.

1. En **Activar la NIC**, seleccione la opción **Activado**.
2. En el menú desplegable **Selección de NIC**, seleccione uno de los puertos siguientes en función de los requisitos de red:
 - **Dedicado:** permite al dispositivo de acceso remoto utilizar la interfaz de red dedicada disponible en Remote Access Controller (RAC). Esta interfaz no se comparte con el sistema operativo de host y enruta el tráfico de administración a una red física separada, lo que permite separarla del tráfico de la aplicación.


Esta opción implica que el puerto de red dedicado de iDRAC enruta su tráfico de manera independiente desde los puertos LOM o NIC del servidor. En relación con la administración del tráfico de red, la opción **Dedicado** permite al iDRAC recibir una dirección IP desde la misma subred o una subred diferente en comparación con las direcciones IP asignadas a los LOM o NIC de host.

 **NOTA:** La opción está disponible solamente en sistemas tipo bastidor o torre.

- LOM1
- LOM2
- LOM3
- LOM4


 **NOTA:** En el caso de los servidores tipo bastidor y torre, hay dos opciones LOM (LOM1 y LOM2) o las cuatro opciones LOM están disponibles en función del modelo del servidor. Los servidores blade no utilizan LOM para la comunicación con iDRAC.

3. En el menú desplegable **Red de protección contra fallas**, seleccione uno de los LOM restantes. Si falla una red, el tráfico se enruta a través de la red de protección contra fallas.

 **NOTA:** Si ha seleccionado **Dedicado** en el menú desplegable **Selección de NIC**, la opción está desactivada.

Por ejemplo, para enrutar el tráfico de red de iDRAC a través de LOM2 cuando LOM1 está fuera de servicio, seleccione **LOM1** para **Selección de NIC** y **LOM2** para **Red de protección contra fallas**.

4. En **Negociación automática**, seleccione **Activado** si iDRAC debe configurar automáticamente el modo dúplex y la velocidad de la red. Esta opción está disponible solamente para el modo dedicado. Si está activada, iDRAC establece la velocidad de la red en 10, 100 o 1000 Mbps en función de la velocidad de la red.
5. Bajo **Velocidad de la red**, seleccione 10 Mbps o 100 Mbps.

 **NOTA:** No es posible configurar manualmente la velocidad de la red en 1000 Mbps. Esta opción solo está disponible si la opción **Negociación automática** está activada.

6. Bajo **Modo dúplex**, seleccione la opción **Dúplex medio** o **Dúplex completo**.

 **NOTA:** Si activa **Negociación automática**, esta opción estará desactivada.

Configuración común

Si la infraestructura de red tiene un servidor DNS, registre iDRAC en el servidor. Estos son los requisitos de configuración inicial para las funciones avanzadas, como los servicios de directorio Active Directory o LDAP, inicio de sesión único y tarjeta inteligente.

Para registrar iDRAC:

1. Active la opción **Registrar DRAC en DNS**.
2. Introduzca el **Nombre DNS del DRAC**.
3. Seleccione **Configuración automática de nombre de dominio** para adquirir automáticamente el nombre de dominio de DHCP. De lo contrario, proporcione el **Nombre de dominio de DNS**.

Configuración de IPv4

Para configurar los valores de IPv4:

1. Seleccione la opción **Activado** en **Activar IPv4**.
2. Seleccione la opción **Activado** en **Activar DHCP** de modo que DHCP pueda asignar automáticamente la dirección IP, la puerta de enlace y la máscara de subred en iDRAC. De lo contrario, seleccione **Desactivado** e ingrese los valores para las siguientes opciones:
 - Dirección IP estática
 - Puerta de enlace estática
 - Máscara de subred estática
3. De manera opcional, active **Usar DHCP para obtener direcciones de servidor DNS**, de modo que el servidor DHCP pueda asignar los valores **Servidor DNS preferido estático** y **Servidor DNS alternativo estático**. De lo contrario, introduzca las direcciones IP en los cuadros **Servidor DNS preferido estático** y **Servidor DNS alternativo estático**.

Configuración de IPv6

De forma alternativa, en función de la configuración de la infraestructura, puede utilizar el protocolo de direcciones IPv6.

Para configurar los valores IPv6:

1. Seleccione la opción **Activado** en **Activar IPv6**.
2. Para que el servidor DHCPv6 asigne automáticamente la dirección IP, la puerta de enlace y la máscara de subred en iDRAC, seleccione la opción **Activado** en **Activar configuración automática**. Si se activa, los valores estáticos se desactivarán. De lo contrario, vaya al paso siguiente para llevar a cabo la configuración con la dirección IP estática.

3. En el cuadro **Dirección IP estática 1**, introduzca la dirección IPv6 estática.
4. En el cuadro **Longitud de prefijo estático**, introduzca un valor entre 0 y 128.
5. En el cuadro **Puerta de enlace estática**, introduzca la dirección de la puerta de enlace.
6. Si utiliza DHCP, active la opción **DHCPv6 para obtener direcciones de servidor DNS** con el fin de obtener las direcciones primaria y secundaria de servidor DNS del servidor DHCPv6. De lo contrario, seleccione **Desactivado** y haga lo siguiente:
 - En el cuadro **Servidor DNS preferido estático**, introduzca la dirección IPv6 del servidor DNS.
 - En el cuadro **Servidor DNS alternativo estático**, introduzca el servidor DNS alternativo estático.

Configuración de IPMI

Para configurar los valores de IPMI:

1. Bajo **Activar IPMI en la LAN**, seleccione **Activado**.
2. En **Límite de privilegio de canal**, seleccione **Administrador**, **Operador** o **Usuario**.
3. En el cuadro **Clave de cifrado**, introduzca la clave de cifrado en el formato de 0 a 40 caracteres hexadecimales (sin caracteres en blanco). El valor predeterminado es todo ceros.

Configuración de VLAN

Puede configurar iDRAC en la infraestructura de la VLAN. Para configurar los valores de la VLAN:

1. En **Activar identificación de VLAN**, seleccione **Activado**.
2. En el cuadro **Identificación de VLAN**, introduzca un número válido de 1 a 4094.
3. En el cuadro **Prioridad**, introduzca un número de cuadro de 0 a 7 para establecer la prioridad de la identificación de VLAN.

 **NOTA:** Después de activar la VLAN, no se podrá acceder a la IP de DRAC durante un tiempo.

Configuración de la IP de iDRAC mediante la interfaz web de CMC

Para configurar la dirección IP de iDRAC mediante la interfaz web de CMC:

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

1. Inicie sesión en la interfaz web de CMC.
2. Vaya a **Información general de servidor** → **Configuración** → **iDRAC**.
Aparecerá la página **Implementar iDRAC**.
3. En **Configuración de red de iDRAC**, seleccione **Activar LAN** y otros parámetros de la red según sea necesario. Para obtener más información, consulte *CMC online help* (Ayuda en línea de CMC).
4. Para conocer valores de red adicionales específicos a cada servidor Blade, vaya a **Información general de servidor** → **<nombre del servidor>**.
Se muestra la página **Estado del servidor**.
5. Haga clic en **Iniciar iDRAC** y vaya a **Información general** → **Configuración de iDRAC** → **Red**.
6. En la página **Red**, especifique los valores de configuración siguientes:
 - Configuración de red
 - Configuración común
 - Configuración de IPv4
 - Configuración de IPv6
 - Configuración de IPMI

- Configuración de VLAN



NOTA: Para obtener más información, consulte la *Ayuda en línea de iDRAC*.

7. Para guardar la información de red, haga clic en **Aplicar**.

Para obtener más información, consulte *Chassis Management Controller User's Guide* (Guía del usuario de Chassis Management Controller) disponible en dell.com/support/manuals.

Activación del descubrimiento automático

La función de descubrimiento automático permite que los servidores recién instalados descubran automáticamente la consola de administración remota que aloja el servidor de aprovisionamiento. El *servidor de aprovisionamiento* proporciona credenciales de usuario administrativo personalizadas para iDRAC, de modo que pueda ser descubierto desde la consola de administración. Para obtener más información acerca del descubrimiento automático, consulte *Lifecycle Controller Remote Services User's Guide* (Guía del usuario de Lifecycle Controller Remote Services) disponible en dell.com/support/manuals.

El descubrimiento automático funciona con una dirección IP estática. DHCP, el servidor DNS o el nombre de host DNS predeterminado descubre el servidor de aprovisionamiento. Si se especifica un valor de DNS, la dirección IP del servidor de aprovisionamiento se recupera desde de DNS y la configuración DHCP no se necesita. Si se especifica el servidor de aprovisionamiento, el descubrimiento se omite, por lo que no se necesita ni DHCP ni DNS.

Puede activar el descubrimiento automático mediante la utilidad de configuración de iDRAC o Lifecycle Controller. Para obtener más información, consulte *Dell Lifecycle Controller Remote Services User's Guide* (Guía del usuario de Dell Lifecycle Controller Remote Services) disponible en dell.com/support/manuals.

Si la función de descubrimiento automático no está activada en el sistema enviado de fábrica, se activa la cuenta de administrador predeterminada (el nombre de usuario es root y la contraseña es calvin). Antes de activar el descubrimiento automático, asegúrese de desactivar esta cuenta de administrador. Si está activado el descubrimiento automático en Lifecycle Controller, todas las cuentas de usuario de iDRAC quedan desactivadas hasta que se *descubra* el servidor de aprovisionamiento.

Para activar el descubrimiento automático mediante la utilidad de configuración de iDRAC:

1. Encienda el sistema administrado.
2. Durante la POST, presione <F2 > y vaya a **Configuración de iDRAC** → **Activación remota**. Se muestra la página **Activación remota de la configuración de iDRAC**.
3. Active el descubrimiento automático, introduzca la dirección IP del servidor de aprovisionamiento y haga clic en **Atrás**.



NOTA: La especificación de la dirección IP del servidor de aprovisionamiento es opcional. Si no se establece, se descubre mediante la configuración de DHCP o DNS (paso 7).

4. Haga clic en **Red**. Aparece la pantalla **Red de configuración de iDRAC**.
5. Active la NIC.
6. Active IPv4.



NOTA: IPv6 no es compatible para el descubrimiento automático.

7. Active DHCP y obtenga el nombre del dominio, la dirección de servidor DNS y el nombre de dominio DNS desde DHCP.



NOTA: El paso 7 es opcional si se proporciona la dirección IP del servidor de aprovisionamiento (paso 3).

Configuración de servidores y componentes del servidor mediante la configuración automática

La función de configuración automática le permite configurar y aprovisionar todos los componentes en un servidor (por ejemplo, iDRAC, PERC y RAID) en una única operación mediante la importación automática de un archivo de configuración XML. Todos los parámetros configurables se especifican en el archivo XML. El servidor DHCP que asigna la dirección IP también proporciona los detalles del archivo XML para configurar iDRAC.

Puede crear un archivo XML basado en la etiqueta de servicio de los servidores o crear un archivo XML genérico que puede usar para configurar todos los iDRAC a los que presta servicio el servidor DHCP. Este archivo XML se almacena en una ubicación compartida (CIFS o NFS) a la que pueden acceder el servidor DHCP y los iDRAC del servidor que se está configurando. El servidor DHCP usa una opción de servidor DHCP para especificar el nombre del archivo XML, la ubicación del archivo XML y las credenciales de usuario para acceder a la ubicación del archivo.

Cuando iDRAC o CMC obtienen una dirección IP desde el servidor DHCP, se utiliza el archivo XML para configurar los dispositivos. La función de configuración automática se invoca solamente después de que iDRAC obtiene la dirección IP desde el servidor DHCP. Si no obtiene respuesta o una dirección IP del servidor DHCP, la función de configuración automática no se invoca.



NOTA:

- Puede activar la configuración automática solamente si las opciones **DHCPv4** y **Activar IPv4** están activadas.
- Las funciones de configuración automática y detección automática son mutuamente excluyentes. Debe desactivar la detección automática para que la configuración automática funcione.

Si todos los servidores Dell PowerEdge de la agrupación de servidores DHCP son del mismo tipo y número de modelo, se necesita un solo archivo xml (**config.xml**). (Este es el nombre de archivo XML predeterminado).

Puede configurar servidores individuales con distintos archivos de configuración asignados mediante de nombres de host individuales. En un entorno que tiene diferentes servidores con requisitos específicos, puede usar distintos nombres de archivo XML para distinguir cada uno de ellos. Por ejemplo, si hay dos servidores, un PowerEdge R720 y un PowerEdge R520, debe utilizar dos archivos XML, **R720-config.xml** y **R520-config.xml**.

El agente de configuración del servidor utiliza las reglas en la secuencia que se indica a continuación para determinar qué archivo XML del recurso compartido de archivos se aplica a cada iDRAC/servidor PowerEdge:

1. El nombre del archivo que se especifica en la opción 60 de DHCP.
2. **<ServiceTag> -config.xml**: si no se especifica un nombre de archivo en la opción 60 de DHCP, utilice la etiqueta de servicio del sistema para identificar de forma exclusiva el archivo de configuración XML del sistema. Por ejemplo, **<servicetag> -config.xml**
3. **<Model number> -config.xml**: si no se especifica el nombre de archivo de la opción 60 y el archivo **<ServiceTag> -config.xml** no se encuentra, utilice el número de modelo del sistema como base para el nombre del archivo de configuración XML que se va a usar. Por ejemplo, **R520-config.xml**.

4. **config.xml**: si el nombre de archivo de la opción 60 y los archivos basados en la etiqueta de servicio y el número de modelo no están disponibles, utilice el archivo predeterminado **config.xml**.

Enlaces relacionados

[Secuencia de configuración automática](#)

[Opciones de DHCP](#)

[Activación de la configuración automática mediante la interfaz web del iDRAC](#)

[Activar configuración automática mediante RACADM](#)

Secuencia de configuración automática

1. Cree o modifique el archivo XML que configura los atributos de los servidores Dell.
2. Coloque el archivo XML en una ubicación de recurso compartido a la que pueda acceder el servidor DHCP y todos los servidores Dell a los que se les ha asignado una dirección IP desde el servidor DHCP.
3. Especifique la ubicación del archivo XML en el campo proveedor-opción 43 del servidor DHCP.
4. Como parte de la adquisición de la dirección IP, el iDRAC anuncia el iDRAC del identificador de clase de proveedor. (Opción 60)
5. El servidor DHCP vincula la clase de proveedor con la opción del proveedor en el archivo **dhcpd.conf** y envía la ubicación del archivo XML y el nombre del archivo XML al iDRAC.
6. El iDRAC procesa el archivo XML y configura todos los atributos que se enumeran en el archivo

Opciones de DHCP

DHCPv4 permite transferir un gran número de parámetros definidos globalmente a los clientes DHCP. Cada parámetro se conoce como una opción de DHCP. Cada opción se identifica con una etiqueta de opción, que es un valor de 1 byte. Las etiquetas de la opción 0 y 255 se reservan para la superficie y el final de las opciones, respectivamente. Todos los demás valores están disponibles para definir opciones.

La opción 43 de DHCP se utiliza para enviar información del servidor DHCP al cliente DHCP. La opción se define como una cadena de texto. Esta cadena de texto se establece para que contenga los valores del nombre de archivo XML, la ubicación del recurso compartido y las credenciales para acceder a la ubicación. Por ejemplo,

```
option myname code 43 = text; option myname "-l 10.35.175.88://xmlfiles -f dhcpProv.xml -u root -p calvin";
```

donde, *-l* es la ubicación del recurso compartido de archivos remoto y *-f* es el nombre de archivo en la cadena junto con las credenciales para el recurso de archivos compartidos remoto. En este ejemplo, *root* y *calvin* son el nombre de usuario y la contraseña para el RFS.

La opción 60 de DHCP identifica y asocia un cliente DHCP con un proveedor en particular. Cualquier servidor DHCP configurado para realizar una acción basada en una Id. de proveedor del cliente debe tener configuradas las opción 60 y la opción 43. Con los servidores Dell PowerEdge, el iDRAC se identifica a sí mismo con la Id. de proveedor: *iDRAC*. Por lo tanto, debe agregar una 'Clase de proveedor' nueva y crear una 'opción de ámbito' en él para el 'código 60' y luego activar la opción de ámbito nueva para el servidor DHCP.

Enlaces relacionados

[Configuración de la opción 43 en Windows](#)

[Configuración de la opción 60 en Windows](#)

[Configuración de la opción 43 y la opción 60 en Linux](#)

Configuración de la opción 43 en Windows

Para configurar la opción 43 en Windows:

1. En el servidor DHCP, vaya a **Inicio** → **Herramientas de administración** → **DHCP** para abrir la herramienta de administración del servidor DHCP.
2. Encuentre el servidor y expanda todos los elementos en él.
3. Haga clic con el botón derecho en **Opciones del ámbito** y seleccione **Configurar opciones**. Aparece el cuadro de diálogo **Opciones del ámbito**.
4. Desplácese y seleccione **Información específica del proveedor 043**.
5. En el campo **Anotación de datos**, haga clic en cualquier lugar en el área debajo de **ASCII** e introduzca la dirección IP del servidor que tiene la ubicación de recurso compartido que contiene el archivo de configuración XML.
El valor aparece a medida que lo escribe bajo **ASCII** pero también aparece en modo binario a la izquierda.
6. Haga clic en **Aceptar** para guardar la configuración.

Configuración de la opción 60 en Windows

Para configurar la opción 60 en Windows:

1. En el servidor DHCP, vaya a **Inicio** → **Herramientas de administración** → **DHCP** para abrir la herramienta de administración del servidor DHCP.
2. Encuentre el servidor y expanda los elementos que se ubican en él.
3. Haga clic con el botón derecho en **IPv4** y elija **Definir clases de proveedores**.
4. Haga clic en **Agregar** e introduzca la siguiente información:
 - **Mostrar nombre:** iDRAC (solo lectura)
 - **Descripción:** clase de proveedor
 - En **ASCII**, haga clic e introduzca el iDRAC.
5. Haga clic en **Aceptar**.
6. En la ventana de DHCP, haga clic con el botón derecho en **IPv4** y seleccione **Establecer opciones predefinidas**.
7. Desde el menú desplegable **Clase de la opción**, seleccione **iDRAC** (creado en el paso 4) y haga clic en **Agregar**.
8. En el cuadro de diálogo **Tipo de opción**, introduzca la siguiente información:
 - **Nombre:** iDRAC
 - **Tipo de dato:** cadena
 - **Código:** 1
 - **Descripción:** identificador de clase de proveedor de Dell
9. Haga clic en **Aceptar** dos veces para volver a la ventana **DHCP**.
10. Expanda de todos los elementos en el nombre del servidor, haga clic con el botón derecho en **Opciones del ámbito** y seleccione **Configurar opciones**.
11. Haga clic en la ficha **Opciones avanzadas**.
12. Desde el menú desplegable **Clase de proveedor**, seleccione **iDRAC**. El 060iDRAC aparece en la columna **Opciones disponibles**.
13. Seleccione la opción **060iDRAC**.
14. Introduzca el valor de cadena que se debe enviar al iDRAC (junto con una dirección IP estándar proporcionada por DHCP). El valor de cadena ayudará a importar el archivo de configuración XML correcto.

Para la configuración de **Entrada de DATOS, Valor de cadena** de la opción, utilice un parámetro que tenga las siguientes opciones de letras y valores:

- Nombre de archivo: **iDRAC_Config.XML** o **iDRAC_Config-<service-tag>.XML**. (-f)
- Nombre de recurso compartido: (-n)
- Tipo de recurso compartido: -s (0 = NFS, 2 = CIFS)
- IPAddress: dirección IP del recurso de archivos compartidos. (-i)
- Nombre de usuario: necesario para CIFS (-u)
- Contraseña: necesaria para CIFS (-p)
- Tipo de apagado: especifique Ordenado o Forzado. (-d)
- Tiempo de espera: el valor predeterminado es 300 (-t)
- Estado de alimentación del host final: (-e)

Configuración de la opción 43 y la opción 60 en Linux

Actualice el archivo `/etc/dhcpd.conf`. De manera similar a Windows, los pasos son:

1. Deje un bloque o agrupación de direcciones que este servidor DHCP puede asignar.
2. Establezca la opción 43 y utilice el identificador de clase de nombre de proveedor para la opción 60.

Por ejemplo:

```
option myname code 43 = text; subnet 192.168.0.0 netmask 255.255.0.0 { #default
gateway option routers      192.168.0.1; option subnet-mask      255.255.255.0;
option nis-domain          "domain.org"; option domain-name      "domain.org"; option
domain-name-servers      192.168.1.1; option time-offset        -18000; # Eastern
Standard Time # option ntp-servers      192.168.1.1; # option netbios-name-
servers      192.168.1.1; # --- Selects point-to-point node (default is hybrid).
Don't change this unless # -- you understand Netbios very well # option
netbios-node-type 2; option vendor-class-identifier "iDRAC"; set vendor-string
= option vendor-class-identifier; option myname "2001::9174:9611:5c8d:e85//
xmlfiles/dhcpProv.xml -u root -p calvin"; range dynamic-bootp 192.168.0.128
192.168.0.254; default-lease-time 21600; max-lease-time 43200; # we want the
nameserver to appear at a fixed address host ns { next-server
marvin.redhat.com; hardware ethernet 12:34:56:78:AB:CD; fixed-address
207.175.42.254; } }
```

Activación de la configuración automática mediante la interfaz web del iDRAC

Asegúrese de que las opciones DHCPv4 y Activar IPv4 están activadas y que Detección automática está desactivada.

Para activar la configuración automática:

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Configuración de iDRAC** → **Red**. Aparecerá la página **Red**.
2. En la sección **Configuración automática**, seleccione una de las siguientes opciones para activar **Configuración automática**:
 - **Activar una vez**: configura el componente solo una vez mediante el archivo XML sugerido por el servidor DHCP. Después de esto, se desactiva la configuración automática.
 - **Activar una vez después de restablecer**: después de restablecer iDRAC, se configuran los componentes solo una vez mediante el archivo XML sugerido por el servidor DHCP. Después de esto, se desactiva la configuración automática.

Para desactivar la función de configuración automática, seleccione **Desactivar**.

3. Haga clic en **Aplicar** para aplicar la configuración.

Activar configuración automática mediante RACADM

Para activar la función de configuración automática mediante RACADM, utilice el objeto `iDRAC.NIC.AutoConfig`. Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8).

Cómo usar contraseñas de algoritmos hash para obtener una mayor seguridad

Para iDRAC en servidores de 13.^a generación, puede configurar las contraseñas de usuario y las contraseñas del BIOS utilizando un formato de hash unidireccional. El mecanismo de autenticación del usuario no se ve afectado (excepto para SNMPv3 e IPMI) y puede proporcionar la contraseña en texto sin formato.

Con la nueva función de contraseña de algoritmos hash:

- Puede generar sus propios algoritmos hash SHA256 para configurar contraseñas de usuario de iDRAC y contraseñas del BIOS. Esto permite tener los valores de SHA256 en el perfil de configuración de servidor, RACADM y WSMAN. Cuando ingresa los valores de la contraseña SHA256, no puede autenticar a través de SNMPv3 e IPMI.
- Puede configurar un servidor de plantillas que incluya todas las cuentas de usuario de iDRAC y BIOS mediante el mecanismo actual de texto sin formato. Después de configurar el servidor, puede exportar el perfil de configuración del servidor con la contraseña que posee los valores de algoritmos hash. La exportación incluirá los valores de algoritmos hash requeridos para la autenticación de SNMPv3 e IPMI.

Puede generar la contraseña de algoritmos hash con y sin Salt mediante SHA256.

Debe tener privilegios de control de servidor para incluir y exportar contraseñas de algoritmos hash.

Si se pierde el acceso a todas las cuentas, use la utilidad de configuración de iDRAC o RACADM local y lleve a cabo la tarea de restablecimiento de los valores predeterminados de iDRAC.

Si la contraseña de la cuenta de usuario de iDRAC se ha configurado solo con el algoritmo hash de contraseña SHA256 y no con otros algoritmos hash (SHA1v3Key o MD5v3Key), no estará disponible la autenticación mediante SNMP v3 e IPMI.

Contraseña de algoritmos hash mediante RACADM

Utilice los siguientes objetos con el subcomando `set racadm` para configurar contraseñas de algoritmos hash:

- `iDRAC.Users.SHA256Password`
- `iDRAC.Users.SHA256PasswordSalt`

Utilice el siguiente comando para incluir la contraseña de algoritmos hash en el perfil de configuración del servidor exportado:

```
racadm get -f <file name> -l <NFS / CIFS share> -u <username> -p <password> -t <filetype> --includePH
```

Debe configurar el atributo Salt al configurar el algoritmo hash asociado.

 **NOTA:** Los atributos no son aplicables al archivo de configuración INI.

Contraseña de algoritmos hash en el perfil de configuración del servidor

Las contraseñas de algoritmos hash nuevas pueden exportarse de manera opcional en el perfil de configuración del servidor.

Al importar el perfil de configuración del servidor, puede quitar el código de comentario del atributo de contraseña existente o de los nuevos atributos de contraseña de algoritmo hash. Si se quita el código de comentario de ambos atributos, se genera un error y no se establece la contraseña. Los atributos comentados no se aplican durante una importación.

Generación de contraseñas de algoritmos hash sin autenticación de SNMPv3 e IPMI

Para generar contraseñas de algoritmos hash sin autenticación de SNMPv3 e IPMI:

1. Para cuentas de usuario de iDRAC, debe configurar el atributo Salt de la contraseña con SHA256. Al configurar el atributo Salt de la contraseña, se agregará una cadena de binarios de 16 bytes. Salt es necesario para tener 16 bytes de largo, si se ha proporcionado.
2. Proporcione el valor del algoritmo hash y del atributo Salt en el perfil de configuración del servidor importado, los comandos de RACADM o WSMAN.
3. Después de configurar la contraseña, la autenticación de contraseña de texto sin formato normal funcionará, excepto que falle la autenticación de SNMP v3 e IPMI para cuentas de usuario de iDRAC que poseen contraseñas actualizadas con algoritmos hash.

Configuración de Management Station

Una estación de administración es un equipo que se utiliza para acceder a las interfaces de iDRAC con el fin de supervisar y administrar servidores PowerEdge de manera remota.

Para configurar la estación de administración.

1. Instale un sistema operativo compatible. Para obtener más información, consulte el archivo Léame.
2. Instale y configure un explorador web compatible (Internet Explorer, Firefox, Chrome o Safari).
3. Instale el Java Runtime Environment (JRE) más reciente (obligatorio si el tipo de complemento Java se utiliza para acceder a iDRAC mediante un explorador web).
4. Desde el DVD *Dell Systems Management Tools and Documentation* (DVD de herramientas y documentación de Dell Systems Management), instale VMCLI y RACADM remoto desde la carpeta SYSMGMT. O bien, ejecute el archivo **Setup** en el DVD para instalar RACADM remoto de manera predeterminada y otro software OpenManage. Para obtener más información acerca de RACADM, consulte *iDRAC8 RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8), disponible en dell.com/support/manuals.
5. Instale los elementos siguientes según los requisitos:
 - Telnet
 - Cliente SSH
 - TFTP
 - Dell OpenManage Essentials

Enlaces relacionados

[Instalación y uso de la utilidad de VMCLI](#)

[Configuración de exploradores web compatibles](#)

Acceso a iDRAC de manera remota

Para acceder a la interfaz web de iDRAC de manera remota desde una estación de administración, asegúrese de que la estación de administración se encuentre en la misma red que iDRAC. Por ejemplo:

- Servidores blade: la estación de administración debe residir en la misma red que CMC. Para obtener más información acerca de cómo aislar la red CMC de la red del sistema administrado, consulte *Chassis Management Controller User's Guide* (Guía del usuario de Chassis Management Controller) disponible en dell.com/support/manuals.
- Servidores tipo bastidor y torre: configure la NIC de iDRAC en LOM1 y asegúrese de que la estación de administración se encuentre en la misma red que iDRAC.

Para acceder a la consola del sistema administrado desde una estación de administración, utilice la consola virtual a través de la interfaz web de iDRAC.

Enlaces relacionados

[Inicio de la consola virtual](#)

[Configuración de red](#)

Configuración de Managed System

Si necesita ejecutar RACADM local o activar la captura de la pantalla de último bloqueo, instale los elementos siguientes desde el DVD *Herramientas y documentación de Dell Systems Management*:

- RACADM local
- Server Administrator

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

Enlaces relacionados

[Modificación de la configuración de la cuenta de administrador local](#)

Modificación de la configuración de la cuenta de administrador local

Después de configurar la dirección IP de iDRAC, puede modificar la configuración de la cuenta de administrador local (es decir, el usuario 2) mediante la utilidad de configuración de iDRAC. Para ello:

1. En la utilidad de configuración de iDRAC, vaya a **Configuración de usuario**.
Se muestra la página **Configuración de usuario de la configuración de iDRAC**.
2. Especifique los detalles de **Nombre de usuario**, **Privilegio de usuario en la LAN**, **Privilegio de usuario de puerto serie** y **Contraseña**.
Para obtener información acerca de las opciones, consulte la *Ayuda en línea de la utilidad de configuración de iDRAC*.
3. Haga clic en **Atrás**, en **Terminar** y, a continuación, en **Sí**.
Se habrán configurado los valores de la cuenta de administrador local.

Configuración de la ubicación de Managed System

Puede especificar los detalles de la ubicación del sistema administrado en el centro de datos mediante la interfaz web de iDRAC o la utilidad de configuración de iDRAC.

Configuración de la ubicación de Managed System mediante la interfaz web

Para especificar los detalles de ubicación del sistema:

1. En la interfaz web de iDRAC, vaya a **Información general** → **Servidor** → **Propiedades** → **Detalles**. Aparecerá la página **Detalles del sistema**.
2. En **Ubicación del sistema**, introduzca los detalles de la ubicación del sistema administrado en el centro de datos.
Para obtener más información acerca de estas opciones, consulte la *Ayuda en línea de iDRAC*.
3. Haga clic en **Aplicar**. Los detalles de la ubicación del sistema se guardan en iDRAC.

Configuración de la ubicación de Managed System mediante RACADM

Para especificar los detalles de ubicación del sistema, utilice los objetos de grupo `System.Location`. Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8)*, disponible en dell.com/support/manuals.

Configuración de la ubicación de Managed System mediante la utilidad de configuración de iDRAC

Para especificar los detalles de ubicación del sistema:

1. En la utilidad de configuración de iDRAC, vaya a **Ubicación del sistema**. Se muestra la página **Ubicación del sistema de la configuración de iDRAC**.
2. Introduzca los detalles de la ubicación del sistema administrado en el centro de datos. Para obtener más información, consulte la *Ayuda en línea de la utilidad de configuración de iDRAC*.
3. Haga clic en **Atrás**, en **Terminar** y, a continuación, en **Sí**.
Los detalles se guardan.

Optimización del rendimiento y el consumo de alimentación del sistema

La alimentación necesaria para refrigerar un servidor puede aumentar en forma significativa la alimentación de todo el sistema. El control térmico es la administración activa de la refrigeración del sistema mediante la administración de la velocidad del ventilador y la alimentación del sistema para asegurar que el sistema sea confiable y minimizar el consumo de alimentación del sistema, el flujo de aire y la salida acústica del sistema. Puede ajustar la configuración del control térmico y optimizar los requisitos de rendimiento del sistema y de rendimiento por vatio.

Si utiliza la interfaz web de iDRAC, RACADM o la utilidad de configuración de iDRAC, puede cambiar las siguientes opciones térmicas:

- Optimizar el rendimiento
- Optimizar la alimentación mínima
- Establecer la temperatura máxima de la salida de aire
- Aumentar el flujo de aire mediante el desplazamiento de un ventilador, si es necesario
- Aumentar el flujo de aire mediante el aumento de la velocidad mínima del ventilador

Modificación de la configuración térmica mediante la interfaz web de iDRAC

Para modificar la configuración térmica:

1. En la interfaz web de iDRAC, vaya a **Información general** → **Hardware** → **Ventiladores** → **Configuración**.


Aparece la página **Configuración del ventilador**.

2. Especifique lo siguiente:

- **Perfil térmico:** seleccione el perfil térmico:
 - **Configuración del perfil térmico predeterminado:** implica que al algoritmo térmico utiliza la misma configuración de perfil del sistema que se ha definido en la página **BIOS del sistema** → **Configuración del BIOS del sistema**. **Configuración del perfil del sistema**.

De forma predeterminada, esta opción está establecida en **Configuración de perfil térmico predeterminada**. También puede seleccionar un algoritmo personalizado, que es independiente del perfil de BIOS. Las opciones disponibles son:

- **Rendimiento máximo (Rendimiento optimizado) :**
 - * Disminución de la probabilidad de limitación de la CPU o de la memoria.
 - * Aumento de la probabilidad de activación del modo turbo.
 - * Por lo general, se dan velocidades de ventilador más altas en cargas de esfuerzo y en estado de inactividad.
- **Alimentación mínima (Rendimiento por vatio optimizado):**
 - * Optimizado para reducir el consumo de alimentación del sistema basado en el estado de alimentación óptimo del ventilador.
 - * Por lo general, se dan velocidades de ventilador menores en cargas de esfuerzo y en estado de inactividad.

 **NOTA:** Si selecciona **Rendimiento máximo** o **Alimentación mínima**, anula la configuración térmica asociada a la configuración del perfil del sistema en la página **BIOS del sistema** → **Configuración BIOS del sistema**. **Configuración del perfil del sistema**.

- **Límite de temperatura de salida máximo:** en el menú desplegable, seleccione la temperatura de aire de salida máxima. Los valores se muestran según el sistema.
El valor predeterminado es **Valor predeterminado, 70 °C (158 °F)**.

Esta opción permite cambiar las velocidades de los ventiladores del sistema para que la temperatura de salida no supere el límite de temperatura de salida seleccionado. Esto no se puede garantizar siempre bajo todas las condiciones de funcionamiento del sistema debido a la dependencia en la carga del sistema y la capacidad de enfriamiento del sistema.

- **Desplazamiento de la velocidad del ventilador:** seleccionar esta opción permite un enfriamiento adicional del servidor. En caso de que se agregue hardware (por ejemplo, tarjetas de PCIe nuevas), es posible que se requiera enfriamiento adicional. Un desplazamiento de la velocidad del ventilador provoca el aumento de las velocidades del ventilador (por el valor de % de desplazamiento) por encima de la línea base de las velocidades del ventilador, que se calculan mediante el algoritmo de control térmico. Los valores posibles son:
 - **Velocidad baja del ventilador:** lleva la velocidad del ventilador a una velocidad moderada.
 - **Velocidad media del ventilador:** lleva la velocidad del ventilador a un valor cercano al valor medio.
 - **Velocidad alta del ventilador:** lleva la velocidad del ventilador a un valor cercano a la velocidad máxima.

- **Velocidad máxima del ventilador:** lleva la velocidad del ventilador a la velocidad máxima.
- **Desactivado:** el desplazamiento de velocidad del ventilador se configura como desactivado. Este es el valor predeterminado. Cuando se configura como desactivado, no se muestra el porcentaje. Se aplica el valor predeterminado de velocidad de los ventiladores sin desplazamiento. De manera inversa, la configuración máxima hará funcionar a todos los ventiladores a su velocidad máxima.

El desplazamiento de la velocidad del ventilador es dinámico y se basa en el sistema. El aumento de la velocidad del ventilador para cada desplazamiento como se muestra junto a cada opción.

El desplazamiento de la velocidad del ventilador aumenta todas las velocidades de los ventiladores con el mismo porcentaje. Las velocidades del ventilador pueden aumentar por encima de las velocidades de desplazamiento en función de las necesidades de enfriamiento de los componentes individuales. Se espera que aumente el consumo de la alimentación del sistema general.


El desplazamiento de la velocidad del ventilador le permite aumentar la velocidad del ventilador del sistema con cuatro pasos graduales. Estos pasos se dividen por igual entre la velocidad de línea base típica y la velocidad máxima de los ventiladores del sistema del servidor. Algunas configuraciones de hardware resultan en mayores velocidades del ventilador de línea base, lo que provoca desplazamientos distintos al desplazamiento máximo para lograr la máxima velocidad.

El escenario de uso más común es el enfriamiento del adaptador PCIe no estándar. Sin embargo, la función se puede utilizar para aumentar el enfriamiento del sistema para otros fines.

- **Velocidad mínima del ventilador en PWM (% del valor máximo):** seleccione esta opción para ajustar la velocidad del ventilador. Al usar esta opción, puede configurar una velocidad más alta del ventilador en el sistema de referencia o aumentar la velocidad del ventilador del sistema si otras opciones de velocidad de ventiladores personalizados que no son necesarias no producen las velocidades más altas del ventilador requeridas.
 - **Predeterminado:** configura la velocidad mínima del ventilador con el valor predeterminado según lo establecido por el algoritmo de refrigeración del sistema.
 - **Personalizado:** introduzca el valor de porcentaje.

El intervalo permitido para Velocidad mínima del ventilador en PWM es dinámico y se basa en la configuración del sistema. El primer valor es la velocidad inactiva, mientras que el segundo es la configuración máx. (que puede o no ser del 100 % según la configuración del sistema).

Los ventiladores del sistema pueden funcionar por encima de esta velocidad según los requisitos térmicos del sistema, pero no por debajo de la velocidad mínima definida. Por ejemplo, la configuración mínima de la velocidad del ventilador al 35 % limita la velocidad del ventilador para que nunca sea inferior al 35 % de PWM.

 **NOTA:** 0 % de PWM no indica que el ventilador está apagado. Es la velocidad más baja que puede alcanzar el ventilador.

Los valores de configuración son persistentes, es decir que, una vez configurados y aplicados, no cambiarán automáticamente a la configuración predeterminada durante el reinicio del sistema, ciclos de encendido y apagado, actualizaciones del BIOS o de iDRAC. Ciertos servidores Dell pueden admitir o no algunas o todas estas opciones de refrigeración personalizadas del usuario. Si no se admiten las opciones, no aparecerán o no se podrá proporcionar un valor personalizado.

3. Haga clic en **Aplicar** para aplicar la configuración.

Aparece el mensaje siguiente:

It is recommended to reboot the system when a thermal profile change has been made. This is to ensure all power and thermal settings are activated.

Haga clic en **Reiniciar más tarde** o **Reiniciar ahora**.



NOTA: Debe reiniciar el sistema para que la actualización tenga efecto.

Modificación de la configuración térmica mediante RACADM

Para modificar la configuración térmica, utilice los objetos en el grupo **system.thermalsettings** con el subcomando **set** según se indica en la siguiente tabla.

Objeto	Descripción	Uso	Ejemplo
AirExhaustTemp	Permite configurar el límite de temperatura máxima de la salida de aire.	<p>Configure esta opción con alguno de los siguientes valores (según el sistema):</p> <ul style="list-style-type: none"> • 0 - Indica 40 °C • 1 - Indica 45 °C • 2 - Indica 50 °C • 3 - Indica 55 °C • 4 - Indica 60 °C • 255 - Indica 70 °C (predeterminado) 	<p>Para comprobar la configuración existente en el sistema:</p> <pre>racadm get system.thermalsettings.AirExhaustTemp</pre> <p>El resultado es:</p> <pre>AirExhaustTemp=70</pre> <p>Esto significa que el sistema está configurado para limitar la temperatura de salida de aire a 70 °C.</p> <p>Para establecer el límite de temperatura de salida en 60 °C:</p> <pre>racadm set system.thermalsettings.AirExhaustTemp 4</pre> <p>El resultado es:</p> <pre>Object value modified successfully.</pre> <p>Si un sistema no admite un determinado límite de temperatura de salida de aire, cuando ejecute el comando</p> <pre>racadm set system.thermalsettings.AirExhaustTemp 0</pre> <p>aparecerá el siguiente mensaje de error:</p> <pre>ERROR: RAC947: Invalid object value specified.</pre> <p>Asegúrese de especificar el valor según el tipo de objeto.</p> <p>Para obtener más información, consulte la ayuda de RACADM.</p>

Objeto	Descripción	Uso	Ejemplo
			Para establecer el límite del valor predeterminado: <pre>racadm set system.thermalsettings.AirExhaustTemp 255</pre>
FanSpeedHighOffsetVal	<ul style="list-style-type: none"> Al obtener esta variable, se lee el valor de desplazamiento de velocidad del ventilador en % de PWM en la opción Desplazamiento de velocidad alta del ventilador. Este valor depende del sistema. Utilice el objeto <code>FanSpeedOffset</code> para configurar este valor con el valor de índice 1. 	Valores de 0 a 100	<pre>racadm get system.thermalsettings FanSpeedHighOffsetVal</pre> <p>Esta acción devuelve un valor como "66". Esto significa que al utilizar el siguiente comando, se aplica una compensación de velocidad alta del ventilador (66 % de PWM) sobre la línea de base de la velocidad del ventilador</p> <pre>racadm set system.thermalsettings FanSpeedOffset 1</pre>
FanSpeedLowOffsetVal	<ul style="list-style-type: none"> Al obtener esta variable, se lee el valor de desplazamiento de velocidad del ventilador en % de PWM en la opción Desplazamiento de velocidad baja del ventilador. Este valor depende del sistema. Utilice el objeto <code>FanSpeedOffset</code> para configurar este valor con el valor de índice 0. 	Valores de 0 a 100	<pre>racadm get system.thermalsettings FanSpeedLowOffsetVal</pre> <p>Esta acción devuelve un valor como "23". Esto significa que al utilizar el siguiente comando, se aplica una compensación de velocidad baja del ventilador (23 % de PWM) sobre la línea de base de la velocidad del ventilador.</p> <pre>racadm set system.thermalsettings FanSpeedOffset 0</pre>
FanSpeedMaxOffsetVal	<ul style="list-style-type: none"> Al obtener esta variable, se lee el valor de desplazamiento de velocidad del ventilador en % de PWM en la opción Desplazamiento de velocidad máxima del ventilador. Este valor depende del sistema. Utilice <code>FanSpeedOffset</code> para configurar este valor con el valor de índice 3 	Valores de 0 a 100	<pre>racadm get system.thermalsettings FanSpeedMaxOffsetVal</pre> <p>Esta acción devuelve un valor como "100". Esto significa que al utilizar el siguiente comando, se aplica una compensación de velocidad máxima del ventilador (es decir la velocidad máxima, 100 % de PWM). En la mayoría de los casos, este desplazamiento produce velocidades de ventilador en aumento hasta llegar a la velocidad máxima.</p> <pre>racadm set system.thermalsettings FanSpeedOffset 3</pre>

Objeto	Descripción	Uso	Ejemplo
FanSpeedMediumOffsetVal	<ul style="list-style-type: none"> Al obtener esta variable, se lee el valor de desplazamiento de velocidad del ventilador en % de PWM en la opción Desplazamiento de velocidad media del ventilador. Este valor depende del sistema. Utilice el objeto FanSpeedOffset para configurar este valor con el valor de índice 2 	Valores de 0 a 100	<pre>racadm get system.thermalsettings FanSpeedMediumOffsetVal</pre> <p>Esta acción devuelve un valor como "47". Esto significa que cuando al utilizar el siguiente comando, se aplica un desplazamiento de velocidad media del ventilador (47 % de PWM) sobre la línea de base de la velocidad del ventilador.</p> <pre>racadm set system.thermalsettings FanSpeedOffset 2</pre>
FanSpeedOffset	<ul style="list-style-type: none"> Si se usa este objeto con el comando get, se muestra el valor de desplazamiento de velocidad del ventilador existente. Si se usa este objeto con el comando set, se puede establecer el valor de desplazamiento de velocidad del ventilador requerido. El valor de índice decide qué desplazamiento que se aplica y los objetos FanSpeedLowOffsetVal, FanSpeedMaxOffsetVal, FanSpeedHighOffsetVal y FanSpeedMediumOffsetVal (definidos anteriormente) son los valores en los cuales se aplica el desplazamiento. 	<p>Los valores son:</p> <ul style="list-style-type: none"> 0 - Velocidad baja del ventilador 1 - Velocidad alta del ventilador 2 - Velocidad media del ventilador 3 - Velocidad máx. del ventilador 255 - Ninguno 	<p>Para ver la configuración existente:</p> <pre>racadm get system.thermalsettings.FanSpeedOffset</pre> <p>Para establecer el valor de desplazamiento de velocidad alta del ventilador (como se define en FanSpeedHighOffsetVal)</p> <pre>racadm set system.thermalsettings.FanSpeedOffset 1</pre>
MFSMaximumLimit	Límite de lectura máximo para MFS	Valores de 1 a 100	<p>Para mostrar el valor más alto que se puede configurar con la opción MinimumFanSpeed:</p> <pre>racadm get system.thermalsettings.MFSMaximumLimit</pre>
MFSMinimumLimit	Límite de lectura mínimo para MFS	<p>Valores de 0 a MFSMaximumLimit</p> <p>El valor predeterminado es 255 (significa None [Ninguno])</p>	<p>Para mostrar el valor más bajo que se puede configurar con la opción MinimumFanSpeed.</p> <pre>racadm get system.thermalsettings.MFSMinimumLimit</pre>

Objeto	Descripción	Uso	Ejemplo
MinimumFanSpeed	<ul style="list-style-type: none"> Permite configurar la velocidad mínima del ventilador que se requiere para que el sistema funcione. Define el valor de la línea de base (piso) de velocidad del ventilador. El sistema permitirá que los ventiladores perforen este valor de velocidad del ventilador definido. Este es el valor de % de PWM para la velocidad del ventilador. 	Valores de MFSMinimumLimit a MFSMaximumLimit Cuando el comando get devuelve el valor 255, significa que no se aplica el desplazamiento configurado por el usuario.	Para asegurarse de que la velocidad mínima del sistema no caiga por debajo del 45 % de PWM (45 debe ser un valor entre MFSMinimumLimit y MFSMaximumLimit): <pre>racadm set system.thermalsettings.MinimumFanSpeed 45</pre>
ThermalProfile	<ul style="list-style-type: none"> Permite especificar el algoritmo térmico de base. Permite configurar el perfil del sistema según sea necesario para el comportamiento térmico asociado con el perfil. 	Valores: <ul style="list-style-type: none"> 0 – Automático 1 – Máximo rendimiento 2 – Alimentación mínima 	Para ver la configuración del perfil térmico existente: <pre>racadm get system.thermalsettings.ThermalProfile</pre> Para establecer el perfil térmico como rendimiento máximo: <pre>racadm set system.thermalsettings.ThermalProfile 1</pre>

Modificación de la configuración térmica mediante la utilidad de configuración de iDRAC

Para modificar la configuración térmica:

1. En la utilidad de configuración de iDRAC, vaya a **Térmico**. Aparece la pantalla **Térmico de la configuración de iDRAC**.
2. Especifique lo siguiente:
 - Perfil térmico
 - Límite de temperatura de salida máximo
 - Compensación de velocidad del ventilador
 - Velocidad mínima del ventilador

Para obtener información sobre los campos, consulte [Modificación de la configuración térmica mediante la interfaz web](#).

Los valores de configuración son persistentes, es decir que, una vez configurados y aplicados, no cambiarán automáticamente a la configuración predeterminada durante el reinicio del sistema, ciclos de encendido y apagado, actualizaciones del BIOS o de iDRAC. Ciertos servidores Dell pueden admitir o no algunas o todas estas opciones de refrigeración personalizadas del usuario. Si no se admiten las opciones, no aparecerán o no se podrá proporcionar un valor personalizado.

3. Haga clic en **Atrás**, en **Terminar** y, a continuación, en **Sí**. Se habrán configurado los valores térmicos.

Configuración de exploradores web compatibles

iDRAC es compatible con los exploradores web Internet Explorer, Mozilla Firefox, Google Chrome y Safari. Para obtener información acerca de las versiones, consulte *Readme* (Léame) en dell.com/support/manuals.

Si se conecta a la interfaz web de iDRAC 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. Esta sección ofrece información para configurar Internet Explorer.

Para configurar el explorador web Internet Explorer:

1. Establezca IE en **Ejecutar como administrador**.
2. En el explorador web, vaya a **Herramientas** → **Opciones de Internet** → **Seguridad** → **Red local**.
3. Haga clic en **Nivel personalizado**, seleccione **Medio-bajo** y haga clic en **Restablecer**. Haga clic en **Aceptar** para confirmar. Haga clic en **Nivel personalizado** para abrir el cuadro de diálogo.
4. Desplácese hacia abajo hasta la sección Controles y complementos de ActiveX y establezca los valores siguientes:



NOTA: Los valores del estado Medio-bajo dependen de la versión de IE.

- 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

Bajo **Descargas**:

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

Bajo **Varios**:

- 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 solo 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 datos de formulario no cifrados: activar
- Usar el bloqueador de elementos emergentes: Desactivar

Bajo **Scripting**:

- Scripting activo: activar
- Permitir operaciones de pegado por medio de un script: activar
- Scripting de applets de Java: activar

5. Vaya a **Herramientas** → **Opciones de Internet** → **Opciones avanzadas**.

6. Bajo **Exploración**:

- Enviar direcciones URL en UTF-8: activado
- Desactivar la depuración de script (Internet Explorer): activado
- Desactivar la depuración de script (otros): activado
- Mostrar una notificación sobre cada error de script: desactivado
- Activar la instalación a petición (otros): activado
- Activar la transición de páginas: activado
- Activar extensiones de explorador de terceros: activado
- Iniciar accesos directos en ventanas ya abiertas: desactivado

Bajo **Configuración HTTP 1.1**:

- Usar HTTP 1.1: activado
- Usar HTTP 1.1 en conexiones de proxy: activado

Bajo **Java (Sun)**:

- Utilizar JRE 1.6.x.yz: activado (opcional; la versión puede diferir)

Bajo **Multimedia**:

- Activar Cambio automático del tamaño de imágenes: activado
- Activar animaciones en páginas web: activado
- Mostrar videos en páginas web: activado
- Mostrar imágenes: activado

En **Seguridad**:

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



NOTA: Para modificar la configuración, es recomendable conocer y comprender las consecuencias. Por ejemplo, si bloquea las ventanas emergentes, es posible que parte de la interfaz web de iDRAC no funcione correctamente.


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

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

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

10. Si utiliza IE9 y una dirección IPv6 para acceder a iDRAC, deje en blanco la opción **Usar secuencias de comandos de configuración automáticas**.

11. Si la casilla **Usar servidor proxy** está seleccionada, seleccione la casilla **No usar servidor proxy para direcciones locales**.
12. Haga clic dos veces en **Aceptar**.
13. Cierre y reinicie el explorador para asegurarse de que todos los cambios tengan efecto.

 **NOTA:** Al iniciar sesión en la interfaz web de iDRAC con Internet Explorer 9.x, en ocasiones el contenido de algunas páginas no se muestra correctamente. Para resolver este problema, presione <F12>. En la ventana **Depuración de Internet Explorer 9**, configure **Modo de documento** como **Internet Explorer 7**. El explorador se actualizará y aparecerá la página **Inicio de sesión** de iDRAC.


Enlaces relacionados

- [Visualización de las versiones traducidas de la interfaz web](#)
- [Cómo agregar iDRAC a la lista de dominios de confianza](#)
- [Desactivación de la función de lista blanca en Firefox](#)

Cómo agregar iDRAC a la lista de dominios de confianza

Cuando accede a la interfaz web de iDRAC, se le solicitará que agregue la dirección IP de iDRAC a la lista de dominios de confianza (si no figura en la lista). Cuando haya terminado, haga clic en **Actualizar** o reinicie el explorador web para establecer conexión a la interfaz web de iDRAC.

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

 **NOTA:** Cuando se conecta a la interfaz web de iDRAC con un certificado que no es de confianza para el explorador, es posible que el aviso de error de certificado del explorador se muestre una segunda vez tras confirmar el primer aviso. Este es el comportamiento esperado por motivos de seguridad.

Para agregar la dirección IP de iDRAC 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 iDRAC en **Agregar este sitio web a la zona**.
3. Haga clic en **Agregar**, en **Aceptar** y, a continuación, en **Cerrar**.
4. Haga clic en **Aceptar** y actualice el explorador.

Desactivación de la función de lista blanca en Firefox

Firefox cuenta con una función de seguridad de "lista blanca" que requiere permiso del usuario para instalar complementos en cada sitio distinto que aloje un complemento. Si se activa, la función de lista blanca requiere la instalación de un visor de consola virtual para cada iDRAC que visita, incluso si las versiones del visor son idénticas.

Para desactivar la función de lista blanca y evitar las instalaciones repetitivas e innecesarias de complementos, realice los pasos siguientes:

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 este. Los valores de **Nombre de la preferencia**, **Estado**, **Tipo** y **Valor** cambian a texto en negrita. El valor **Estado** cambia al conjunto de usuario y la opción **Valor** cambia a falso.
4. En la columna **Nombre de la preferencia**, busque **xpinstall.enabled**.

Asegúrese de que la opción **Valor** se haya establecido en **verdadero**. De no ser así, haga doble clic en **xpinstall.enabled** para establecer la opción **Valor** en **verdadero**.


Visualización de las versiones traducidas de la interfaz web

La interfaz web de iDRAC es compatible con los siguientes idiomas:

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

Los identificadores ISO entre paréntesis indican las variantes de los idiomas admitidos. Para algunos idiomas admitidos, se deberá cambiar el tamaño de la ventana en 1024 píxeles para ver todas las funciones.

La interfaz web de iDRAC está diseñada para funcionar con teclados localizados para las variantes de idioma admitidas. Algunas funciones de la interfaz web de iDRAC, como la consola virtual, podrían requerir pasos adicionales para acceder a funciones o letras específicas. Otros teclados no son compatibles y podrían provocar problemas inesperados.

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

Actualización del firmware de dispositivos

Con iDRAC es posible actualizar iDRAC, el BIOS y el firmware de todos los dispositivos compatibles con la actualización de Lifecycle Controller, por ejemplo:

- Lifecycle Controller
- Diagnóstico
- Paquete de controladores del sistema operativo
- Tarjeta de interfaz de red (NIC)
- Controladora RAID
- Unidad de fuente de alimentación (PSU)
- Unidades de estado sólido (SSD) de PCIe

Se debe cargar el firmware requerido para iDRAC. Una vez que la carga se completa, se muestra la versión actual del firmware instalado en el dispositivo y la versión aplicada. Si el firmware que se carga no es válido, aparece un mensaje de error. Las actualizaciones que no requieren un reinicio se aplican de inmediato. Las actualizaciones que sí lo requieren se preconfiguran y su ejecución queda confirmada para el siguiente reinicio del sistema. Un solo reinicio del sistema es suficiente para realizar todas las actualizaciones.

Una vez que se actualiza el firmware, la página **Inventario del sistema** muestra la versión de firmware actualizada y se graban los registros.

Los tipos de archivo de imagen admitidos del firmware son:

- **.exe** — Dell Update Package (DUP) basado en Windows
- **.d7**: contiene tanto al iDRAC como al firmware de Lifecycle Controller.

Para los archivos con extensión **.exe**, debe contar con el privilegio de control del sistema. La función con licencia de actualización remota del firmware y Lifecycle Controller deben estar activados.

Para los archivos con extensión **.d7**, debe contar el privilegio Configurar.

Puede realizar actualizaciones de firmware mediante los siguientes métodos:

- Use el archivo de imagen del firmware en un sistema local o en un recurso compartido de red.
- Conéctese con el sitio FTP, TFTP, HTTP o con un repositorio de red que contenga un catálogo de actualizaciones disponibles. Puede crear repositorios personalizados con Repository Manager. Para obtener más información, consulte *Repository Manager User's Guide* (Guía del usuario de Repository Manager). iDRAC proporciona automáticamente una diferencia entre el BIOS y el firmware que está instalado en el servidor y la ubicación del repositorio o el sitio FTP. Todas las actualizaciones aplicables contenidas en el repositorio se aplican al sistema. Esta función está disponible con la licencia iDRAC Enterprise.
- Programación de actualizaciones recurrentes y automatizadas del firmware mediante el archivo de catálogo ubicado en el sitio FTP o en la ubicación del repositorio de red.

La siguiente tabla proporciona información sobre si es necesario o no reiniciar el sistema cuando se actualiza el firmware de un componente en particular.


 **NOTA:** Cuando se aplican varias actualizaciones de firmware a través de los métodos fuera de banda, las actualizaciones se ordenan de la manera más eficiente posible para reducir los reinicios innecesarios del sistema.

Tabla 6. Actualización del firmware: componentes admitidos

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

Nombre del componente	¿Reversión del firmware admitida? (Sí o No)	Fuera de banda: ¿es necesario reiniciar el sistema?	En banda: ¿es necesario reiniciar el sistema?	Interfaz gráfica de usuario de Lifecycle Controller: ¿es necesario reiniciar?
CPLD	No	Sí	Sí	Sí
Tarjetas de FC	Sí	Sí	Sí	Sí
SSD PCIe	Sí	Sí	Sí	Sí

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

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

Enlaces relacionados

- [Descarga del firmware de dispositivos](#)
- [Actualización del firmware de un dispositivo individual](#)
- [Actualización del firmware mediante el repositorio](#)
- [Actualización del firmware mediante FTP](#)
- [Actualización del firmware de dispositivos mediante TFTP](#)
- [Actualización del firmware de dispositivos mediante HTTP](#)
- [Actualización del firmware de dispositivos mediante RACADM](#)
- [Programación de actualizaciones automáticas del firmware](#)
- [Actualización del firmware mediante la interfaz web de CMC](#)
- [Actualización del firmware mediante DUP](#)
- [Actualización del firmware mediante RACADM remoto](#)
- [Actualización del firmware mediante Lifecycle Controller Remote Services](#)

Descarga del firmware de dispositivos

El formato de archivo de imagen descargado depende del método de actualización:

- Interfaz web de iDRAC: descargue el archivo de imagen binario empaquetado como archivo autoextraíble. El archivo de imagen de firmware predeterminado es **firmimg.d7**.
 -  **NOTA:** Se utiliza el mismo formato de archivo para recuperar iDRAC mediante la interfaz web de CMC.
- Sistema administrado: descargue Dell Update Package (DUP) específico del sistema operativo. Las extensiones de archivo son **.bin** para los sistemas operativos Linux y **.exe** para los sistemas operativos de Windows.
- Lifecycle Controller: descargue el último archivo de catálogo y DUP, y utilice la función *Actualización de plataforma* en Lifecycle Controller para actualizar el firmware de dispositivos. Para obtener más información acerca de la actualización de la plataforma, consulte *Lifecycle Controller User's Guide* (Guía del usuario de Lifecycle Controller) disponible en **dell.com/support/manuals**.


Actualización del firmware mediante la interfaz web de iDRAC


Puede actualizar el firmware del dispositivo mediante imágenes del firmware disponibles en el sistema local, desde un repositorio de un recurso compartido de red (CIFS o NFS) o desde el FTP.

Actualización del firmware de un dispositivo individual


Antes de actualizar el firmware mediante el método de actualización de un dispositivo individual, asegúrese de que ha descargado la imagen del firmware en una ubicación del sistema local.

Para actualizar el firmware de un dispositivo individual mediante la interfaz web de iDRAC:

1. Vaya a **Descripción general** → **Configuración del iDRAC** → **Actualizar y revertir**.
Se muestra la ventana **Actualización del firmware**.
2. En la ficha **Actualizar**, seleccione **Local** como la **Ubicación del archivo**.
3. Haga clic en **Examinar**, seleccione el archivo de imagen del firmware del componente requerido y, a continuación, haga clic en **Cargar**.
4. Una vez finalizada la carga, la sección **Detalles de la actualización** muestra cada archivo del firmware cargado en el iDRAC y su estado.
Si el archivo de imagen de firmware es válido y se cargó satisfactoriamente, la columna **Contenido** muestra un  icono junto al nombre del archivo de imagen del firmware. Expanda el nombre para ver la información de **Nombre del dispositivo**, **Actual** y **Versión del firmware disponible**.
5. Seleccione el archivo del firmware requerido que se actualizará y haga clic en una de las siguientes opciones:
 - Para las imágenes del firmware que no requieren un reinicio del sistema host, haga clic en **Instalar**. Por ejemplo, en el archivo del firmware del iDRAC.
 - Para las imágenes de firmware que requieren un reinicio del sistema host, haga clic **Instalar y reiniciar** o **Instalar en el próximo reinicio**.
 - Para cancelar la actualización del firmware, haga clic en **Cancelar**.

 **NOTA:** Si ha cargado el mismo archivo de imagen del firmware más de una vez, solo estará disponible para la selección el archivo de firmware más reciente. La casilla de verificación para los archivos de imagen de firmware anteriores estará desactivada.

Al hacer clic en **Instalar**, **Instalar y reiniciar** o **Instalar en el próximo reinicio**, se muestra el mensaje `Updating Job Queue` (Actualizando cola de trabajos).
6. Haga clic en **Cola de trabajos** para mostrar la página **Cola de trabajos**, donde puede ver y administrar las actualizaciones del firmware preconfiguradas, o bien, haga clic en **Aceptar** para actualizar la página en uso en ese momento y ver el estado de la actualización del firmware.

 **NOTA:** Si abandona la página sin realizar las actualizaciones, aparecerá un mensaje de error y se perderá todo el contenido actualizado.

Enlaces relacionados

[Actualización del firmware de dispositivos](#)

[Visualización y administración de actualizaciones preconfiguradas](#)

[Descarga del firmware de dispositivos](#)

Actualización del firmware mediante el repositorio

Puede realizar varias actualizaciones de firmware mediante la especificación de un recurso compartido de red que contenga un repositorio válido de los DUP y un catálogo que describa los DUP disponibles. Cuando el iDRAC se conecta a la ubicación del recurso compartido de red y comprueba las

actualizaciones disponibles, se genera un informe de comparación que muestra una lista de todas las actualizaciones disponibles. A continuación, puede seleccionar y aplicar las actualizaciones necesarias contenidas en el repositorio en el sistema.

Antes de realizar una actualización mediante el repositorio, asegúrese de que:

- Se haya creado un repositorio que contenga paquetes de actualización basados en Windows (DUP) y un archivo de catálogo en el recurso compartido de red (CIFS o NFS). Si no hay un archivo de catálogo definido por el usuario disponible, se utiliza **Catalog.xml** de manera predeterminada.
- Lifecycle Controller está activado.
- Usted tiene privilegio de control del servidor para actualizar el firmware de dispositivos a excepción del iDRAC.

Para actualizar el firmware del dispositivo mediante un repositorio:

1. En la interfaz web de iDRAC, vaya a **Información general** → **Configuración de iDRAC** → **Actualizar y revertir**.

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

2. En la ficha **Actualizar**, seleccione **Recurso compartido de red** como **Ubicación de archivo**.

3. En la sección **Ubicación del catálogo**, introduzca los detalles de la configuración de la red.

Mientras se especifica la configuración para el recurso compartido de red, se recomienda evitar el uso de caracteres especiales en el nombre de usuario y la contraseña o codificar por porcentaje los caracteres especiales.

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

4. Haga clic en **Comprobar actualización**.

La sección **Detalles de la actualización** tiene un informe de comparación que muestra las versiones actuales de firmware y las versiones de firmware disponibles en el repositorio.



NOTA: El informe de comparación no incluye las actualizaciones del repositorio que no puedan aplicarse al sistema o hardware instalado o que no se admitan.

5. Seleccione las actualizaciones necesarias y realice una de las acciones siguientes:

- Para las imágenes de firmware que no requieren un reinicio del sistema host, haga clic en **Instalar**. Por ejemplo, en el archivo de firmware **.d7**.
- Para las imágenes de firmware que requieren un reinicio del sistema host, haga clic **Instalar y reiniciar** o **Instalar en el próximo reinicio**.
- Para cancelar la actualización del firmware, haga clic en **Cancelar**.

Al hacer clic en **Instalar**, **Instalar y reiniciar** o **Instalar en el próximo reinicio**, se muestra el mensaje **Updating Job Queue** (Actualizando cola de trabajos).

6. Haga clic en **Cola de trabajos** para mostrar la página **Cola de trabajos**, donde puede ver y administrar las actualizaciones del firmware preconfiguradas, o bien, haga clic en **Aceptar** para actualizar la página en uso en ese momento y ver el estado de la actualización del firmware.

Enlaces relacionados

[Actualización del firmware de dispositivos](#)

[Visualización y administración de actualizaciones preconfiguradas](#)

[Descarga del firmware de dispositivos](#)

[Programación de actualizaciones automáticas del firmware](#)

Actualización del firmware mediante FTP

Puede conectarse directamente al sitio FTP de Dell o a cualquier otro sitio FTP desde el iDRAC para realizar las actualizaciones del firmware. También puede utilizar los paquetes de actualización basados en

Windows (DUP) y un archivo de catálogo que se encuentran disponibles en el sitio FTP en lugar de a crear repositorios personalizados.

Antes de realizar una actualización mediante el repositorio, asegúrese de que:

- Lifecycle Controller está activado.
- Usted tiene privilegio de control del servidor para actualizar el firmware de dispositivos a excepción del iDRAC.

Para actualizar el firmware de un dispositivo mediante FTP:

1. En la interfaz web de iDRAC, vaya a **Información general** → **Configuración de iDRAC** → **Actualizar y revertir**.

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

2. En la ficha **Actualizar**, seleccione **FTP** como la **Ubicación del archivo**.
3. En la sección **Configuración del servidor FTP**, introduzca los detalles de FTP.
Para obtener información acerca de los campos, consulte la *Ayuda en línea de iDRAC*.
4. Haga clic en **Comprobar actualización**.
5. Una vez que la carga ha finalizado, la sección **Detalles de la actualización** tiene un informe de comparación que muestra las versiones actuales del firmware y las versiones del firmware que se encuentran disponibles en el repositorio.



NOTA: Las actualizaciones del repositorio que no se aplican al sistema o al hardware instalado o que no se admiten no se incluyen en el informe de comparación.

6. Seleccione las actualizaciones necesarias y realice una de las acciones siguientes:
 - Para las imágenes de firmware que no requieren un reinicio del sistema host, haga clic en **Instalar**. Por ejemplo, en el archivo de firmware **.d7**.
 - Para las imágenes de firmware que requieren un reinicio del sistema host, haga clic **Instalar y reiniciar** o **Instalar en el próximo reinicio**.
 - Para cancelar la actualización del firmware, haga clic en **Cancelar**.

Al hacer clic en **Instalar**, **Instalar y reiniciar** o **Instalar en el próximo reinicio**, se muestra el mensaje `Updating Job Queue` (Actualizando cola de trabajos).

7. Haga clic en **Cola de trabajos** para mostrar la página **Cola de trabajos**, donde puede ver y administrar las actualizaciones del firmware preconfiguradas, o bien, haga clic en **Aceptar** para actualizar la página en uso en ese momento y ver el estado de la actualización del firmware.

Enlaces relacionados

[Actualización del firmware de dispositivos](#)

[Visualización y administración de actualizaciones preconfiguradas](#)

[Descarga del firmware de dispositivos](#)

[Programación de actualizaciones automáticas del firmware](#)

Actualización del firmware de dispositivos mediante TFTP

Puede conectarse directamente al sitio TFTP desde iDRAC para realizar las actualizaciones del firmware. También puede utilizar los paquetes de actualización basados en Windows (DUP) y un archivo de catálogo disponible en el sitio TFTP en lugar de crear repositorios personalizados.

Antes de realizar una actualización, asegúrese de lo siguiente:

- Lifecycle Controller está activado.

- Usted tiene privilegio de control del servidor para actualizar el firmware de dispositivos a excepción del iDRAC.

Para actualizar el firmware de un dispositivo mediante TFTP:

1. En la interfaz web de iDRAC, vaya a **Información general** → **Configuración de iDRAC** → **Actualizar y revertir**.

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

2. En la ficha **Actualizar**, seleccione **TFTP** como la **Ubicación del archivo**.
3. En la sección **Configuración del servidor TFTP**, introduzca los detalles de TFTP.
Para obtener información acerca de los campos, consulte la *Ayuda en línea de iDRAC*.
4. Haga clic en **Comprobar actualización**.
5. Una vez que la carga ha finalizado, la sección **Detalles de la actualización** tiene un informe de comparación que muestra las versiones actuales del firmware y las versiones del firmware que se encuentran disponibles en el repositorio.



NOTA: Las actualizaciones del repositorio que no se aplican al sistema o al hardware instalado o que no se admiten no se incluyen en el informe de comparación.

6. Seleccione las actualizaciones necesarias y realice una de las acciones siguientes:
 - Para las imágenes de firmware que no requieren un reinicio del sistema host, haga clic en **Instalar**. Por ejemplo, en el archivo de firmware **.d7**.
 - Para las imágenes de firmware que requieren un reinicio del sistema host, haga clic **Instalar y reiniciar** o **Instalar en el próximo reinicio**.
 - Para cancelar la actualización del firmware, haga clic en **Cancelar**.

Al hacer clic en **Instalar**, **Instalar y reiniciar** o **Instalar en el próximo reinicio**, se muestra el mensaje `Updating Job Queue` (Actualizando cola de trabajos).

7. Haga clic en **Cola de trabajos** para mostrar la página **Cola de trabajos**, donde puede ver y administrar las actualizaciones del firmware preconfiguradas, o bien, haga clic en **Aceptar** para actualizar la página en uso en ese momento y ver el estado de la actualización del firmware.

Enlaces relacionados

[Descarga del firmware de dispositivos](#)

[Actualización del firmware de dispositivos](#)

[Visualización y administración de actualizaciones preconfiguradas](#)

[Descarga del firmware de dispositivos](#)

[Programación de actualizaciones automáticas del firmware](#)

Actualización del firmware de dispositivos mediante HTTP

Puede conectarse directamente al sitio HTTP desde iDRAC para realizar las actualizaciones del firmware. Puede utilizar los paquetes de actualización basados en Windows (DUP) y un archivo de catálogo disponible en el sitio HTTP en lugar de crear repositorios personalizados.

Antes de realizar una actualización mediante el repositorio, asegúrese de que:

- Lifecycle Controller está activado.
- Usted tiene privilegio de control del servidor para actualizar el firmware de dispositivos a excepción del iDRAC.

Para actualizar el firmware de un dispositivo mediante HTTP:

1. En la interfaz web de iDRAC, vaya a **Información general** → **Configuración de iDRAC** → **Actualizar y revertir**.

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

2. En la ficha **Actualizar**, seleccione **HTTP** como la **Ubicación del archivo**.
3. En la sección **Configuración del servidor HTTP**, introduzca los detalles de HTTP.
Para obtener información acerca de los campos, consulte la *Ayuda en línea de iDRAC*.
4. Haga clic en **Comprobar actualización**.
5. Una vez que la carga ha finalizado, la sección **Detalles de la actualización** tiene un informe de comparación que muestra las versiones actuales del firmware y las versiones del firmware que se encuentran disponibles en el repositorio.



NOTA: Las actualizaciones del repositorio que no se aplican al sistema o al hardware instalado o que no se admiten no se incluyen en el informe de comparación.

6. Seleccione las actualizaciones necesarias y realice una de las acciones siguientes:
 - Para las imágenes de firmware que no requieren un reinicio del sistema host, haga clic en **Instalar**. Por ejemplo, en el archivo de firmware **.d7**.
 - Para las imágenes de firmware que requieren un reinicio del sistema host, haga clic **Instalar y reiniciar** o **Instalar en el próximo reinicio**.
 - Para cancelar la actualización del firmware, haga clic en **Cancelar**.

Al hacer clic en **Instalar**, **Instalar y reiniciar** o **Instalar en el próximo reinicio**, se muestra el mensaje *Updating Job Queue* (Actualizando cola de trabajos).

7. Haga clic en **Cola de trabajos** para mostrar la página **Cola de trabajos**, donde puede ver y administrar las actualizaciones del firmware preconfiguradas, o bien, haga clic en **Aceptar** para actualizar la página en uso en ese momento y ver el estado de la actualización del firmware.

Introduzca las tareas que el usuario debe realizar al finalizar la tarea actual (opcional).

Enlaces relacionados

[Descarga del firmware de dispositivos](#)

[Actualización del firmware de dispositivos](#)

[Visualización y administración de actualizaciones preconfiguradas](#)

[Descarga del firmware de dispositivos](#)

[Programación de actualizaciones automáticas del firmware](#)

Actualización del firmware de dispositivos mediante RACADM

Para actualizar el firmware de dispositivos mediante RACADM, utilice el subcomando **update**. Para obtener más información, consulte *RACADM Reference Guide for iDRAC and CMC* (Guía de referencia de RACADM para iDRAC y CMC), disponible en dell.com/support/manuals.

Ejemplos:

- Para generar un informe de comparación mediante un repositorio de actualizaciones:

```
racadm update -f catalog.xml -l //192.168.1.1 -u test -p passwd --verifycatalog
```
- Para llevar a cabo todas las actualizaciones aplicables desde un repositorio de actualizaciones mediante **myfile.xml** como un archivo de catálogo y realizar un reinicio ordenado:

```
racadm update -f "myfile.xml" -b "graceful" -l //192.168.1.1 -u test -p passwd
```
- Para llevar a cabo todas las actualizaciones aplicables desde un repositorio de actualizaciones FTP mediante **Catalog.xml** como un archivo de catálogo:

```
racadm update -f "Catalog.xml" -t FTP -e 192.168.1.20/Repository/Catalog
```

Programación de actualizaciones automáticas del firmware

Puede crear un programa periódico recurrente para que el iDRAC compruebe las nuevas actualizaciones del firmware. En la fecha y la hora programadas, el iDRAC se conecta al recurso compartido de red especificado (CIFS o NFS) o el FTP, busca nuevas actualizaciones y aplica o divide en etapas todas las actualizaciones aplicables. El archivo de registro del servidor remoto contiene información sobre el acceso al servidor y las actualizaciones del firmware en etapas.

Las actualizaciones automáticas están disponibles únicamente para la licencia iDRAC Enterprise.

Puede programar actualizaciones automáticas del firmware mediante la interfaz web del iDRAC o RACADM.

 **NOTA:** La dirección IPv6 no se admite para programar actualizaciones automáticas del firmware.

Enlaces relacionados


[Descarga del firmware de dispositivos](#)

[Actualización del firmware de dispositivos](#)

[Visualización y administración de actualizaciones preconfiguradas](#)

Programación de la actualización automática del firmware mediante la interfaz web


Para programar la actualización automática del firmware mediante la interfaz web:

 **NOTA:** Si ya hay un trabajo programado, no cree la próxima ocurrencia programada de un trabajo. Se sobrescribe el trabajo programado actual.

1. En la interfaz web de iDRAC, vaya a **Información general** → **Configuración de iDRAC** → **Actualizar y revertir**.

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

2. Haga clic en la ficha **Actualización automática**.
3. Seleccione la opción **Activar actualización automática**.
4. Seleccione cualquiera de las siguientes opciones para especificar si es necesario reiniciar el sistema después de apilar las actualizaciones:
 - **Programar actualizaciones:** se apilan las actualizaciones del firmware pero no se reinicia el servidor.
 - **Programar actualizaciones y reiniciar el servidor:** se activa el reinicio del servidor una vez apiladas las actualizaciones del firmware.
5. Seleccione una de las siguientes opciones para especificar la ubicación de las imágenes del firmware:
 - **Red:** use el archivo de catálogo de un recurso compartido de red (CIFS o NFS). Introduzca los detalles de ubicación del recurso compartido de red.

 **NOTA:** Mientras se especifica la configuración para el recurso compartido de red, se recomienda evitar el uso de caracteres especiales en el nombre de usuario y la contraseña o codificar por porcentaje los caracteres especiales.

- **FTP:** utilice el archivo de catálogo del sitio FTP. Escriba los detalles del sitio FTP.
6. Según la opción elegida en el paso 5, introduzca los valores de configuración de la red o la configuración de FTP.

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

7. En la sección **Actualizar programa de ventana**, especifique la hora de inicio de la actualización del firmware y la frecuencia de las actualizaciones (diaria, semanal o mensual).

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

8. Haga clic en **Programar actualización**.

Se crea el próximo trabajo programado en la cola de trabajos. El trabajo del próximo período de tiempo se crea cinco minutos después del comienzo de la primera instancia del trabajo recurrente.

Programación de la actualización automática del firmware mediante RACADM

Para programar la actualización automática del firmware, utilice los siguientes comandos:

- Para activar la actualización automática del firmware:
`racadm set lifecycleController.lcattributes.AutoUpdate.Enable 1`
- Para ver el estado de la actualización automática del firmware:
`racadm get lifecycleController.lcattributes.AutoUpdate`
- Para programar la hora de inicio y la frecuencia de la actualización del firmware:
`racadm AutoUpdateScheduler create -u username -p password -l <location> [-f catalogfilename -pu <proxyuser> -pp<proxypassword> -po <proxy port> -pt <proxytype>] -time < hh:mm> [-dom < 1 - 28,L,'*'> -wom <1-4,L,'*'> -dow <sun-sat,'*'>] -rp <1-366> -a <applyserverReboot (1-enabled | 0-disabled)>`

Por ejemplo:

- Para actualizar de forma automática el firmware mediante un recurso compartido CIFS:

```
racadm AutoUpdateScheduler create -u admin -p pwd -l //1.2.3.4/CIFS-share -f cat.xml -time 14:30 -wom 1 -dow sun -rp 5 -a 1
```

- Para actualizar de forma automática el firmware mediante FTP:

```
racadm AutoUpdateScheduler create -u admin -p pwd -l ftp.mytest.com -pu puser -pp puser -po 8080 -pt http -f cat.xml -time 14:30 -wom 1 -dow sun -rp 5 -a 1
```

- Para ver el programa actual de actualización del firmware:
`racadm AutoUpdateScheduler view`
- Para desactivar la actualización automática del firmware:
`racadm set lifecycleController.lcattributes.AutoUpdate.Enable 0`
- Para borrar los detalles de programa:
`racadm AutoUpdateScheduler clear`

Actualización del firmware mediante la interfaz web de CMC

Puede actualizar el firmware de iDRAC para servidores blade mediante la interfaz web de CMC.

Para actualizar el firmware de iDRAC mediante la interfaz web de CMC:

1. Inicie sesión en la interfaz web de CMC.
2. Vaya a **Servidor** → **Descripción general** → **<nombre del servidor>**.
Se muestra la página **Estado del servidor**.
3. Haga clic en **Iniciar iDRAC** para iniciar la interfaz web y seleccione **Actualización del firmware de iDRAC**.

Enlaces relacionados

[Actualización del firmware de dispositivos](#)

[Descarga del firmware de dispositivos](#)

[Actualización del firmware mediante la interfaz web de iDRAC](#)

Actualización del firmware mediante DUP

Antes de actualizar el firmware mediante Dell Update Package (DUP), asegúrese de realizar lo siguiente:

- Instalar y activar los controladores de sistema administrado y la IPMI correspondientes.
- Activar e iniciar el servicio Instrumental de administración de Windows (WMI) si el sistema ejecuta el sistema operativo Windows.
 - ✎ **NOTA:** Mientras actualiza el firmware de iDRAC mediante la utilidad DUP en Linux, si aparecen mensajes de error tipo `usb 5-2: device descriptor read/64, error -71` en la consola, puede omitirlos.
- Si el sistema tiene el hipervisor ESX instalado, para que se ejecute el archivo DUP, asegúrese de que el servicio "usbarbitrator" se detenga mediante el comando: `service usbarbitrator stop`

Para actualizar iDRAC mediante DUP:

1. Descargue el DUP en función del sistema operativo y ejecútelos en el sistema administrado.
2. Ejecute el DUP.
El firmware se actualiza. No es necesario reiniciar el sistema una vez completado el firmware.

Actualización del firmware mediante RACADM remoto

Para actualizar mediante RACADM remoto:

1. Descargue la imagen del firmware al servidor TFTP o FTP. Por ejemplo, `C:\downloads\firmimg.d7`
2. Ejecute el siguiente comando de RACADM:

Servidor TFTP:

- Mediante el comando **fwupdate**: `racadm -r <iDRAC 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.d7**.
- Mediante el comando **update**: `racadm -r <iDRAC IP address> -u <username> -p <password> update -f <filename>`

Servidor FTP:

- Mediante el comando **fwupdate**: `racadm -r <iDRAC IP address> -u <username> -p <password> fwupdate -f <ftpserver IP> <ftpserver username> <ftpserver password> -d <path>`
donde *ruta de acceso* es la ubicación en el servidor FTP en la que está almacenado **firmimg.d7**.
- Mediante el comando **update**: `racadm -r <iDRAC IP address> -u <username> -p <password> update -f <filename>`

Para obtener más información, consulte la sección sobre el comando **fwupdate** en *iDRAC8 RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8), disponible en dell.com/support/manuals.

Actualización del firmware mediante Lifecycle Controller Remote Services

Para obtener información para actualizar el firmware mediante Lifecycle Controller Remote Services, consulte *Lifecycle Controller Remote Services Quick Start Guide* (Guía de inicio rápido de Lifecycle Controller Remote Services) disponible en dell.com/support/manuals.

Actualización del firmware del CMC desde el iDRAC

En los chasis FX2/FX2s, puede actualizar el firmware de Chassis Management Controller y de cualquier componente que se pueda actualizar mediante CMC y compartir por los servidores desde el iDRAC.

Antes de aplicar la actualización, asegúrese de lo siguiente:

- Los servidores no se admiten para el encendido mediante CMC.
- Los chasis con LCD deben mostrar un mensaje que indica "La actualización está en progreso".
- Los chasis sin LCD deben indicar el progreso de la actualización mediante el patrón de parpadeo del LED.
- Durante la actualización, los comandos de acción de alimentación del chasis se desactivan.

Las actualizaciones para componentes como Programmable System-on-Chip (PSoC) de IOM que requieren que todos los servidores estén inactivos se aplican en el siguiente ciclo de encendido del chasis.

Configuración del CMC para la actualización del firmware del CMC desde el iDRAC

En los chasis FX2/FX2s, antes de realizar la actualización del firmware del CMC y sus componentes compartidos desde el iDRAC, realice lo siguiente:

1. Inicie la interfaz web del CMC.
2. Navegue hacia **Descripción general del chasis** → **Configuración** → **General**.
3. En el menú desplegable **Modo administración de chasis en el servidor**, seleccione **Administrar y supervisar**, y haga clic en **Aplicar**.

Actualización del iDRAC para actualizar el firmware del CMC

En los chasis FX2/FX2s, antes de actualizar el firmware del CMC y sus componentes compartidos desde el iDRAC, realice las siguientes configuraciones en el iDRAC:

1. En la interfaz web de iDRAC, vaya a **Información general** → **Configuración de iDRAC** → **Actualizar y revertir** → **Configuración**
Aparecerá la página **Configuración de la actualización del firmware de Chassis Management Controller**.
2. Para **Permitir actualizaciones del a través de SO y Lifecycle Controller**, seleccione **Activado** para activar la actualización de firmware del CMC desde el iDRAC.
3. En **Configuración actual del CMC**, asegúrese de que la opción **Administración de chasis en modo de servidor** muestra **Administrar y supervisar**. Puede configurar esto en el CMC.

Visualización y administración de actualizaciones preconfiguradas

Es posible ver y eliminar los trabajos programados, incluidos los trabajos de configuración y actualización. Esta es una función que requiere licencia. Se pueden eliminar todos los trabajos puestos en cola para su ejecución durante el siguiente reinicio.

Enlaces relacionados

[Actualización del firmware de dispositivos](#)

Visualización y administración de actualizaciones preconfiguradas mediante la interfaz web de iDRAC

Para ver la lista de trabajos programados mediante la interfaz web de iDRAC, vaya a **Información general** → **Servidor** → **Cola de trabajos**. La página **Cola de trabajos** muestra el estado de los trabajos en la cola de trabajos de Lifecycle Controller. Para obtener información acerca de los campos mostrados, consulte la *Ayuda en línea de iDRAC*.

Para eliminar trabajos, seleccione los trabajos y haga clic en **Eliminar**. La página se actualiza y se eliminan de la cola de trabajos de Lifecycle Controller los trabajos seleccionados. Es posible eliminar todos los trabajos puestos en cola para la ejecución durante el próximo reinicio. No se pueden eliminar los trabajos activos, es decir, aquellos cuyo estado es *En ejecución* o *Descargando*.

Para eliminar los trabajos debe tener el privilegio de control del servidor.

Visualización y administración de actualizaciones preconfiguradas mediante RACADM

Para ver las actualizaciones en etapas mediante RACADM, utilice el subcomando **jobqueue**. Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8)*, disponible en dell.com/support/manuals.


Reversión del firmware del dispositivo

Puede revertir el firmware de iDRAC o de cualquier dispositivo admitido por Lifecycle Controller incluso si anteriormente se realizó una actualización con otra interfaz. Por ejemplo, si el firmware se actualizó con la interfaz gráfica de usuario de Lifecycle Controller, puede revertirlo con la interfaz web de iDRAC. Puede realizar una reversión de firmware para varios dispositivos con un solo reinicio de sistema.

En los servidores de 13.^a generación que tienen un solo firmware para iDRAC y Lifecycle Controller, la reversión de firmware de iDRAC también revertirá el firmware de Lifecycle Controller.

Puede realizar la reversión del firmware para los siguientes componentes:

- iDRAC con Lifecycle Controller
- BIOS
- Tarjeta de interfaz de red (NIC)
- Unidad de fuente de alimentación (PSU)
- Controladora RAID
- Plano posterior

 **NOTA:** No puede realizar la reversión de firmware de diagnósticos, Driver Pack y CPLD.

Antes de revertir el firmware, asegúrese de lo siguiente:

- Tener privilegios de configuración para revertir el firmware de iDRAC.
- Tener privilegios de control del servidor y tener Lifecycle Controller activado para revertir el firmware de cualquier dispositivo más allá de iDRAC.

Puede revertir el firmware a la versión anterior instalada mediante cualquiera de los métodos siguientes:

- Interfaz web del iDRAC
- Interfaz web del CMC
- CLI de RACADM (iDRAC y CMC)
- Lifecycle Controller
- Lifecycle Controller–Remote Services

Enlaces relacionados

- [Reversión del firmware mediante la interfaz web de iDRAC](#)
- [Reversión del firmware mediante la interfaz web de CMC](#)
- [Reversión del firmware mediante RACADM](#)
- [Reversión del firmware mediante Lifecycle Controller](#)
- [Reversión del firmware mediante Lifecycle Controller Remote Services](#)

Reversión del firmware mediante la interfaz web de iDRAC

Para revertir el firmware de un dispositivo:

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Configuración de iDRAC** → **Actualizar y revertir** → **Revertir**.
La página **Revertir** muestra los dispositivos cuyo firmware se puede revertir. Puede ver el nombre del dispositivo, los dispositivos asociados, la versión del firmware instalado actualmente y la versión de reversión del firmware disponible.
2. Seleccione uno o más de los dispositivos cuyo firmware desea revertir.
3. Según los dispositivos seleccionados, haga clic en **Instalar y reiniciar** o **Instalar en el próximo reinicio**. Si sólo se selecciona el iDRAC, haga clic en **Instalar**.
Al hacer clic en **Instalar y reiniciar** o **Instalar en el próximo reinicio**, se muestra el mensaje "Actualizando cola de trabajos".
4. Haga clic en **Cola de trabajo**.
Se muestra la página **Cola de trabajo**, donde puede ver y administrar las actualizaciones de firmware definidas.

NOTA:

- Mientras se encuentra en modo reversión, el proceso de reversión sigue en segundo plano incluso si se aleja de esta página.
- Si la configuración de iDRAC se restablece a los valores predeterminados, la dirección IP de iDRAC se restablece en 192.168.0.120. Puede acceder a iDRAC mediante esta IP o volver a configurar la dirección de iDRAC con el RACADM local o la tecla F2 (RACADM remoto requiere acceso de red).

Aparece un mensaje de error si:

- No tiene el privilegio de control de servidor para revertir otro firmware más allá de iDRAC o el privilegio de configuración para revertir firmware de iDRAC.
- La reversión de firmware ya está en progreso en otra sesión.
- Existe una ejecución programada de actualizaciones o ya se están ejecutando.

Si Lifecycle Controller está desactivado o en estado de recuperación e intenta realizar una reversión de firmware para cualquier dispositivo a excepción del iDRAC, aparecerá el mensaje de aviso correspondiente junto con los pasos a seguir para activar Lifecycle Controller.

Reversión del firmware mediante la interfaz web de CMC

Para revertir mediante la interfaz web de CMC:

1. Inicie sesión en la interfaz web de CMC.
2. Vaya a **Información general del servidor** → <nombre del servidor>. Se muestra la página **Estado del servidor**.
3. Haga clic en **Iniciar iDRAC** y realice una reversión del firmware del dispositivo como se indica en la sección [Reversión del firmware mediante la interfaz web de iDRAC](#).

Reversión del firmware mediante RACADM

Para revertir el firmware de un dispositivo mediante de racadm:

1. Compruebe el estado de la reversión y la propiedad FQDD con el comando `swinventory`:
`racadm swinventory`

Para el dispositivo para el que desea revertir el firmware, la `Rollback Version` (Versión de reversión) debe estar `Available` (Disponible). Asimismo, tome nota de la propiedad FQDD.

2. Reverta el firmware del dispositivo mediante:

```
racadm rollback <FQDD>
```

Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8), disponible en dell.com/support/manuals.

Reversión del firmware mediante Lifecycle Controller

Para obtener más información, consulte *Lifecycle Controller User's Guide* (Guía del usuario de Lifecycle Controller) disponible en dell.com/support/manuals.

Reversión del firmware mediante Lifecycle Controller Remote Services

Para obtener información, consulte *Lifecycle Controller Remote Services Quick Start Guide* (Guía de inicio rápido de Lifecycle Controller Remote Services) disponible en dell.com/support/manuals.

Recuperación de iDRAC


iDRAC admite dos imágenes de sistema operativo garantizar un iDRAC iniciable. En el caso de un error catastrófico imprevisto y la pérdida de ambas rutas de acceso de inicio

- El cargador de inicio de la CLI de iDRAC detecta que no hay ninguna imagen iniciable.
- El LED de condición e identificación del sistema parpadea en intervalos de ~1/2 segundos (el LED se encuentra en la parte posterior de los servidores tipo bastidor y torre y en la parte anterior de un servidor Blade).
- El cargador de inicio de la CLI ahora sondea en la ranura de la tarjeta SD.
- Formatee una tarjeta SD con FAT mediante el sistema operativo Windows o EXT3 mediante un sistema operativo Linux.
- Copie el archivo **firmimg.d7** en la tarjeta SD.
- Inserte la tarjeta SD en el servidor.

- El cargador de inicio de la CLI detecta la tarjeta SD, convierte el LED que parpadea en ámbar sólido, lee el archivo `firmimg.d7`, vuelve a programar iDRAC y luego reinicia iDRAC.

Uso del servidor TFTP

Puede configurar el servidor de protocolo de transferencia de archivos trivial (TFTP) para actualizar o revertir el firmware de iDRAC o instalar certificados. Se utiliza en interfaces de línea de comandos SM-CLP y RACADM para transferir archivos desde y hacia iDRAC. Debe poder accederse al servidor TFTP mediante una dirección IP de iDRAC o un nombre de DNS.

 **NOTA:** Si utiliza la interfaz web de iDRAC para transferir certificados y actualizar el firmware, el servidor TFTP no es necesario.

Puede utilizar el comando `netstat -a` en los sistemas operativos Windows o Linux para ver si hay un servidor TFTP en ejecución. El puerto predeterminado para TFTP es 69. Si el servidor TFTP no está en ejecución, realice uno de los procedimientos siguientes:

- Busque otro equipo en la red que ejecute un servicio TFTP.
- Instale un servidor TFTP en el sistema operativo.

Copia de seguridad del perfil del servidor

Puede realizar una copia de seguridad de la configuración del sistema, incluidas las imágenes del firmware instalado en los distintos componentes, como BIOS, RAID, NIC, iDRAC, Lifecycle Controller y las tarjetas de red dependientes (NDC) y los valores de configuración de dichos componentes. La operación de copia de seguridad también incluye los datos de configuración del disco duro, la placa base y las piezas reemplazadas. La copia de seguridad crea un archivo individual que puede guardar en una tarjeta vFlash SD o en un recurso compartido de red (CIFS o NFS).

Además, puede activar y programar copias de seguridad periódicas del firmware y de la configuración del servidor en un determinado día, semana o mes.

La función de copia de seguridad requiere una licencia y está disponible con la licencia Enterprise de iDRAC.

 **NOTA:** En los servidores de 13ª generación, esta función se activa de forma automática.

Antes de realizar una operación de copia de seguridad, asegúrese de que:

- La opción Recopilar inventario del sistema al reiniciar (CSIOR) está activada. Si CSIOR está desactivada e inicia una operación de copia de seguridad, se muestra el siguiente mensaje:
`System Inventory with iDRAC may be stale, start CSIOR for updated inventory`
- Para realizar una copia de seguridad en una tarjeta vFlash SD:
 - La tarjeta vFlash SD admitida por Dell esté colocada, activada e inicializada.
 - La tarjeta vFlash SD cuente con espacio suficiente para almacenar el archivo de copia de seguridad.

El archivo de copia de seguridad contiene datos confidenciales del usuario cifrados, información de configuración e imágenes del firmware que puede usar para la operación de importación del perfil del servidor.

Los sucesos de copia de seguridad se graban en el registro de Lifecycle.

Enlaces relacionados

[Programación de la copia de seguridad automática del perfil del servidor](#)
[Importación del perfil del servidor](#)

Cómo hacer una copia de seguridad del perfil del servidor mediante la interfaz web de iDRAC

Para hacer una copia de seguridad del perfil del servidor mediante la interfaz web de iDRAC:

1. Vaya a **Descripción general** → **Configuración del iDRAC** → **Perfil del servidor**. Aparece la página **Hacer copia de seguridad y exportar perfil del servidor**.
2. Seleccione una de las siguientes opciones para guardar la imagen del archivo de copia de seguridad:
 - **Red** para guardar la imagen del archivo de copia de seguridad en un recurso compartido CIFS o NFS.
 - **vFlash** para guardar la imagen del archivo de copia de seguridad en la tarjeta vFlash.
3. Introduzca el nombre del archivo de copia de seguridad y la frase de contraseña del cifrado (opcional).
4. Si **Red** está seleccionada como la ubicación del archivo, introduzca la configuración de la red.
 **NOTA:** Mientras se especifica la configuración para el recurso compartido de red, se recomienda evitar el uso de caracteres especiales en el nombre de usuario y la contraseña o codificar por porcentaje los caracteres especiales.
Para obtener información acerca de los campos, consulte la *Ayuda en línea de iDRAC*.
5. Haga clic en **Hacer copia de seguridad ahora**.
La operación de copia de seguridad se inicia y puede ver el estado en la página **Cola de trabajos**. Después de que la operación se complete correctamente, se creará el archivo de copia de seguridad en la ubicación especificada.

Copia de seguridad del perfil del servidor mediante RACADM

Para hacer una copia de seguridad del perfil del servidor mediante RACADM, utilice el subcomando **systemconfig backup**. Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8), disponible en dell.com/support/manuals.

Programación de la copia de seguridad automática del perfil del servidor

Puede activar y programar copias de seguridad periódicas de la configuración del firmware y del servidor según un día, una semana o un mes determinados.

Antes de programar la operación de copia de seguridad automática del perfil del servidor, asegúrese de que:

- La opción Lifecycle Controller y Recopilar inventario del sistema al reiniciar (CSIOR) está activada.
- El protocolo de hora de red (NTP) está activado de modo que las desviaciones de tiempo no afecten los tiempos reales de ejecución de los trabajos programados y cuando se crea el siguiente trabajo programado.
- Para realizar una copia de seguridad en una tarjeta vFlash SD:
 - La tarjeta vFlash SD admitida por Dell esté colocada, activada e inicializada.
 - La tarjeta vFlash SD cuente con espacio suficiente para almacenar el archivo de copia de seguridad.



NOTA: No se admite la dirección IPv6 para la programación de la copia de seguridad automática del perfil del servidor.

Programación de la copia de seguridad automática del perfil del servidor mediante la interfaz web

Para programar la copia de seguridad automática del perfil del servidor:

1. En la interfaz web de iDRAC, vaya a **Información general** → **Configuración de iDRAC** → **Perfil del servidor**.
Aparece la página **Hacer copia de seguridad y exportar perfil del servidor**.
2. Haga clic en la ficha **Copia de seguridad automática**.
3. Seleccione la opción **Activar copia de seguridad automática**.
4. Seleccione una de las siguientes opciones para guardar la imagen del archivo de copia de seguridad:
 - **Red** para guardar la imagen del archivo de copia de seguridad en un recurso compartido CIFS o NFS.
 - **vFlash** para guardar la imagen del archivo de copia de seguridad en la tarjeta vFlash.
5. Introduzca el nombre del archivo de copia de seguridad y la frase de contraseña del cifrado (opcional).
6. Si **Red** está seleccionada como la ubicación del archivo, introduzca la configuración de la red.
 - NOTA:** Mientras se especifica la configuración para el recurso compartido de red, se recomienda evitar el uso de caracteres especiales en el nombre de usuario y la contraseña o codificar por porcentaje los caracteres especiales.

Para obtener información acerca de los campos, consulte la *Ayuda en línea de iDRAC*

7. En la sección **Programa de la ventana de copia de seguridad**, especifique la hora de inicio y la frecuencia (diaria, semanal o mensual) de la operación de copia de seguridad.
Para obtener información acerca de los campos, consulte la *Ayuda en línea de iDRAC*.
8. Haga clic en **Programar copia de seguridad**.
El trabajo recurrente se representa en la cola de trabajos con una fecha y hora de inicio para la próxima operación de copia de seguridad programada. Cinco minutos después de que comienza la primera instancia de un trabajo recurrente, se crea el trabajo del próximo período de tiempo. La operación de copia de seguridad del perfil del servidor se lleva a cabo a la fecha y hora programadas.

Programación de la copia de seguridad automática del perfil del servidor mediante RACADM

Para activar la copia de seguridad automática utilice el comando:

```
racadm set lifecyclecontroller.lcattributes.autobackup Enabled
```

Para programar una operación de copia de seguridad del perfil del servidor:

```
racadm systemconfig backup -f <filename> <target> [-n <passphrase>] -time  
<hh:mm> -dom <1-28,L,'*'> -dow<*,Sun-Sat> -wom <1-4, L,'*'> -rp <1-366>-mb <Max  
Backups>
```

Para ver el programa de copia de seguridad actual:

```
racadm systemconfig getbackupscheduler
```

Para desactivar la copia de seguridad automática, utilice el comando:

```
racadm set LifeCycleController.lcattributes.autobackup Disabled
```

Para borrar el programa de copia de seguridad:

```
racadm systemconfig clearbackupscheduler
```


Para obtener más información, consulte iDRAC8 RACADM Command Line Interface Reference Guide (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8) disponible en dell.com/support/manuals.

Importación del perfil del servidor

Puede usar un archivo de imagen de copia de seguridad para importar (restaurar) la configuración y el firmware para el mismo servidor sin reiniciarlo.

En los servidores de 13ª generación, esta función automatiza todo el proceso de reemplazo de la placa base. Después de reemplazar la placa base y volver a instalar la memoria, las unidades de disco duro y otro hardware, aparece una pantalla de inicio especial que proporciona una opción para restaurar toda la configuración guardada, la etiqueta de servicio y la configuración de licencia y los programas de diagnóstico. El iDRAC de la placa base nueva lee esta información y restaura la configuración guardada.

La función de importación no está bajo licencia.

 **NOTA:** Para la operación de restauración, la etiqueta de servicio del sistema y la etiqueta de servicio en el archivo de copia de seguridad deben ser idénticas. La operación de restauración se aplica a todos los componentes del sistema que sean iguales y que estén presentes en la misma ubicación (por ejemplo, en la misma ranura) que en el momento que el archivo de copia de seguridad los capturó. Si los componentes son diferentes o no están en la misma ubicación, no se modificarán y las fallas de restauración se registrarán en el registro de Lifecycle.

Antes de realizar una operación de importación, asegúrese de que Lifecycle Controller esté activado. Si Lifecycle Controller no está activado e inicia una operación de importación, aparecerá el siguiente mensaje:

```
Lifecycle Controller is not enabled, cannot create Configuration job.
```

Cuando la importación está en progreso e inicia una operación de importación nuevamente, aparece un mensaje de error:

```
Restore is already running
```

Los sucesos de importación se graban en el registro de Lifecycle.


Enlaces relacionados

[Secuencia de operaciones de restauración](#)

Importación del perfil del servidor mediante la interfaz web de iDRAC

Para importar el perfil del servidor mediante la interfaz web de iDRAC:

1. Vaya a **Descripción general** → **Configuración del iDRAC** → **Perfil del servidor** → **Importar**. Aparecerá la sección **Importar perfil de servidor**.
2. Seleccione una de las siguientes opciones para especificar la ubicación del archivo de copia de seguridad:
 - **Network (Red)**

- **vFLASH**
3. Introduzca el nombre del archivo de copia de seguridad y la frase de contraseña del descifrado (opcional).
 4. Si **Red** está seleccionada como la ubicación del archivo, introduzca la configuración de la red.
-  **NOTA:** Mientras se especifica la configuración para el recurso compartido de red, se recomienda evitar el uso de caracteres especiales en el nombre de usuario y la contraseña o codificar por porcentaje los caracteres especiales.

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

5. Seleccione una de las siguientes opciones para **Configuración de discos virtuales y datos del disco duro**:
 - **Preservar:** preserva el nivel de RAID, el disco virtual, los atributos de la controladora y los datos del disco duro en el sistema y restaura el sistema a un estado anterior conocido mediante el archivo de imagen de copia de seguridad.
 - **Eliminar y reemplazar:** elimina y reemplaza el nivel de RAID, el disco virtual, los atributos de la controladora y la información de configuración del disco duro en el sistema con los datos del archivo de imagen de copia de seguridad.
6. Haga clic en **Importar**.

Se inicia la operación de importación del perfil del servidor.

Importación del perfil del servidor mediante RACADM

Para importar el perfil del servidor mediante RACADM, utilice el comando **systemconfig restore**. Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8), disponible en dell.com/support/manuals.

Secuencia de operaciones de restauración

La secuencia de operaciones de restauración es la siguiente:

1. El sistema host se apaga.
2. La información del archivo de copia de seguridad se utiliza para restaurar Lifecycle Controller.
3. El sistema host se enciende.
4. El proceso de restauración del firmware y de la configuración de los dispositivos se completa.
5. El sistema host se apaga.
6. El proceso de restauración del firmware y de la configuración de iDRAC se completa.
7. iDRAC se reinicia.
8. El sistema host restaurado se enciende para reanudar el funcionamiento normal.

Supervisión de iDRAC mediante otras herramientas de administración del sistema

Puede descubrir y supervisar iDRAC mediante Dell Management Console o Dell OpenManage Essentials. También puede utilizar Dell Remote Access Configuration Tool (DRACT) para descubrir iDRAC, actualizar el firmware y configurar Active Directory. Para obtener más información, consulte las guías del usuario correspondientes.

Configuración de iDRAC


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

Antes de configurar iDRAC, asegúrese de que estén configuradas las opciones de red de iDRAC y un explorador compatible. Asimismo, asegúrese de que las licencias adecuadas estén actualizadas. Para obtener más información acerca de la función con licencia en iDRAC, consulte [Administración de licencias](#).

Puede configurar iDRAC con los siguientes elementos:

- Interfaz web del iDRAC
- RACADM
- Servicios remotos (consulte la *Lifecycle Controller Remote Services User's Guide* (Guía del usuario de Dell Lifecycle Controller Remote Services))
- IPMITool (consulte la *Baseboard Management Controller Management Utilities User's Guide* (Guía del usuario de Baseboard Management Controller Management Utilities))

Para configurar iDRAC:

1. Inicie sesión en iDRAC.
2. Si fuera necesario, modifique la configuración de la red.
 -  **NOTA:** Si ha configurado las opciones de red de iDRAC mediante la utilidad de configuración de iDRAC durante la configuración de la dirección IP de iDRAC, puede omitir este paso.
3. Configure las interfaces para acceder a iDRAC.
4. Configure la visualización del panel frontal.
5. Si fuera necesario, configure la ubicación del sistema.
6. Configure la zona horaria y el protocolo de hora de red (NTP), en caso de ser necesario.
7. Establezca cualquiera de los siguientes métodos de comunicación alternativos con iDRAC:
 - Comunicación en serie IPMI o RAC
 - Comunicación en serie IPMI en la LAN
 - IPMI en la LAN
 - Cliente SSH o Telnet
8. Obtenga los certificados necesarios.
9. Agregue y configure los usuarios con privilegios de iDRAC.
10. Configure y active las alertas por correo electrónico, las capturas SNMP o las alertas IPMI.
11. Si fuera necesario, establezca la política de límite de alimentación.
12. Active la pantalla de último bloqueo.
13. Si fuera necesario, configure la consola virtual y los medios virtuales.
14. Si fuera necesario, configure la tarjeta vFlash SD.
15. Si fuera necesario, establezca el primer dispositivo de inicio.
16. Establezca el paso del sistema operativo a iDRAC, en caso de ser necesario.

Enlaces relacionados

- [Inicio de sesión en iDRAC](#)
- [Modificación de la configuración de red](#)
- [Configuración de servicios](#)
- [Configuración del panel frontal](#)
- [Configuración de la ubicación de Managed System](#)
- [Configuración de zona horaria y NTP](#)
- [Configuración de la comunicación de iDRAC](#)
- [Configuración de cuentas de usuario y privilegios](#)
- [Supervisión y administración de la alimentación](#)
- [Activación de la pantalla de último bloqueo](#)
- [Configuración y uso de la consola virtual](#)
- [Administración de medios virtuales](#)
- [Administración de la tarjeta vFlash SD](#)
- [Configuración del primer dispositivo de inicio](#)
- [Activación o desactivación del paso del sistema operativo a iDRAC](#)
- [Configuración de iDRAC para enviar alertas](#)

Visualización de la información de iDRAC

Puede ver las propiedades básicas de iDRAC.

Visualización de la información de iDRAC mediante la interfaz web

En la interfaz web de iDRAC, vaya a **Información general** → **Configuración de iDRAC** → **Propiedades** para ver la siguiente información relacionada con iDRAC. Para obtener información acerca de las propiedades, consulte la *Ayuda en línea de iDRAC*.

- Versión de hardware y firmware
- Última actualización del firmware
- Hora del RAC
- Versión de IPMI
- Información de la barra de título de la interfaz de usuario
- Configuración de red
- Configuración de IPv4
- Configuración de IPv6

Visualización de la información de iDRAC mediante RACADM


Para ver la información de iDRAC mediante RACADM, consulte los detalles de los subcomandos `getsysinfo` o `get` incluidos en *iDRAC8 RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8), disponible en dell.com/support/manuals.

Modificación de la configuración de red

Después de establecer la configuración de red de iDRAC mediante la utilidad de configuración de iDRAC, también puede modificarla mediante la interfaz web de iDRAC, RACADM, Lifecycle Controller, Dell

Deployment Toolkit y Server Administrator (después de iniciar en el sistema operativo). Para obtener más información sobre las herramientas y la configuración de privilegios, consulte las guías de usuario correspondientes.

Para modificar la configuración de la red mediante la interfaz web de iDRAC o RACADM, deberá disponer de los privilegios **Configurar**.

 **NOTA:** Si modifica la configuración de red, es posible que se anulen las conexiones de red actuales a iDRAC.

Modificación de la configuración de red mediante la interfaz web

Para modificar la configuración de red de iDRAC:


1. En la interfaz web de iDRAC, vaya a **Información general** → **Configuración de iDRAC** → **Red**. Aparecerá la página **Red**.
2. Especifique la configuración de red, los valores comunes, IPv4, IPv6, IPMI y/o la configuración de VLAN según sus requisitos y haga clic en **Aplicar**.

Si selecciona **NIC autodedicada** en **Configuración de red**, cuando iDRAC tenga una NIC como LOM compartida (1, 2, 3 o 4) y se detecte un vínculo en la NIC dedicada de iDRAC, iDRAC cambiará su selección de NIC para utilizar la NIC dedicada. Si no se detecta ningún vínculo en la NIC dedicada, iDRAC utiliza la LOM compartida. El cambio del tiempo de espera de compartida a dedicada es de 5 segundos y de dedicada a compartida es de 30 segundos. Es posible configurar este valor de tiempo de espera mediante RACADM o WS-MAN.

Para obtener información acerca de los distintos campos, consulte la *Ayuda en línea de iDRAC*.

Modificación de la configuración de red mediante RACADM local

Para generar una lista de las propiedades de red disponibles, escriba lo siguiente:

 **NOTA:** Es posible usar los comandos **getconfig** y **config** o los comandos **get** y **set** con los objetos RACADM.

- Mediante el comando **getconfig**: `racadm getconfig -g cfgLanNetworking`
- Mediante el comando **get**: `racadm get iDRAC.Nic`

Para utilizar DHCP para obtener una dirección IP, utilice el siguiente comando para escribir el objeto **cfgNicUseDhcp** o **DHCPEnable** y activar esta función:

- Mediante el comando **config**: `racadm config -g cfgLanNetworking -o cfgNicUseDHCP 1`
- Mediante el comando **set**: `racadm set iDRAC.IPv4.DHCPEnable 1`

El siguiente es un ejemplo de cómo se pueden utilizar los comandos para configurar las propiedades de la red LAN necesarias.


- Mediante el comando **config**:

```
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 MYDOMAIN
```

- Mediante el comando **set**:

```
racadm set iDRAC.Nic.Enable 1 racadm set iDRAC.IPv4.Address 192.168.0.120
racadm set iDRAC.IPv4.Netmask 255.255.255.0 racadm set iDRAC.IPv4.Gateway
192.168.0.120 racadm set iDRAC.IPv4.DHCPEnable 0 racadm set
iDRAC.IPv4.DNSFromDHCP 0 racadm set iDRAC.IPv4.DNS1 192.168.0.5 racadm set
iDRAC.IPv4.DNS2 192.168.0.6 racadm set iDRAC.Nic.DNSRegister 1 racadm set
iDRAC.Nic.DNSRacName RAC-EK00002 racadm set iDRAC.Nic.DNSDomainFromDHCP 0
racadm set iDRAC.Nic.DNSDomainName MYDOMAIN
```


 **NOTA:** Si `cfgNicEnable` o `iDRAC.Nic.Enable` están configurados con el valor **0**, la LAN de iDRAC se desactivará aún cuando DHCP esté activado.


Configuración del filtrado de IP

Además de la autenticación de usuario, utilice las siguientes opciones para proporcionar seguridad adicional mientras accede a iDRAC:

- El filtrado de IP limita el rango de direcciones IP de los clientes que acceden a iDRAC. Compara la dirección IP de un inicio de sesión entrante con el rango especificado y solo permite el acceso a iDRAC desde una estación de administración cuya dirección IP se encuentre dentro de dicho rango. Todas las demás solicitudes de inicio de sesión se deniegan.
- Cuando se producen fallas repetidas de inicio de sesión desde una dirección IP específica, se impide el inicio de sesión de esa dirección en iDRAC durante un lapso de tiempo predefinido. Si intenta iniciar sesión sin éxito dos veces, se le permitirá iniciar sesión nuevamente recién después de 30 segundos. Si intenta iniciar sesión sin éxito más de dos veces, se le permitirá iniciar sesión nuevamente recién después de 60 segundos.

A medida que se acumulen fallas de inicio de sesión de una dirección IP concreta, estos se registran mediante un contador interno. Cuando el usuario inicie sesión correctamente, el historial de fallos se borrará y el contador interno se restablecerá.

 **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: `ssh exchange identification: Connection closed by remote host.`

 **NOTA:** Si utiliza Dell Deployment Toolkit (DTK), consulte la *Dell Deployment Toolkit User's Guide* (Guía del usuario de Dell Deployment Toolkit) para conocer los privilegios.

Configuración del filtrado IP mediante la interfaz web de iDRAC

Debe disponer del privilegio Configurar para realizar estos pasos.

Para configurar el filtrado de IP:

1. En la interfaz web de iDRAC, vaya a **Información general** → **Configuración de iDRAC** → **Red** → **Red**. Aparecerá la página **Red**.
2. Haga clic en **Configuración avanzada**. Se muestra la página **Seguridad de la red**.
3. Especifique la configuración de filtrado de IP. Para obtener más información acerca de estas opciones, consulte la *Ayuda en línea de iDRAC*.
4. Haga clic en **Aplicar** para guardar la configuración.

Configuración del filtrado de IP mediante RACADM

Debe disponer del privilegio Configurar para realizar estos pasos.

Para configurar el filtrado de IP, utilice los siguientes objetos RACADM:

- Con el comando **config**:
 - `cfgRacTuneIpRangeEnable`
 - `cfgRacTuneIpRangeAddr`
 - `cfgRacTuneIpRangeMask`
- Con el comando **set**, utilice los objetos del grupo **iDRAC.IPBlocking**:
 - `RangeEnable`
 - `RangeAddr`
 - `RangeMask`

La propiedad `cfgRacTuneIpRangeMask` o **RangeMask** se aplica a la dirección IP entrante y a la propiedad `cfgRacTuneIpRangeAddr` o **RangeAddr**. Si los resultados son idénticos, se le permite el acceso a iDRAC a la solicitud de inicio de sesión entrante. Si se inicia sesión desde una dirección IP fuera de este rango, se producirá un error.

El inicio de sesión continúa si el valor de la siguiente expresión es igual a cero:

- Mediante la sintaxis heredada: `cfgRacTuneIpRangeMask & (<dirección IP entrante> ^ cfgRacTuneIpRangeAddr)`
- Mediante la nueva sintaxis: `RangeMask & (<dirección IP entrante> ^ RangeAddr)`

donde `&` es el operador Y a nivel de bits de las cantidades y `^` es el operador O exclusivo a nivel de bits.

Ejemplos del filtrado IP

- Los siguientes comandos de RACADM bloquean todas las direcciones IP, excepto la dirección 192.168.0.57:
 - Mediante el comando **config**:

```
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
```
 - Mediante el comando **set**:

```
racadm set iDRAC.IPBlocking.RangeEnable 1 racadm set iDRAC.IPBlocking.RangeAddr 192.168.0.57 racadm set iDRAC.IPBlocking.RangeMask 255.255.255.255
```
- Para restringir los inicios de sesión a un conjunto de cuatro direcciones IP adyacentes (por ejemplo, de 192.168.0.212 a 192.168.0.215), seleccione todo excepto los últimos dos bits de la máscara:
 - Mediante el comando **set**:

```
racadm set iDRAC.IPBlocking.RangeEnable 1 racadm set iDRAC.IPBlocking.RangeAddr 192.168.0.212 racadm set iDRAC.IPBlocking.RangeMask 255.255.255.252
```

El último byte de la máscara de rango está establecido en 252, el equivalente decimal de 11111100b.

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

Configuración de servicios

Puede configurar y activar los siguientes servicios en iDRAC:

- Configuración local: desactive el acceso a la configuración de iDRAC (desde el sistema host) mediante RACADM local y la utilidad de configuración de iDRAC.
- Web Server: permita el acceso a la interfaz web de iDRAC. Si desactiva la opción, utilice RACADM local para volver a activar el servidor web, ya que si lo desactiva también desactivará RACADM remoto.
- SSH: acceda a iDRAC a través del firmware RACADM.
- Telnet: acceda a iDRAC a través del firmware RACADM.
- RACADM remoto: acceda a iDRAC de forma remota.
- Agente SNMP: admite consultas SNMP (operaciones GET, GETNEXT y GETBULK) en iDRAC.
- Agente de recuperación automatizado del sistema: active la pantalla de último bloqueo del sistema.
- Servidor VNC: active el servidor VNC con o sin el cifrado SSL.

Configuración de servicios mediante la interfaz web

Para configurar los servicios mediante la interfaz web de iDRAC:

1. En la interfaz web de iDRAC, vaya a **Información general** → **Configuración de iDRAC** → **Red** → **Servicios**.
Aparecerá la página **Servicios de directorio**.
2. Especifique la información necesaria y haga clic en **Aplicar**.
Para obtener información acerca de los distintos valores, consulte la *Ayuda en línea de iDRAC*.

Configuración de servicios mediante RACADM

Para activar y configurar los diversos servicios mediante RACADM:

- Utilice los objetos siguientes con el comando **config**:
 - `cfgRacTuneLocalConfigDisable`
 - `cfgRacTuneCtrlEConfigDisable`
 - `cfgSerialSshEnable`
 - `cfgRacTuneSshPort`
 - `cfgSsnMgtSshIdleTimeout`
 - `cfgSerialTelnetEnable`
 - `cfgRacTuneTelnetPort`
 - `cfgSsnMgtTelnetIdleTimeout`
 - `cfgRacTuneWebserverEnable`
 - `cfgSsnMgtWebserverTimeout`
 - `cfgRacTuneHttpPort`
 - `cfgRacTuneHttpsPort`
 - `cfgRacTuneRemoteRacadmEnable`

- cfgSsnMgtRacadmTimeout
- cfgOobSnmpAgentEnable
- cfgOobSnmpAgentCommunity
- Utilice los objetos de los siguientes grupos de objetos con el comando **set**:
 - iDRAC.LocalSecurity
 - iDRAC.LocalSecurity
 - iDRAC.SSH
 - iDRAC.Websserver
 - iDRAC.Telnet
 - iDRAC.Racadm
 - iDRAC.SNMP

Para obtener más información sobre estos objetos, consulte *iDRAC8 RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8), disponible en dell.com/support/manuals.

Activación o desactivación de la redirección de HTTPs

Si no desea la redirección automática de HTTP a HTTPs debido a un problema de aviso de certificado con el certificado de iDRAC predeterminado o como configuración temporal para fines de depuración, puede configurar el iDRAC de manera tal que la redirección del puerto http (el predeterminado es 80) al puerto https (el predeterminado es el 443) esté desactivada. Está activada de manera predeterminada. Debe cerrar sesión e iniciar sesión en el iDRAC para que esta configuración surta efecto. Al desactivar esta función, se mostrará un mensaje de advertencia.

Debe tener privilegio de Configurar el iDRAC para activar o desactivar la redirección de HTTPs.

Cuando se activa o desactiva esta función, se graba un suceso en el archivo de registro de Lifecycle Controller.

Para desactivar la redirección de HTTP a HTTPs:

```
racadm set iDRAC.Websserver.HttpsRedirection Disabled
```

Para activar la redirección de HTTP a HTTPs:

```
racadm set iDRAC.Websserver.HttpsRedirection Enabled
```


Para ver el estado de la redirección de HTTP a HTTPs:

```
racadm get iDRAC.Websserver.HttpsRedirection
```

Uso del cliente de VNC Client para administrar el servidor remoto

Puede utilizar un cliente de VNC de estándar abierto para administrar el servidor remoto mediante dispositivos de escritorio y móviles, como Dell Wyse PocketCloud. Cuando los servidores de los centros de datos dejan de funcionar, el iDRAC o el sistema operativo envían una alerta a la consola en la estación de administración. La consola luego envía un mensaje de correo electrónico o un SMS a un dispositivo móvil con la información requerida e inicia la aplicación del visor de VNC en la estación de administración. Este visor de VNC puede conectarse con el sistema operativo/hipervisor en el servidor y proporcionar acceso al teclado, video y mouse del servidor host para realizar las reparaciones necesarias. Antes de iniciar el cliente de VNC, debe activar el servidor VNC y configurar sus valores en iDRAC, como

contraseña, número de puerto VNC, cifrado de SSL y el valor del tiempo de espera. Puede configurar estos valores mediante la interfaz web de iDRAC o RACADM.

 **NOTA:** La función de VNC está sujeta a licencia y se encuentra disponible en la licencia Enterprise de iDRAC.

Puede elegir entre muchas aplicaciones de VNC o clientes de escritorio, como los de RealVNC o Dell Wyse PocketCloud.

Solo puede haber una sesión de cliente de VNC activa al mismo tiempo.

Si hay una sesión de VNC activa, solo podrá ejecutar los medios virtuales a través de la opción Iniciar consola virtual, no con Virtual Console Viewer.

Si el cifrado de video está desactivado, el cliente de VNC inicia un protocolo de enlace directamente y no se necesita un protocolo de enlace de SSL. Durante el protocolo de enlace del cliente de VNC (RFB o SSL), si hay otra sesión de VNC activa o si hay una sesión de Consola virtual abierta, se rechaza la sesión nueva del cliente de VNC. Después de finalizar el primer protocolo de enlace, el servidor VNC desactiva la consola virtual y permite solo los medios virtuales. Una vez concluida la sesión de VNC, el servidor de VNC restaura el estado original de la consola virtual (activado o desactivado).

 **NOTA:**

- Cuando la NIC de iDRAC se encuentra en modo compartido y se ejecuta un ciclo de apagado y encendido en el sistema host, se pierde la conexión de red durante unos segundos. Durante este lapso, si no se lleva a cabo ninguna acción en el cliente de VNC activo, la sesión de VNC puede cerrarse. Debe esperar a que se acabe el tiempo de espera (el valor establecido en la configuración del servidor VNC en la página **Servicios** de la interfaz web de iDRAC) y, a continuación, volver a establecer la conexión de VNC.
- La ventana del cliente de VNC se cierra si se minimiza durante más de 60 segundos y debe abrir una nueva sesión de VNC. Si maximiza la ventana del cliente de VNC antes de que transcurran los 60 segundos, puede continuar utilizando dicho cliente.

Configuración del servidor VNC mediante la interfaz web del iDRAC

Para configurar los valores del servidor VNC:


1. En la interfaz web de iDRAC, vaya a **Información general** → **Configuración de iDRAC** → **Red** → **Servicios**.
Aparecerá la página **Servicios de directorio**.
2. En la sección **Servidor VNC**, active el servidor VNC, especifique la contraseña, el número de puerto y active o desactive el cifrado SSL.
Para obtener información acerca de los campos, consulte la *Ayuda en línea de iDRAC*.
3. Haga clic en **Apply (Aplicar)**.
El servidor VNC está configurado.

Configuración del servidor VNC mediante RACADM

Para configurar el servidor VNC, utilice el objeto `VNCserver` con el comando `set`. Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8), disponible en dell.com/support/manuals.

Configuración del visor VNC sin Cifrado SSL

Al configurar los valores del servidor VNC en el iDRAC, si la opción **Cifrado SSL** está activada, entonces la aplicación de túnel SSL debe usarse junto con el visor VNC para establecer la conexión cifrada con el servidor VNC del iDRAC.

 **NOTA:** La mayoría de los clientes VNC no tienen el soporte incorporado en el cifrado SSL.

Para configurar la aplicación de túnel SSL:

1. Configure el túnel SSL para aceptar la conexión en `<localhost>:<localport number>`. Por ejemplo, 127.0.0.1:5930.
2. Configure el túnel SSL para conectarse a `<iDRAC IP address>:<VNC server port Number>`. Por ejemplo, 192.168.0.120:5901.
3. Inicie la aplicación de túnel.

Para establecer la conexión con el servidor VNC del iDRAC en el canal de cifrado SSL, conecte el visor VNC al host local (dirección IP local de vínculo) y el número de puerto local (127.0.0.1: <número de puerto local>).

Configuración del visor VNC sin Cifrado SSL

En general, todos de búfer de tramas remoto (RFB) compatible con los visores VNC se conectan al servidor VNC utilizando la dirección IP del iDRAC y el número de puerto que se ha configurado para el servidor VNC. Si la opción de cifrado SSL está desactivada en el momento de configurar los valores del servidor VNC en el iDRAC, entonces para conectarse al visor VNC haga lo siguiente:

En el cuadro de diálogo **Visor VNC**, introduzca la dirección IP del iDRAC y número de puerto VNC en el campo **Servidor VNC**.

El formato es `<iDRAC IP address:VNC port number>`

Por ejemplo, si la dirección IP del iDRAC es 192.168.0.120 y el número de puerto VNC es 5901, entonces introduzca `192.168.0.120:5901`.

Configuración del panel frontal

Puede configurar el LCD del panel frontal y la visualización de indicadores LED para el sistema administrado.

Para servidores tipo bastidor y torre, hay dos paneles frontales disponibles:

- Panel frontal de LCD y LED de ID del sistema
- Panel frontal de LED y LED de ID del sistema

Para servidores Blade, solo el LED de ID del sistema está disponible en el panel frontal del servidor, ya que el chasis del servidor Blade contiene la pantalla LCD.

Enlaces relacionados

[Configuración de los valores de LCD](#)

[Configuración del valor LED del Id. del sistema](#)

Configuración de los valores de LCD

Puede definir y mostrar una cadena predeterminada, tal como un nombre de iDRAC, una dirección IP, etc. o una cadena definida por el usuario en el panel frontal del sistema administrado.

Configuración de los valores LCD mediante la interfaz web

Para configurar la pantalla de panel anterior LCD del servidor:

1. En la interfaz web de iDRAC, vaya a **Información general** → **Hardware** → **Panel frontal**.
2. En la sección **Configuración de LCD**, en el menú desplegable **Configurar mensaje de inicio** seleccione cualquiera de los elementos siguientes:
 - Etiqueta de servicio (predeterminado)
 - Etiqueta de propiedad
 - Dirección MAC de DRAC
 - Dirección IPv4 de DRAC
 - Dirección IPv6 de DRAC
 - Alimentación del sistema
 - Temperatura ambiente
 - Modelo del sistema
 - Nombre del host
 - Definido por el usuario
 - Ninguno

Si selecciona **Definido por el usuario**, introduzca el mensaje necesario en el cuadro de texto.

Si selecciona **Ninguno**, el mensaje de inicio no se muestra en el panel frontal del LCD.
3. Active la indicación de la consola virtual (opcional). Una vez activada, la sección Fuente en directo del panel frontal y el panel LCD del servidor mostrarán el mensaje `Virtual console session active` cuando haya una sesión de consola virtual activa.
4. Haga clic en **Apply (Aplicar)**.

El panel frontal del LCD muestra el mensaje de inicio configurado.

Configuración de los valores LCD mediante RACADM

Para configurar la pantalla LCD del panel frontal del servidor, utilice los objetos en el grupo **System.LCD**. Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8), disponible en dell.com/support/manuals.

Configuración de LCD mediante la utilidad de configuración de iDRAC

Para configurar la pantalla de panel anterior LCD del servidor:

1. En la utilidad de configuración de iDRAC, vaya a **Seguridad del panel frontal**.

Se mostrará la página **Configuración de iDRAC - Seguridad del panel frontal**.
2. Active o desactive el botón de encendido.
3. Especifique lo siguiente:
 - Acceso al panel frontal
 - Cadena de mensajes de LCD

- Unidades de alimentación del sistema, unidades de temperatura ambiente y visualización de errores
4. Active o desactive la indicación de consola virtual.
Para obtener información acerca de las opciones, consulte la *Ayuda en línea de la utilidad de configuración de iDRAC*.
 5. Haga clic en **Atrás**, en **Terminar** y, a continuación, en **Sí**.

Configuración del valor LED del Id. del sistema

Para identificar un servidor, active o desactive el parpadeo de LED del ID del sistema administrado.

Configuración del valor LED de Id. del sistema mediante la interfaz web

Para configurar la visualización de LED de ID del sistema:

1. En la interfaz web de iDRAC, vaya a **Información general** → **Hardware** → **Panel frontal**. Aparecerá la página **Panel frontal**.
2. En la sección **Configuración de LED de ID del sistema**, seleccione cualquier de las opciones siguientes para activar o desactivar el parpadeo de LED:
 - Desactivar parpadeo
 - Activar parpadeo
 - Activar parpadeo del tiempo de espera de 1 día
 - Activar parpadeo del tiempo de espera de 1 semana
 - Activar parpadeo del tiempo de espera de 1 mes
3. Haga clic en **Apply (Aplicar)**.
Se habrá configurado el parpadeo de LED en el panel frontal.

Configuración del valor LED de Id. del sistema mediante RACADM

Para configurar el LED de identificación del sistema, utilice el comando **setled**. Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8), disponible en dell.com/support/manuals.

Configuración de zona horaria y NTP

Es posible configurar la zona horaria en iDRAC y sincronizar la hora de iDRAC mediante el de hora de red (NTP) en lugar de las horas de BIOS o del sistema host.

Debe contar con el privilegio Configurar para establecer la zona horaria o los parámetros de NTP.

Configuración de zona horaria y NTP mediante la interfaz web de iDRAC

Para configurar la zona horaria y NTP mediante la interfaz web de iDRAC:

1. Vaya a **Descripción general** → **Configuración de iDRAC** → **Propiedades** → **Configuración**.
Se mostrará la página **Zona horaria y NTP**.
2. Para configurar la zona horaria, en el menú desplegable **Zona horaria**, seleccione la zona horaria requerida y haga clic en **Aplicar**.
3. Para configurar NTP, active NTP, introduzca las direcciones del servidor NTP y haga clic en **Aplicar**.
Para obtener información sobre los campos, consulte la *Ayuda en línea de iDRAC*.

Configuración de zona horaria y NTP mediante RACADM

Para configurar la zona horaria y NTP mediante RACADM, utilice los objetos de los grupos **iDRAC.Time** e **iDRAC.NTPConfigGroup** con el comando **set**. Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8), disponible en dell.com/support/manuals.

Configuración del primer dispositivo de inicio

Puede configurar el primer dispositivo de inicio solo para el siguiente inicio o para todos los reinicios subsiguientes. Según esta selección, puede establecer el primer dispositivo de inicio para el sistema. El sistema se inicia desde el dispositivo seleccionado la próxima vez y todos los reinicios subsiguientes, y permanece como el primer dispositivo en el orden de inicio del BIOS hasta que se vuelva a cambiar esta opción en la interfaz web de iDRAC o en la secuencia de inicio del BIOS. Puede configurar el primer dispositivo de inicio con una de las siguientes opciones:

- Inicio normal
- PXE
- Configuración del BIOS
- Disco flexible local/unidades extraíbles principales
- CD/DVD local
- Unidad de disco duro
- Disco flexible virtual
- Virtual CD/DVD/ISO
- Tarjeta SD local
- vFLASH
- Lifecycle Controller
- BIOS Boot Manager

NOTA:

- Configuración del BIOS (F2), Lifecycle Controller (F10) y BIOS Boot Manager (F11) solo admiten el inicio una vez activado.
- La consola virtual no admite la configuración de inicio de manera permanente. Se inicia siempre una vez.
- La configuración del primer dispositivo de inicio en la interfaz web de iDRAC invalida la configuración de inicio del BIOS del sistema.

Configuración del primer dispositivo de inicio mediante la interfaz web

Para establecer el primer dispositivo de inicio mediante la interfaz web de iDRAC:

1. Vaya a **Información general** → **Servidor** → **Configuración** → **Primer dispositivo de inicio**. Aparece la pantalla **Primer dispositivo de inicio**.
2. Seleccione el primer dispositivo de inicio necesario de la lista desplegable y haga clic en **Aplicar**. El sistema se reinicia desde el dispositivo seleccionado para los reinicios subsiguientes.
3. Para iniciar desde el dispositivo seleccionado solo una vez durante el siguiente inicio, seleccione **Inicio único**. A partir de entonces, el sistema se iniciará desde el primer dispositivo de inicio según el orden de inicio del BIOS.

Para obtener más información acerca de estas opciones, consulte la *Ayuda en línea de iDRAC*.

Configuración del primer dispositivo de inicio mediante RACADM

- Para establecer el primer dispositivo de inicio, utilice el objeto **cfgServerFirstBootDevice**.
- Para activar el inicio único de un dispositivo, utilice el objeto **cfgServerBootOnce**.

Para obtener más información sobre estos objetos, consulte *iDRAC8 RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8), disponible en dell.com/support/manuals.

Configuración del primer dispositivo de inicio mediante la consola virtual

Es posible seleccionar el dispositivo desde el que se realizará el inicio debido a que el servidor se ve en el visor de la consola virtual antes de que funcione a través de su secuencia de inicio. Puede realizar el inicio una vez en todos los dispositivos admitidos que se muestran en [Configuración del primer dispositivo de inicio](#).

Para configurar el primer dispositivo de inicio mediante la consola virtual:

1. Inicie la consola virtual.
2. En el visor de la consola virtual, en el menú **Siguiente inicio**, configure el dispositivo requerido como el primer dispositivo de inicio.

Activación de la pantalla de último bloqueo

Para buscar la causa de un bloqueo del sistema administrado, puede capturar una imagen de bloqueo del sistema mediante iDRAC.

Para activar la pantalla de último bloqueo:

1. En el DVD *Herramientas y documentación de Dell Systems Management*, instale Server Administrator en el sistema administrado.
Para obtener más información, consulte *Dell OpenManage Server Administrator Installation Guide* (Guía de instalación de Dell OpenManage Server Administrator) disponible en dell.com/support/manuals.
2. En la ventana de inicio y recuperación de **Windows**, asegúrese de que la opción de reinicio automático no esté activada.
Para obtener más información, consulte la documentación de Windows.
3. Utilice Server Administrator para activar el temporizador **Recuperación automática**, establezca la acción de recuperación automática en **Restablecer**, **Apagado** o **Ciclo de encendido** y establezca el temporizador en segundos (un valor entre 60 y 480).
Para obtener más información, consulte *Dell OpenManage Server Administrator Installation Guide* (Guía de instalación de Dell OpenManage Server Administrator) disponible en dell.com/support/manuals.
4. Active la opción **Apagado y recuperación automática** (ASR) mediante uno de los procedimientos siguientes:
 - Server Administrator: consulte *Dell OpenManage Server Administrator User's Guide* (Guía del usuario de Dell OpenManage Server Administrator) disponible en dell.com/support/manuals.
 - RACADM local: utilice el comando siguiente.

```
racadm config -g cfgRacTuning -o cfgRacTuneAsrEnable 1
```
5. Active la opción **Agente de recuperación automatizado del sistema**. Para ello, vaya a **Información general** → **Configuración de iDRAC** → **Red** → **Servicios**, seleccione **Activado** y haga clic en **Aplicar**.

Activación o desactivación del paso del sistema operativo a iDRAC

En los servidores que cuentan con dispositivos de tarjeta secundaria de red (NDC) o LAN en la placa base (LOM) incorporada, es posible activar la función Paso del sistema operativo a iDRAC, que proporciona una comunicación dentro de banda bidireccional de alta velocidad entre iDRAC y el sistema operativo host a través de una LOM compartida (servidores tipo bastidor o torre), una NIC dedicada (servidores tipo bastidor, torre o blade) o a través de la NIC de USB. Esta función está disponible para la licencia iDRAC Enterprise.

Cuando esta opción se encuentra activada a través de una NIC dedicada, es posible iniciar el explorador en el sistema operativo host y acceder a la interfaz web de iDRAC. La NIC queda dedicada para los servidores blade a través de Chassis Management Controller.

Alternar entre una NIC dedicada o una LOM compartida no requiere reinicios o restablecimientos del sistema operativo host o iDRAC.

Es posible activar este canal mediante las siguientes opciones:

- Interfaz web del iDRAC
- RACADM o WS-MAN (entorno posterior a la carga del sistema operativo)
- Utilidad de configuración de iDRAC (entorno previo al sistema operativo)

Si la configuración de red se cambia a través de la interfaz web de iDRAC, debe esperar al menos 10 segundos antes de activar el paso del sistema operativo a iDRAC.

Si utiliza el archivo de configuración XML a través de RACADM o WS-MAN y si se cambia la configuración de la red en este archivo, debe esperar 15 segundos para activar la función "Paso del sistema operativo a iDRAC" o para establecer la dirección IP del sistema operativo host.

Antes de activar el paso del sistema operativo a iDRAC, asegúrese de lo siguiente:

- El iDRAC está configurado para utilizar NIC dedicada o modo compartido (es decir, la selección de NIC está asignada a una de las LOM).
- El sistema operativo host e iDRAC se encuentran en la subred y la misma VLAN.
- La dirección IP del sistema operativo host está configurada.
- Una tarjeta que admite la función Paso del sistema operativo al iDRAC está instalada.
- Dispone del privilegio Configurar.

Cuando active esta función:

- En el modo compartido, se utiliza la dirección IP del sistema operativo host.
- En el modo dedicado, debe proporcionar una dirección IP válida del sistema operativo host. Si hay más de una LOM activa, introduzca la primera dirección IP de la LOM.

Si después de activar la función Paso del sistema operativo a iDRAC, el canal no funciona:

- Compruebe si el cable de la NIC dedicada de iDRAC está conectado correctamente.
- Asegúrese de que al menos una LOM esté activa.

Enlaces relacionados

[Tarjetas admitidas para el paso del sistema operativo al iDRAC](#)

[Sistemas operativos admitidos para la NIC de USB](#)

[Activación o desactivación del paso del sistema operativo a iDRAC mediante la interfaz web](#)

[Activación o desactivación del paso del sistema operativo a iDRAC mediante RACADM](#)

[Activación o desactivación del paso del sistema operativo a iDRAC mediante la utilidad de configuración de iDRAC](#)

Tarjetas admitidas para el paso del sistema operativo al iDRAC

La siguiente tabla proporciona una lista de las tarjetas que admiten la función Paso del sistema operativo al iDRAC mediante LOM.

Tabla 7. :Paso del sistema operativo al iDRAC mediante LOM: tarjetas admitidas

Categoría	Fabricante	Tipo
NDC	Broadcom	<ul style="list-style-type: none">• 5720 QP rNDC 1G BASE-T• 57810S DP bNDC KR• 57800S QP rNDC (10G BASE-T + 1G BASE-T)• 57800S QP rNDC (10G SFP+ + 1G BASE-T)• 57840 4x10G KR.• 57840 rNDC
	Intel	<ul style="list-style-type: none">• i540 QP rNDC (10G BASE-T + 1G BASE-T)• i350 QP rNDC 1G BASE-T• x520/i350 rNDC de 1GB
	QLogic	QMD8262 Blade NDC

Las tarjetas LOM integradas también admiten la función Paso del sistema operativo al iDRAC.

Las tarjetas siguientes no admiten la función Paso del sistema operativo a iDRAC:

- Intel de 10 GB NDC.
- Intel rNDC con dos controladoras: las controladoras de 10G no admiten.
- Qlogic bNDC
- Tarjetas PCIe, mezzanine y de interfaz de red.

Sistemas operativos admitidos para la NIC de USB

Los sistemas operativos admitidos para la NIC de USB son:

- Windows Server 2008 SP2 (64 bits)
- Windows Server 2008 SP2 R2 (64 bits)
- Windows Server 2012 SP1
- SLES 10 SP4 (64 bits)
- SLES 11 SP2 (64 bits)
- RHEL 5.9 (32 bits y 64 bits)
- RHEL 6.4
- vSphere v5.0 U2 ESXi
- vSphere v5.1 U1 ESXi
- vSphere v5.5 ESXi

En los servidores con sistema operativo Windows 2008 SP2 de 64 bits, el dispositivo USC del CD virtual del iDRAC no se detecta (o activa) automáticamente. Debe activarlo manualmente. Para obtener más información, consulte los pasos recomendados por Microsoft para actualizar manualmente el controlador Remote Network Driver Interface Specification (RNDIS) para este dispositivo.

Para los sistemas operativos Linux, configure la NIC de USB como DHCP en el sistema operativo host antes de activar la NIC de USB.

Si el sistema operativo del host es SUSE Linux Enterprise Server 11, después de activar la NIC de USB en el iDRAC, deberá activar manualmente el cliente DHCP en el sistema operativo host. Para obtener información para activar DHCP, consulte los documentos para los sistemas operativos SUSE Linux Enterprise Server 11.

En vSphere, debe instalar el archivo VIB antes de activar la NIC de USB.

En el caso de los siguientes sistemas operativos, si instala los paquetes Avahi y nss-mdns, puede utilizar <https://idrac.local> para iniciar el iDRAC desde el sistema operativo host. Si estos paquetes no están instalados, utilice <https://169.254.0.1> para iniciar el iDRAC.

Sistema operativo	Estado del servidor de seguridad	Paquete Avahi	Paquete nss-mdns
RHEL 5.9 de 32 bits	Desactiva r	Instale como un paquete independiente (avahi-0.6.16-10.el5_6.i386.rpm)	Instale como un paquete independiente (nss-mdns-0.10-4.el5.i386.rpm)
RHEL 6.4 de 64 bits	Desactiva r	Instale como un paquete independiente (avahi-0.6.25-12.el6.x86_64.rpm)	Instale como un paquete independiente (nss-mdns-0.10-8.el6.x86_64.rpm)
SLES 11 SP3 de 64 bits	Desactiva r	El paquete Avahi es la parte del DVD del sistema operativo	nss-mdns se instala al instalar Avahi

En el sistema host, al instalar el sistema operativo RHEL 5.9, el modo de paso de la NIC de USB está desactivado. Si se activa una vez finalizada la instalación, la interfaz de red correspondiente al dispositivo NIC USB no se activa automáticamente. Puede realizar cualquiera de las siguientes para activar el dispositivo NIC USB:

- Configure la interfaz de la NIC de USB con la herramienta Network Manager. Vaya a **Sistema** → **Administrador** → **Red** → **Dispositivos** → **Nuevo** → **Conexión de Ethernet** y seleccione **Dell computer corp.iDRAC Virtual NIC USB Device**. Haga clic en el icono Activar para activar el dispositivo. Para obtener más información, consulte la documentación de RHEL 5.9.
- Cree el archivo de configuración correspondiente a la interfaz como **ifcfg-ethX** en el directorio **/etc/sysconfig/network-script/**. Agregue las anotaciones básicas DEVICE, BOOTPROTO, HWADDR, ONBOOT. Agregue TYPE en el archivo **ifcfg-ethX** y reinicie los servicios de red mediante el comando `service network restart`.
- Reinicie el sistema.
- Apague y encienda el sistema.

En sistemas con el sistema operativo RHEL 5.9, si se desactivó la NIC de USB y usted apaga el sistema o viceversa, cuando el sistema se enciende y si la NIC de USB está activada, el dispositivo NIC USB no se

activa automáticamente. Para activarlo, compruebe que haya algún archivo **ifcfg-ethX.bak** disponible en el directorio **/etc/sysconfig/network-script** para la interfaz de la NIC de USB. Si está disponible, cambie el nombre a **ifcfg-ethX** y luego utilice el comando `ifup ethX`.

Enlaces relacionados

[Instalación del archivo VIB](#)

Instalación del archivo VIB

Para los sistemas operativos vSphere, antes de activar la NIC de USB debe instalar el archivo VIB.

Para instalar el archivo VIB:

1. Mediante Win-SCP, copie el archivo VIB a la carpeta **/tmp/** del sistema operativo host ESX-i.
2. Vaya al símbolo de ESXi y ejecute el siguiente comando:

```
esxcli software vib install -v /tmp/ iDRAC_USB_NIC-1.0.0-799733X03.vib --no-sig-check
```

El resultado es:

```
Message: The update completed successfully, but the system needs to be
rebooted for the changes to be effective. Reboot Required: true VIBs
Installed: Dell_bootbank_iDRAC_USB_NIC_1.0.0-799733X03 VIBs Removed: VIBs
Skipped:
```

3. Reinicie el servidor.
4. A petición de ESXi, ejecute el comando: `esxconfig-vmknics -l`.


El resultado muestra la anotación `usb0`.

Activación o desactivación del paso del sistema operativo a iDRAC mediante la interfaz web

Para activar el paso del sistema operativo a iDRAC mediante la interfaz web:

1. Vaya a **Descripción general** → **Configuración de iDRAC** → **Red** → **Paso del sistema operativo a iDRAC**.
Se mostrará la página **Paso del sistema operativo a iDRAC**.
2. Seleccione cualquiera de las siguientes opciones para activar el paso del sistema operativo al iDRAC:
 - **LOM**: el vínculo de paso del sistema operativo al iDRAC entre el iDRAC y el sistema operativo host se establece mediante la LOM o NDC.
 - **NIC de USB**: el vínculo de paso del sistema operativo al iOS entre el iDRAC y el sistema operativo host se establece mediante la DRAC o USB.

Para desactivar esta función, seleccione **Desactivado**.

3. Si selecciona **LOM** como configuración de paso, y si el servidor está conectado mediante el modo dedicado, introduzca la dirección IPv4 del sistema operativo.
 **NOTA:** Si el servidor está conectado en el modo LOM compartido, el campo **Dirección IP del sistema operativo** estará desactivado.
4. Si selecciona **NIC de USB** como configuración del paso, introduzca la dirección IP de la NIC de USB. El valor predeterminado es 169.254.0.1. Se recomienda utilizar la dirección IP predeterminada. Sin embargo, si esta dirección IP entra en conflicto con una dirección IP de otras interfaces del sistema host o la red local, deberá cambiarla.

No introduzca las IP 169.254.0.3 y 169.254.0.4. Estas IP están reservadas para el puerto de la NIC de USB en el panel frontal cuando se utiliza un cable A/A.

5. Haga clic en **Aplicar** para aplicar la configuración.
6. Haga clic en **Probar configuración de la red** para comprobar si la IP es accesible y si el vínculo está establecido entre iDRAC y el sistema operativo host.

Activación o desactivación del paso del sistema operativo a iDRAC mediante RACADM

Para activar o desactivar el paso del sistema operativo a iDRAC mediante RACADM, utilice los objetos en el grupo **iDRAC.OS-BMC**. Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8), disponible en dell.com/support/manuals.

Activación o desactivación del paso del sistema operativo a iDRAC mediante la utilidad de configuración de iDRAC

Para activar o desactivar el paso del sistema operativo a iDRAC mediante la utilidad de configuración de iDRAC:

1. En la utilidad de configuración de iDRAC, vaya a **Permisos de comunicaciones**. Aparecerá la página **Configuración de los permisos de comunicaciones de iDRAC**.
2. Seleccione cualquiera de las siguientes opciones para activar el paso del sistema operativo al iDRAC:
 - **LOM**: el vínculo de paso del sistema operativo al iDRAC entre el iDRAC y el sistema operativo host se establece mediante la LOM o NDC.
 - **NIC de USB**: el vínculo de paso del sistema operativo al iDRAC entre el iDRAC y el sistema operativo host se establece mediante la DRAC o USB.

Para desactivar esta función, seleccione **Desactivado**.



NOTA: Solo se puede seleccionar la opción LOM si la tarjeta admite la función Paso del sistema operativo al iDRAC. De lo contrario, esta opción aparece en gris.

3. Si selecciona **LOM** como configuración de paso, y si el servidor está conectado mediante el modo dedicado, introduzca la dirección IPv4 del sistema operativo.




NOTA: Si el servidor está conectado en el modo LOM compartido, el campo **Dirección IP del sistema operativo** estará desactivado.

4. Si selecciona **NIC de USB** como configuración del paso, introduzca la dirección IP de la NIC de USB. El valor predeterminado es 169.254.0.1. Sin embargo, si esta dirección IP entra en conflicto con una dirección IP de otras interfaces del sistema host o la red local, debe cambiarla. No introduzca las IP 169.254.0.3 y 169.254.0.4. Estas IP están reservadas para el puerto de la NIC de USB en el panel frontal cuando se utiliza un cable A/A.
5. Haga clic en **Atrás**, en **Terminar** y, a continuación, en **Sí**. Se guardarán los detalles.

Obtención de certificados

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

Tabla 8. Tipos de certificado basados en el tipo de inicio de sesión

Tipo de inicio de sesión	Tipo de certificado	Cómo obtenerlo
Inicio de sesión único mediante Active Directory	Certificado de CA de confianza	<p>Generar una CSR y hacer que la firme una autoridad de certificados</p> <p>También se admiten los certificados SHA-2.</p>
Inicio de sesión mediante tarjeta inteligente como usuario local o de Active Directory	<ul style="list-style-type: none"> • Certificado de usuario • Certificado de CA de confianza 	<ul style="list-style-type: none"> • Certificado de usuario: exportar el certificado de usuario de tarjeta inteligente como un archivo de codificación Base64 mediante el software de administración de tarjetas suministrado por el proveedor de la tarjeta inteligente. • Certificado de CA de confianza: este certificado lo emite una CA. <p>También se admiten los certificados SHA-2.</p>
Inicio de sesión de usuario de Active Directory	Certificado de CA de confianza	<p>Este certificado lo emite una CA.</p> <p>También se admiten los certificados SHA-2.</p>
Inicio de sesión de usuario local	Certificado SSL	<p>Generar una CSR y hacer que la firme una CA de confianza</p> <p> NOTA: iDRAC se entrega con un certificado de servidor SSL autofirmado predeterminado. El servidor web de iDRAC, los medios virtuales y la consola virtual utilizan este certificado.</p> <p>También se admiten los certificados SHA-2.</p>

Enlaces relacionados

- [Certificados de servidor SSL](#)
- [Generación de una nueva solicitud de firma de certificado](#)

Certificados de servidor SSL

iDRAC incluye un servidor web configurado para usar el protocolo de seguridad SSL estándar del sector para transferir datos cifrados a través de una red. Basado en la tecnología de cifrado asimétrico, SSL se acepta ampliamente para el suministro de comunicaciones autenticadas y cifradas entre los clientes y servidores con el fin de impedir la escucha a escondidas a través de una red.

Un sistema habilitado para SSL puede realizar las siguientes tareas:

- Autenticarse ante un cliente habilitado con SSL
- Permitir a los dos sistemas establecer una conexión cifrada

El proceso de cifrado proporciona un alto nivel de protección de datos. iDRAC emplea el estándar de cifrado SSL de 128 bits, la manera más segura de cifrados generalmente disponible para los exploradores web en Norteamérica.

De manera predeterminada, el servidor web de iDRAC cuenta con un certificado digital SSL único autofirmado de Dell. Puede reemplazar el certificado SSL predeterminado por un certificado firmado por una Autoridad de certificados (CA) conocida. Una Autoridad de certificados es una entidad comercial reconocida en la industria de TI por cumplir con altas normas de filtrado confiable, identificación y otros criterios de seguridad importantes. Algunas Autoridades de certificados son Thawte y VeriSign. Para iniciar el proceso de obtención de un certificado firmado por CA, utilice la interfaz web de iDRAC o la interfaz de RACADM a fin de generar una solicitud de firma de certificado (CSR) con la información de la empresa. A continuación, envíe la CSR generada a una CA como VeriSign o Thawte. La CA puede ser una CA raíz o una CA intermedia. Una vez que reciba el certificado SSL firmado de AC, cárguelo en iDRAC.

Para que cada iDRAC sea de confianza para la estación de administración, el certificado SSL de iDRAC se debe colocar en el almacén de certificados de la estación de administración. Una vez instalado el certificado SSL en las estaciones de administración, los exploradores admitidos pueden acceder a iDRAC sin advertencias de certificados.

Puede también cargar un certificado de firma personalizado para firmar el certificado SSL, en lugar de confiar en el certificado de firma predeterminado para esta función. Al importar un certificado de firma personalizado en todas las estaciones de administración, todos los iDRAC que utilizan el certificado de firma personalizado son de confianza. Si un certificado de firma personalizado se carga cuando un certificado SSL personalizado ya se encuentra en uso, el certificado SSL personalizado se desactiva y se utiliza un certificado SSL generado automáticamente una sola vez, firmado con el certificado de firma personalizado. Es posible cargar el certificado de firma personalizado (sin la clave privada). Además, se puede eliminar un certificado de firma personalizado existente. Después de eliminar el certificado de firma personalizado, iDRAC se restablece y genera automáticamente un nuevo certificado SSL autofirmado. Si se vuelve a generar un certificado autofirmado, se debe volver a establecer la confianza entre iDRAC y la estación de trabajo de administración. Los certificados SSL generados automáticamente son autofirmados y tienen una fecha de expiración de siete años y un día y una fecha de inicio de un día en el pasado (para diferentes configuraciones de zonas horarias en estaciones de administración e iDRAC).

El certificado SSL del servidor web de iDRAC admite el carácter asterisco (*) como parte del componente ubicado más a la izquierda del nombre común al generar una solicitud de firma de certificado (CSR). Por ejemplo, *.qa.com o *.company.qa.com. Esto se denomina certificado comodín. Si se genera una CSR comodín fuera de iDRAC, podrá contar con un solo certificado SSL comodín firmado que se puede cargar en varios iDRAC. De esta manera, todos los iDRAC serán confiables para los exploradores compatibles. Si se conecta a la interfaz web de iDRAC mediante un explorador compatible que admite un certificado comodín, iDRAC será confiable para el explorador. Mientras inicia los visores, los iDRAC serán confiables para los clientes de los visores.

Enlaces relacionados

[Generación de una nueva solicitud de firma de certificado](#)

[Carga del certificado del servidor](#)

[Visualización del certificado del servidor](#)

[Carga del certificado de firma personalizado](#)

[Descarga del certificado de firma del certificado SSL personalizado](#)

Generación de una nueva solicitud de firma de certificado

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

Después de que la CA recibe la CSR, revisa y comprueba la información que contiene la CSR. Si el solicitante cumple los estándares de la CA, la CA emite un certificado del servidor SSL firmado digitalmente que identifica de manera única el servidor del solicitante cuando establece conexiones SSL con exploradores que se ejecutan en estaciones de administración.

Después de que la CA apruebe la CSR y emita el certificado del servidor SSL, podrá cargarse en iDRAC. La información que se utiliza para generar la CSR, almacenada en el firmware de iDRAC, debe coincidir con la información incluida en el certificado del servidor SSL; es decir, el certificado debe haberse generado mediante la CSR que ha creado iDRAC.

Enlaces relacionados

[Certificados de servidor SSL](#)

Generación de CSR mediante la interfaz web

Para generar una CSR nueva:

 **NOTA:** Cada CSR nueva sobrescribe los datos CSR almacenados en el firmware. La información de la CSR debe coincidir con la información del certificado SSL. De lo contrario, iDRAC no aceptará el certificado.

1. En la interfaz web de iDRAC, vaya a **Información general** → **Configuración de iDRAC** → **Red** → **SSL**, seleccione **Generar una solicitud de firma de certificado (CSR)** y, a continuación, haga clic en **Siguiente**.

Aparece la página **Generar una nueva solicitud de firma de certificado (CSR)**.


2. Introduzca un valor para cada atributo de la CSR.
Para obtener más información, consulte la *Ayuda en línea de iDRAC*.
3. Haga clic en **Generar**.
Se genera una nueva CSR. Guárdela en la estación de administración.

Generación de CSR mediante RACADM

Para generar una CSR mediante RACADM, utilice los objetos en el grupo **cfgRacSecurity** con el comando **config** o utilice los objetos en el grupo **iDRAC.Security** con el comando **set** y, a continuación, utilice el comando **sslcsrgen** para generar la CSR. Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide* (Guía de referencia rápida de la interfaz de línea de comandos RACADM para iDRAC8), disponible en dell.com/support/manuals.

Carga del certificado del servidor

Después de generar una CSR, puede cargar el certificado del servidor SSL firmado en el firmware de iDRAC. iDRAC debe reiniciarse para aplicar el certificado. iDRAC solo acepta certificados de servidor web codificados X509, base 64. También se admiten certificados SHA-2.

 **PRECAUCIÓN:** Durante el restablecimiento, iDRAC no estará disponible por algunos minutos.

Enlaces relacionados

[Certificados de servidor SSL](#)

Carga del certificado del servidor mediante la interfaz web

Para cargar el certificado de servidor SSL:

1. En la interfaz web de iDRAC, vaya a **Información general** → **Configuración de iDRAC** → **Red** → **SSL**, seleccione **Cargar certificado del servidor** y haga clic en **Siguiente**.

Aparecerá la página **Carga del certificado**.

2. En **Ruta de acceso del archivo**, haga clic en **Examinar** y seleccione el certificado en la estación de administración.

3. Haga clic en **Apply (Aplicar)**.

El certificado de servidor SSL se carga en iDRAC.

4. Aparecerá un mensaje emergente solicitándole que reinicie iDRAC de inmediato o más adelante. Haga clic en **Reiniciar iDRAC** o en **Reiniciar iDRAC más adelante**, según sea necesario.

Se reiniciará iDRAC y se aplicará el nuevo certificado. iDRAC no estará disponible por algunos minutos durante el reinicio.



NOTA: Debe reiniciar iDRAC para aplicar el nuevo certificado. Hasta que no se reinicie iDRAC, estará activo el certificado existente.

Carga del certificado del servidor mediante RACADM

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

Si la CSR se genera fuera del iDRAC con una clave privada disponible, para cargar el certificado en el iDRAC:

1. Envíe la CSR a una Autoridad de certificados raíz reconocida. La autoridad de certificados firma la CSR y ésta se convierte en un certificado válido.

2. Cargue la clave privada mediante el comando `racadm remoto sslkeyupload`.

3. Cargue el certificado firmado al iDRAC mediante el comando `racadm remoto sslcertupload`.

El nuevo certificado se ha cargado en iDRAC. Aparecerá un mensaje solicitándole que reinicie iDRAC.

4. Ejecute el comando `racadm racreset` para reiniciar iDRAC.

Se reiniciará iDRAC y se aplicará el nuevo certificado. iDRAC no estará disponible por algunos minutos durante el reinicio.



NOTA: Debe reiniciar iDRAC para aplicar el nuevo certificado. Hasta que no se reinicie iDRAC, estará activo el certificado existente.

Visualización del certificado del servidor

Puede ver el certificado de servidor SSL que se utiliza actualmente en iDRAC.

Enlaces relacionados

[Certificados de servidor SSL](#)

Visualización del certificado del servidor mediante la interfaz web

En la interfaz web de iDRAC, vaya a **Descripción general** → **Configuración de iDRAC** → **Red** → **SSL**. La página **SSL** muestra el certificado del servidor SSL que se encuentra actualmente en uso en la parte superior de la página.

Visualización del certificado del servidor mediante RACADM

Para ver el certificado del servidor SSL, utilice el comando **sslcertview**. Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8), disponible en dell.com/support/manuals.


Carga del certificado de firma personalizado

Puede cargar un certificado de firma personalizado para firmar el certificado SSL. También se admiten los certificados SHA-2.

Carga del certificado de firma personalizado mediante la interfaz web

Para cargar el certificado de firma personalizado mediante la interfaz web de iDRAC:

1. Vaya a **Descripción general** → **Configuración de iDRAC** → **Red** → **SSL**.
Aparecerá la página **SSL**.
2. En **Certificado de firma del certificado SSL personalizado**, seleccione **Cargar certificado de firma del certificado SSL personalizado** y haga clic en **Siguiente**.
Aparecerá la página **Cargar certificado de firma del certificado SSL personalizado**.
3. Haga clic en **Examinar** y seleccione el archivo del certificado de firma del certificado SSL personalizado.
Solo se admite el certificado que cumple con las normas de criptografía de claves públicas N.º 12 (PKCS N.º 12).
4. Si el certificado está protegido con contraseña, introduzca la contraseña en el campo **Contraseña de PKCS N.º 12**.
5. Haga clic en **Apply (Aplicar)**.
El certificado se ha cargado en iDRAC.
6. Aparecerá un mensaje emergente solicitándole que reinicie iDRAC de inmediato o más adelante. Haga clic en **Reiniciar iDRAC** o en **Reiniciar iDRAC más adelante**, según sea necesario.
Luego de reiniciar iDRAC se aplicará el nuevo certificado. iDRAC no estará disponible por algunos minutos durante el reinicio.

 **NOTA:** Debe reiniciar iDRAC para aplicar el nuevo certificado. Hasta que no se reinicie iDRAC, estará activo el certificado existente.

Carga del certificado de firma del certificado SSL personalizado mediante RACADM

Para cargar el certificado de firma del certificado SSL personalizado mediante RACADM, utilice el subcomando **sslcertupload** y, a continuación, utilice el subcomando **racreset** para reiniciar iDRAC. Para obtener más información, consulte *iDRAC8 2.00.00.00 RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM 2.00.00.00 para iDRAC8), disponible en www.dell.com/esmanuals.

Descarga del certificado de firma del certificado SSL personalizado

Puede descargar el certificado de firma personalizado mediante la interfaz web de iDRAC o RACADM.

Descarga del certificado de firma personalizado

Para descargar el certificado de firma personalizado mediante la interfaz web de iDRAC:

1. Vaya a **Descripción general** → **Configuración de iDRAC** → **Red** → **SSL**.
Aparecerá la página **SSL**.
2. En **Certificado de firma del certificado SSL personalizado**, seleccione **Descargar certificado de firma del certificado SSL personalizado** y haga clic en **Siguiente**.
Se mostrará un mensaje emergente que permite guardar el certificado de firma personalizado en la ubicación que seleccione.

Descarga del certificado de firma del certificado SSL personalizado mediante RACADM

Para descargar el certificado de firma del certificado SSL personalizado, utilice el subcomando **sslcertdownload**. Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8), disponible en dell.com/support/manuals.

Eliminación del certificado de firma del certificado SSL personalizado

También es posible eliminar un certificado de firma personalizado existente mediante la interfaz web de iDRAC o RACADM.

Eliminación del certificado de firma personalizado mediante la interfaz web de iDRAC

Para eliminar el certificado de firma personalizado mediante la interfaz web de iDRAC:

1. Vaya a **Descripción general** → **Configuración de iDRAC** → **Red** → **SSL**.
Aparecerá la página **SSL**.
2. En **Certificado de firma del certificado SSL personalizado**, seleccione **Eliminar certificado de firma del certificado SSL personalizado** y haga clic en **Siguiente**.
3. Aparecerá un mensaje emergente solicitándole que reinicie iDRAC de inmediato o más adelante. Haga clic en **Reiniciar iDRAC** o en **Reiniciar iDRAC más adelante**, según sea necesario.
Luego de reiniciar iDRAC, se generará un nuevo certificado autofirmado.

Eliminación del certificado de firma del certificado SSL personalizado mediante RACADM

Para eliminar el certificado de firma del certificado SSL personalizado mediante RACADM, utilice el subcomando **sslcertdelete**. A continuación, utilice el comando **racreset** para reiniciar iDRAC. Para obtener más información, consulte *iDRAC8 2.00.00.00 RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM 2.00.00.00 para iDRAC8), disponible en www.dell.com/esmanuals.

Configuración de varios iDRAC mediante RACADM

Puede configurar uno o varios iDRAC con propiedades idénticas mediante RACADM. Al consultar un iDRAC específico con su ID de grupo e ID de objeto, RACADM crea el archivo de configuración **.cfg** en

función de la información recuperada. El usuario especifica el nombre de archivo. Importe el archivo a otros iDRAC para configurarlos de manera idéntica.

 **NOTA:**


- El archivo de configuración contiene información que es aplicable para el servidor particular. La información se organiza en diferentes grupos de objetos.
- Pocos archivos de configuración contienen información de iDRAC única (tal como la dirección IP estática) que debe modificarse antes de exportar el archivo a otros iDRAC.


Es posible utilizar el archivo XML de configuración del sistema para configurar varios iDRAC mediante RACADM. El archivo XML de configuración del sistema contiene la información de configuración de los componentes y se utiliza para aplicar la configuración para BIOS, iDRAC, RAID y NIC importándolo en un sistema objetivo. Para obtener más información, consulte el documento técnico *XML Configuration Workflow* (Flujo de trabajo de configuración de XML) disponible en dell.com/support/manuals o en Dell Tech Center.

Para configurar varios iDRAC con el archivo **.cfg**:

1. Consulte el iDRAC de destino que contiene la configuración necesaria mediante el comando:
`racadm getconfig -f myfile.cfg`.


El comando solicita la configuración de iDRAC y genera el archivo **myfile.cfg**. Si fuera necesario, puede configurar el archivo con otro nombre.

 **NOTA:** La redirección de la configuración de iDRAC hacia un archivo por medio de `getconfig -f` solo se admite con las interfaces local y remota de RACADM.

 **NOTA:** El archivo **.cfg** generado no contiene contraseñas de usuario.

El comando **getconfig** muestra todas las propiedades de un grupo (especificado por el nombre y el índice del grupo) y todas las propiedades de configuración para un usuario por nombre de usuario.

2. Modifique el archivo de configuración con un editor de textos simple (opcional).

 **NOTA:** Se recomienda que modifique este archivo con un editor de textos sencillo; la utilidad RACADM utiliza un analizador de textos ASCII, y cualquier formato del texto confunde al analizador y podría dañar la base de datos de RACADM.

3. Utilice el nuevo archivo de configuración para modificar el iDRAC de destino mediante el comando:
`racadm config -f myfile.cfg`

De este modo, la información se carga en el otro iDRAC. Puede utilizar el subcomando **config** para sincronizar la base de datos de usuarios y contraseñas mediante Server Administrator.

4. Reinicie el iDRAC de destino mediante el comando: `racadm racreset`

Creación de un archivo de configuración de iDRAC

El archivo de configuración **.cfg** se puede:

- crear
- Obtener desde el comando `racadm getconfig -f <filename>.cfg` o `racadm get -f <filename>.cfg`
- Obtener desde el comando `racadm getconfig -f <filename>.cfg` o `racadm get -f <filename>.cfg` y después editarse

Para obtener información sobre los comandos `getconfig` y `get`, consulte *iDRAC8 RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8), disponible en dell.com/support/manuals.

El archivo `.cfg` se analiza en primer lugar para verificar que contenga nombres de grupo y objeto válidos y que se cumplan las reglas de sintaxis básicas. Los errores se indican con el número de línea que ha detectado el error, y un mensaje explica el problema. Se analiza todo el archivo para verificar su integridad y se muestran todos los errores. Los comandos de escritura no se transmiten a iDRAC si se encuentra un error en el archivo `.cfg`. El usuario debe corregir todos los errores antes de utilizar el archivo para configurar iDRAC. Utilice la opción `-c` en el subcomando `config`, que verifica la sintaxis y no realiza ninguna operación de escritura en iDRAC.

Utilice las siguientes directrices al crear un archivo `.cfg`:

- Si el analizador encuentra un grupo indexado, el índice del grupo se utiliza como ancla. Las modificaciones realizadas en los objetos del grupo indexado también se asocian al valor de índice. Por ejemplo:
 - Si ha utilizado el comando `getconfig`:

```
[cfgUserAdmin] # cfgUserAdminIndex=11 cfgUserAdminUserName= #
cfgUserAdminPassword=***** (Write-Only) cfgUserAdminEnable=0
cfgUserAdminPrivilege=0x00000000 cfgUserAdminIpmiLanPrivilege=15
cfgUserAdminIpmiSerialPrivilege=15 cfgUserAdminSolEnable=0
```
 - Si ha utilizado el comando `get`:

```
[idrac.users.16] Enable=Disabled IpmiLanPrivilege=15
IpmiSerialPrivilege=15 !!Password=***** (Write-Only) Privilege=0x0
SNMPv3AuthenticationType=SHA SNMPv3Enable=Disabled SNMPv3PrivacyType=AES
SolEnable=Disabled UserName=
```
- Los índices son de solo lectura y no se pueden modificar. Los objetos del grupo indexado están enlazados al índice bajo el que se enumeran y la configuración válida para el valor de objeto se aplica solamente a ese índice en particular.
- Existe un conjunto predefinido de índices disponible para cada grupo indexado. Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8), disponible en dell.com/support/manuals.
- Utilice el subcomando `racresetcfg` para restablecer la configuración predeterminada de iDRAC y, a continuación, ejecute el comando `racadm config -f <filename>.cfg` o `racadm set -f <filename>.cfg`. Asegúrese de que el archivo `.cfg` incluya todos los objetos, usuarios, índices y demás parámetros requeridos.

⚠ PRECAUCIÓN: Utilice el subcomando `racresetcfg` para restablecer la configuración de la base de datos y de la NIC de iDRAC a sus valores predeterminados, y elimine todos los usuarios y las configuraciones de usuario. Aunque el usuario raíz está disponible, los demás valores de configuración de usuario también se restablecen a los valores predeterminados.

Reglas de análisis

- Todas las líneas que comienzan con '#' se tratan como comentarios. Una línea de comentario debe comenzar en la columna uno. Un carácter '#' en cualquier otra columna se trata como un carácter '#'. Algunos parámetros modernos podrían incluir caracteres '#' en su cadena. No se requiere un carácter de escape. Puede generar un archivo `.cfg` desde un comando `racadm getconfig -f <filename>.cfg` y luego ejecutar un comando `racadm config -f <filename>.cfg` a un iDRAC diferente, sin agregar caracteres de escape. Por ejemplo:

```
#
# This is a comment
```

```
[cfgUserAdmin]
```

```
cfgUserAdminPageModemInitString=<Modem init # not a comment>
```

- Todas las entradas de grupo deben estar encerradas por los caracteres "[" y "]". El carácter de apertura "[" que indica un nombre de grupo *debe* comenzar en la columna uno. Este nombre de grupo *debe* especificarse antes de cualquiera de los objetos de ese grupo. Los objetos que no incluyen un nombre de grupo asociado generarán errores. Los datos de la configuración se organizan en grupos, según se define en *iDRAC8 RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8), disponible en dell.com/support/manuals. En el siguiente ejemplo se muestra un nombre de grupo, un objeto y el valor de la propiedad del objeto.

```
[cfgLanNetworking] -{group name}
```

```
cfgNicIpAddress=143.154.133.121 {object name}
```

- Todos los parámetros están especificados como pares "objeto=valor" sin espacios en blanco entre el objeto, el símbolo "=" y el valor.

Los espacios en blanco que se incluyan después de un valor se omiten. Un espacio en blanco dentro de una cadena de valores queda sin modificar. Cualquier carácter a la derecha de '=' se toma como tal (por ejemplo, un segundo '=', o un '#', '[', ']', etc.). Estos caracteres son caracteres de secuencia de comandos de chat de módem válidos.

Consulte el ejemplo en el punto anterior.

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

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

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

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

```
[cfgUserAdmin]
```

```
cfgUserAdminIndex=11
```

Si escribe `racadm getconfig -f <myexample>.cfg`, el comando genera un archivo **.cfg** para la configuración actual de iDRAC. Este archivo de configuración se puede usar como un ejemplo y como punto de inicio para el archivo **.cfg** único.

Modificación de la dirección IP de iDRAC

Cuando modifique la dirección IP de iDRAC en el archivo de configuración, elimine todas las entradas `<variable>=value` innecesarias. Solo la etiqueta del grupo de variables real con "[" y "]" permanece, incluidas las dos entradas `<variable>=value` que pertenecen al cambio de dirección IP.

Por ejemplo:

```
#
```

```
# Object Group "cfgLanNetworking"
```

```
#
```

```
[cfgLanNetworking]

cfgNicIpAddress=10.35.10.110

cfgNicGateway=10.35.10.1
```

Este archivo se actualiza de la siguiente forma:

```
#

# Object Group "cfgLanNetworking"

#

[cfgLanNetworking]


cfgNicIpAddress=10.35.9.143

# comment, the rest of this line is ignored

cfgNicGateway=10.35.9.1
```

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


Utilice este archivo para descargar cambios que abarcan toda la empresa o para configurar nuevos sistemas en la red.

 **NOTA:** "Anchor" es un término interno y no debe utilizarlo en el archivo.

Desactivación del acceso para modificar los valores de configuración de iDRAC en el sistema host

Puede desactivar el acceso para modificar la configuración de iDRAC a través de RACADM local o la utilidad de configuración de iDRAC. No obstante, puede ver estos valores de configuración. Para ello:

1. En la interfaz web de iDRAC, vaya a **Información general** → **Configuración de iDRAC** → **Red** → **Servicios**.
2. Seleccione una o ambas opciones siguientes:
 - **Desactivar la configuración local de iDRAC mediante la configuración de iDRAC:** desactiva el acceso para modificar los valores de configuración en la utilidad de configuración de iDRAC.
 - **Desactivar la configuración local de iDRAC mediante RACADM:** desactiva el acceso para modificar los valores de configuración en RACADM local.
3. Haga clic en **Apply (Aplicar)**.

 **NOTA:** Si se desactiva el acceso, no podrá utilizar Server Administrator ni IPMITool para realizar las configuraciones de iDRAC. Sin embargo, podrá utilizar IPMI en la LAN.

Visualización de la información de iDRAC y el sistema administrado

Es posible ver la condición y las propiedades de iDRAC y del sistema administrado, su inventario de hardware y firmware, la condición de los sensores, los dispositivos de almacenamiento y los dispositivos de red, así como ver y terminar las sesiones de usuario. En el caso de los servidores blade, también se puede ver la información de dirección flexible.

Enlaces relacionados

[Visualización de la condición y las propiedades de Managed System](#)

[Visualización del inventario del sistema](#)

[Visualización de la información del sensor](#)

[Supervisión del índice de rendimiento de CPU, memoria y módulos de E/S](#)

[Consulta del sistema para verificar el cumplimiento de aire fresco](#)

[Visualización de los datos históricos de temperatura](#)

[Inventario y supervisión de dispositivos de almacenamiento](#)

[Inventario y supervisión de dispositivos de red](#)

[Inventario y supervisión de dispositivos HBA FC](#)

[Visualización de las conexiones de red Fabric de la tarjeta mezzanine FlexAddress](#)

[Visualización o terminación de sesiones iDRAC](#)

Visualización de la condición y las propiedades de Managed System

Cuando se inicia sesión en la interfaz web de iDRAC, la página **Resumen del sistema** permite ver la condición del sistema administrado, la información básica de iDRAC y la vista previa de la consola virtual. También permite agregar y ver notas de trabajo e iniciar rápidamente tareas como apagado o encendido, ciclo de encendido, ver registros, actualizar y revertir firmware, encender y apagar el LED en el panel anterior y restablecer iDRAC.

Para acceder a la página **Resumen del sistema**, vaya a **Descripción general** → **Servidor** → **Propiedades** → **Resumen**. Se mostrará la página **Resumen del sistema**. Para obtener más información, consulte la *Ayuda en línea de iDRAC*.

También puede ver información básica resumida del sistema mediante la utilidad de configuración de iDRAC. Para ello, en la utilidad de configuración de iDRAC, vaya a **Resumen del sistema**. Se muestra la página **Configuración de iDRAC - Resumen del sistema**. Para obtener más información, consulte *iDRAC Settings Utility Online Help* (Ayuda en línea de la utilidad de configuración de iDRAC).

Visualización del inventario del sistema

Es posible ver información acerca de los componentes de hardware y firmware instalados en el sistema administrado. Para ello, en la interfaz web de iDRAC, vaya a **Descripción general** → **Servidor** →

Propiedades → **Inventario del sistema**. Para obtener más información acerca de las propiedades mostradas, consulte la *Ayuda en línea de iDRAC*.

La sección Inventario de hardware muestra información sobre los siguientes componentes disponibles en el sistema administrado:

- iDRAC
- Controladora RAID
- Baterías
- CPU
- DIMM
- HDD
- Planos posteriores
- Tarjetas de interfaz de red (integradas e incorporadas)
- Tarjeta de vídeo
- la tarjeta SD
- Unidades de suministro de energía (PSU)
- Ventiladores
- HBA de Fibre Channel
- USB

La sección Inventario de firmware muestra la versión de firmware de los siguientes componentes:

- BIOS
- Lifecycle Controller
- iDRAC
- Driver Pack del SO
- Diagnósticos de 32 bits
- Sistema CPLD
- Controladoras PERC
- Baterías
- Discos físicos
- Fuente de alimentación
- NIC
- Fibre Channel
- Plano posterior
- Gabinete
- Unidades SSD PCIe

Si reemplaza algún componente de hardware o actualiza versiones de firmware, asegúrese de activar y ejecutar la opción **Recopilar inventario del sistema en el reinicio** (CSIOR) para recopilar el inventario del sistema al reiniciar. Después de unos minutos, inicie sesión en iDRAC y vaya a la página **Inventario del sistema** para ver los detalles. Es posible que haya una demora de hasta 5 minutos para que la información esté disponible, según el hardware instalado en el servidor.



NOTA: La opción CSR está activada de forma predeterminada.

Haga clic en **Exportar** para exportar el inventario de hardware en formato XML y guárdelo en la ubicación que desee.

Visualización de la información del sensor

Los sensores siguientes ayudan a supervisar la condición del sistema administrado:

- **Baterías:** proporciona información acerca de las baterías del CMOS en la placa del sistema y del RAID de almacenamiento en la placa base (ROMB).
 - ✎ **NOTA:** La configuración de las baterías de ROMB de almacenamiento solo se encuentra disponible si el sistema tiene ROMB con una batería.
- **Ventilador** (disponible solo para los servidores tipo bastidor y torre): proporciona información acerca de los ventiladores del sistema; la redundancia de ventiladores y la lista de ventiladores que muestra la velocidad de los ventiladores y los valores del umbral.
- **CPU** : indica la condición y el estado de la CPU en el sistema administrado. Informa además la regulación automática del procesador y la falla predictiva.
- **Memoria:** indica la condición y el estado de los módulos de memoria doble en línea (DIMM) presentes en el sistema administrado.
- **Intrusión:** proporciona información sobre el chasis.
- **Suministros de energía** (disponible solo para los servidores tipo bastidor y torre): proporciona información acerca de los suministros de energía y el estado de redundancia del suministro de energía.
 - ✎ **NOTA:** Si solo existe un suministro de energía en el sistema, la redundancia del mismo estará **desactivada**.
- **Medios flash extraíbles:** proporciona información acerca de los módulos SD internos; vFlash y módulo SD dual interno (IDSDM).
 - Cuando está activada la redundancia de IDSDM, se muestra el siguiente estado de sensor de IDSDM: el estado de la redundancia de IDSDM, IDSDM SD1, IDSDM SD2. Cuando la redundancia está desactivada, solo se muestra IDSDM SD1.
 - Si la redundancia de IDSDM está desactivada inicialmente cuando el sistema se enciende o después de restablecer el iDRAC, el estado del sensor IDSDM SD1 se muestra solo después de que se inserte una tarjeta.
 - Si la redundancia de IDSDM está activada con dos tarjetas SD presentes en el IDSDM y el estado de una tarjeta SD es *en línea* mientras el estado de la otra es *fuera de línea*, se requiere un reinicio del sistema para restaurar la redundancia entre las dos tarjetas SD en el IDSDM. Una vez restaurada la redundancia, el estado de ambas tarjetas SD en el IDSDM será *en línea*.
 - Durante la operación de regeneración para restaurar la redundancia entre dos tarjetas SD presentes en el IDSDM, el estado IDSDM no se muestra, ya que los sensores de IDSDM están apagados.
 - ✎ **NOTA:** Si el sistema host se reinicia durante la operación de recreación, el sistema iDRAC no muestra la información de IDSDM. Para resolver esto, recree IDSDM nuevamente o restablezca el sistema iDRAC.
 - Los registros de sucesos de sistema (SEL) para una tarjeta SD protegida contra escritura o dañada en el módulo IDSDM no se repitan hasta que se borren. Para ello, se debe reemplazar la tarjeta SD con una tarjeta escribible o en buen estado, respectivamente.
- **Temperatura:** proporciona información acerca de la temperatura interna de la placa del sistema y la temperatura de expulsión (solo se aplica a servidores en bastidor). La sonda de temperatura indica si el estado de la sonda se encuentra dentro de los valores de umbral críticos y de advertencia.
- **Voltaje:** indica el estado y la lectura de los sensores de voltaje de los distintos componentes del sistema.

En la tabla siguiente se proporciona información sobre cómo ver la información de los sensores mediante la interfaz web de iDRAC y RACADM. Para obtener información acerca de las propiedades que se muestran en la interfaz web, consulte la *Ayuda en línea de iDRAC* de las páginas correspondientes.

Tabla 9. Información del sensor mediante la interfaz web y RACADM

Visualización de la información del sensor	Mediante la interfaz web	Mediante RACADM
Baterías	Información general → Hardware → Baterías	Utilice el comando getsensorinfo . Para suministros de energía, también puede usar el comando System.Power.Supply con el subcomando get . Para obtener más información, consulte <i>iDRAC8 RACADM Command Line Interface Reference Guide (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8)</i> disponible en dell.com/support/manuals .
Ventilador	Información general → Hardware → Ventiladores	
CPU	Información general → Hardware → CPU	
Memoria	Información general → Hardware → Memoria	
Intrusión	Información general → Servidor → Intrusión	
Fuentes de alimentación	Información general → Hardware → Suministros de energía	
Medios flash extraíbles	Información general → Hardware → Unidades Flash extraíbles	
Temperatura	Información general → Servidor → Alimentación/Térmico → Temperaturas	
Tensión	Información general → Servidor → Alimentación/Térmico → Voltajes	

Supervisión del índice de rendimiento de CPU, memoria y módulos de E/S

En los servidores Dell PowerEdge de 13.^a generación, Intel ME admite la funcionalidad Cómputo de uso por segundo (CUPS). Esta funcionalidad proporciona supervisión en tiempo real sobre la utilización de la CPU, la memoria y los módulos de E/S, así como el índice de utilización en el nivel de sistema. Como esto se realiza a través de Intel ME, la operación es independiente del sistema operativo y no consume recursos de la CPU. Intel ME contiene un sensor de CUPS sobre el sistema que brinda el valor de utilización de recursos de computación, memoria y E/S como un índice CUPS. iDRAC supervisa este índice CUPS para comprobar la utilización de todo el sistema y también supervisa el valor instantáneo de índice de utilización de CPU, memoria y E/S.

Para obtener la información de utilización de los recursos del sistema, es necesario consultar los datos con un conjunto de contadores dedicados que se proporcionan en la CPU y el conjunto de chips. Estos contadores se llaman Contadores de supervisión de recursos (RMC). Es el administrador de nodos quien agrega estos contadores para medir la utilización acumulada de cada uno de los recursos del sistema. Los valores de utilización se leen desde iDRAC por medio de mecanismos de intercomunicación existentes para proporcionar estos datos vitales en las interfaces de administración fuera de banda.


Como la representación de los sensores Intel para los parámetros de rendimiento y los valores de índice abarca el sistema físico completo, la representación de los datos de rendimiento en las interfaces abarca todo el sistema físico, aunque el sistema se haya virtualizado y aloje varios hosts virtuales.

Para mostrar los parámetros de rendimiento, los sensores admitidos deben estar presentes en el servidor.

Los cuatro parámetros de utilización del sistema son:

- **Utilización de CPU:** existen contadores de supervisión de recursos (RMC) individuales para cada núcleo de CPU que se agrega para proporcionar la utilización acumulada de todos los núcleos en el sistema. Esta utilización se basa en el tiempo transcurrido en estado activo y el tiempo transcurrido en estado inactivo. Se toma una muestra de RMC cada seis segundos.
- **Utilización de memoria:** existen contadores (RMC) individuales para medir el tráfico de memoria que se produce en cada canal de memoria o instancia de la controladora de memoria. Estos contadores se agregan para medir el tráfico de memoria acumulado en todos los canales de memoria que se encuentran en el sistema. Esta es una medida para el consumo de ancho de banda de la memoria y no la cantidad de utilización de la memoria. iDRAC agrega este valor por un período de un minuto, por lo que es posible que coincida o no con la utilización de memoria que muestran otras herramientas del sistema operativo como TOP en Linux. La utilización de ancho de banda de la memoria que muestra iDRAC indica si la carga de trabajo de la memoria es intensiva o no.
- **Utilización de E/S:** existen contadores de supervisión de recursos (RMC) individuales, uno por cada puerto raíz en el complejo raíz PCI Express para medir el tráfico de PCI Express que se emite desde o se dirige hacia ese puerto raíz y el segmento menor. Posteriormente, se agregan estos contadores para medir el tráfico de PCI Express para todos los segmentos PCI Express que se emiten desde el paquete. Esta es una medida de la utilización de ancho de banda de E/S para el sistema.
- **Índice CUPS en el nivel del sistema:** el índice CUPS es la suma de los índices de CPU, memoria y E/S en la que se considera un factor de carga predefinido para cada recurso del sistema. El factor de carga depende de la naturaleza de la carga de trabajo que se ejecuta en el sistema. Es por eso que el índice CUPS representa la medición de la capacidad de aumento para cómputo disponible en el servidor en un momento dado. Por lo tanto, si el sistema presenta un índice CUPS alto, la capacidad de aumento para colocar una carga de trabajo adicional sobre ese sistema es limitada. A medida que el consumo de recursos disminuye, también disminuye el índice CUPS del sistema. Un índice CUPS bajo indica que existe una capacidad de aumento para cómputo alta y que el servidor es un destino

principal para recibir las cargas de trabajo nuevas o migrar la carga de trabajo, así como para colocar el servidor en un estado de menor consumo de energía a fin de reducir el consumo de energía. Esa supervisión de la carga de trabajo se puede aplicar a todo el centro de datos, a fin de proporcionar una vista integral de alto nivel de la carga de trabajo en el centro de datos y así, brindar una solución de centro de datos dinámica.

 **NOTA:** Los índices de utilización de CPU, memoria y E/S se suman a cada minuto. Por lo tanto, si se produce algún pico instantáneo en estos índices, es posible suprimirlos. Estos índices indican los patrones de carga de trabajo, no la cantidad de utilización de recursos.

Cuando se alcanzan los umbrales de los índices de utilización, se generan capturas IPMI, SEL y SNMP, y se activan los sucesos de servidor. Los indicadores de sucesos de sensor se encuentran desactivados de manera predeterminada. Se pueden activar mediante la interfaz de IPMI estándar.

Los privilegios requeridos son:

- Se requiere el privilegio de inicio de sesión para supervisar los datos de rendimiento.
- Se requiere el privilegio de configuración para establecer los umbrales de advertencia y restablecer los picos históricos.
- Se requiere el privilegio de inicio de sesión y la licencia Enterprise para leer los datos estadísticos históricos.

Supervisión del índice de rendimiento de CPU, memoria y módulos de E/S mediante la interfaz web

Para supervisar el índice de rendimiento de la CPU, la memoria y los módulos de E/S, en la interfaz web de iDRAC, vaya a **Descripción general** → **Hardware**. Se mostrará la página **Descripción general de hardware** donde se muestra lo siguiente:

- Sección **Hardware**: haga clic en el vínculo requerido para ver la condición de cada componente.
- Sección **Rendimiento del sistema**: se muestra la lectura actual y la lectura de advertencia para el índice de utilización de la CPU, la memoria y los módulos de E/S, así como el índice CUPS en el nivel del sistema en una vista gráfica.
- Sección **Datos históricos de rendimiento del sistema**:
 - Se proporcionan las estadísticas para la utilización de la CPU, la memoria y los módulos de E/S, así como el índice CUPS en el nivel del sistema. Si el sistema host se encuentra apagado, el gráfico muestra la línea de apagado por debajo de 0 %.
 - Es posible restablecer la utilización pico para un determinado sensor. Haga clic en **Restablecer pico histórico**. Es necesario tener el privilegio de configuración para restablecer el valor pico.
- Sección **Métricas de rendimiento**:
 - Se puede ver el estado y la lectura presente.
 - Vea o especifique el límite de utilización para el umbral de advertencia. Es necesario tener el privilegio de configuración de servidores para establecer los valores de umbral.

Para obtener información acerca de las propiedades que se muestran, consulte la *Ayuda en línea de iDRAC*.


Supervisión del índice de rendimiento de CPU, memoria y módulos de E/S mediante RACADM

Utilice el subcomando **SystemPerfStatistics** para supervisar el índice de rendimiento de la CPU, la memoria y los módulos de E/S. Para obtener más información, consulte *iDRAC RACADM Command Line*

Reference Guide (Guía de referencia de la línea de comandos RACADM de iDRAC) disponible en dell.com/esmanuals.

Consulta del sistema para verificar el cumplimiento de aire fresco

La refrigeración de aire fresco utiliza directamente el aire exterior para enfriar los sistemas en el centro de datos. Los sistemas que cumplen con el requisito de aire fresco pueden funcionar por encima de su rango de funcionamiento ambiente normal (temperaturas de hasta 113 °F (45 °C)).


 **NOTA:** Algunos servidores o ciertas configuraciones de un servidor pueden no cumplir con la normativa de "aire fresco". Consulte el manual del servidor específico para obtener detalles relacionados con el cumplimiento de esa normativa o póngase en contacto con Dell para obtener más detalles.

Para consultar el sistema para verificar el cumplimiento de aire fresco

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Servidor** → **Alimentación / Térmico** → **Temperaturas**.
Aparecerá la página **Temperaturas**.
2. Consulte la sección **Aire fresco** que indica si el servidor cumple o no con el requisito de aire fresco.

Visualización de los datos históricos de temperatura

Es posible supervisar el porcentaje de tiempo en que el sistema ha funcionado a una temperatura ambiente que es mayor que el umbral de temperatura de aire fresco admitido normalmente. La lectura del sensor de temperatura de la placa del sistema se recopila durante un período de tiempo para supervisar la temperatura. La recopilación de datos comienza cuando el sistema se enciende por primera vez después de salir de fábrica. Los datos se recopilan y se muestran mientras el sistema permanece encendido. Se puede realizar un seguimiento y almacenar la temperatura que se supervisó en los últimos siete años.

 **NOTA:** Es posible realizar un seguimiento sobre el historial de temperaturas incluso para los sistemas que no cumplen con el requisito de aire fresco. Sin embargo, los límites de umbral y las advertencias relacionadas con aire fresco que se generan se basan en los límites de aire fresco admitidos. Los límites son 42 °C para el umbral de advertencia y 47 °C para el umbral crítico. Estos valores corresponden a los límites de aire fresco de 40 °C y 45 °C con un margen de 2 °C para asegurarse de su precisión.

Se realiza un seguimiento de dos bandas de temperatura fijas asociadas a los límites de aire fresco:

- Banda de advertencia: consta de la duración en la que un sistema ha funcionado por encima del umbral de advertencia del sensor de temperatura (42 °C). El sistema puede funcionar en la banda de advertencia durante el 10 % del tiempo por 12 meses.
- Banda crítica: consta de la duración en la que un sistema ha funcionado por encima del umbral crítico del sensor de temperatura (47 °C). El sistema puede funcionar en la banda crítica durante el 1% del tiempo por 12 meses, lo que también provoca incrementos de tiempo en la banda de advertencia.

Los datos recopilados se representan en un gráfico para realizar un seguimiento de los niveles de 10 % y 1%. Los datos de temperatura registrados se pueden borrar solamente antes de que salga de fábrica.

Se genera un suceso si el sistema continúa funcionando por encima del umbral de la temperatura normalmente admitida durante un tiempo específico de funcionamiento. Si la temperatura promedio

durante un tiempo específico de funcionamiento es igual o mayor que el nivel de advertencia (> = 8%) o el nivel crítico (> = 0.8%), se registra un suceso en el registro de Lifecycle y se genera la correspondiente captura SNMP. Los sucesos son:

- Suceso de advertencia cuando la temperatura fue mayor que el umbral de advertencia por una duración del 8 % o más en los últimos 12 meses.
- Suceso crítico cuando la temperatura fue mayor que el umbral de advertencia por una duración del 10 % o más en los últimos 12 meses.
- Suceso de advertencia cuando la temperatura fue mayor que el umbral crítico por una duración del 0,8 % o más en los últimos 12 meses.
- Suceso crítico cuando la temperatura fue mayor que el umbral crítico por una duración del 1 % o más en los últimos 12 meses.

Puede además configurar iDRAC para que genere sucesos adicionales. Para obtener más información, consulte la sección [Configuración de suceso de periodicidad de alertas](#).

Visualización de los datos históricos de temperatura mediante la interfaz web de iDRAC

Para ver los datos históricos de temperatura:

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Servidor** → **Alimentación / Térmico** → **Temperaturas**.
Aparecerá la página **Temperaturas**.
2. Consulte la sección **Datos históricos de temperatura de la placa del sistema** donde se muestra un gráfico de la temperatura almacenada (valores promedio y pico) correspondientes al último día, a los últimos 30 días y al año anterior.

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



NOTA: Después de una actualización del firmware de iDRAC o de reiniciar iDRAC, es posible que algunos datos de temperatura no se muestren en el gráfico.

Visualización de datos históricos de temperatura mediante RACADM

Para ver los datos históricos mediante RACADM, utilice el subcomando **inlettemphistory**. Para obtener más información, consulte *iDRAC8 RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM para iDRAC8)*.

Configuración del umbral de advertencia para la temperatura de entrada

Es posible modificar los valores de umbral de advertencia mínimo y máximo para el sensor de temperatura de entrada de la placa del sistema. Si se realiza una acción para restablecer los valores predeterminados, los umbrales de temperatura se establecen en los valores predeterminados. Es necesario tener el privilegio de usuario de configuración para establecer los valores de umbral de advertencia para el sensor de temperatura de entrada.


Configuración del umbral de advertencia para la temperatura de entrada mediante la interfaz web

Para configurar el umbral de advertencia para la temperatura de entrada:

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Servidor** → **Alimentación/Térmico** → **Temperaturas**.

Aparecerá la página **Temperaturas**.

2. En la sección **Sondas de temperatura**, para **Temperatura de entrada de la placa del sistema**, introduzca los valores mínimo y máximo para **Umbral de advertencia** en grados Celsius o Fahrenheit. Si se introduce el valor en grados Celsius, el sistema calcula y muestra automáticamente el valor en Fahrenheit. De la misma manera, si se introduce en grados Fahrenheit, se muestra el valor en Celsius.
3. Haga clic en **Apply (Aplicar)**.
Se configuran los valores.

 **NOTA:** Los cambios realizados en los umbrales predeterminados no se reflejan en el gráfico de datos históricos, ya que los límites en el gráfico corresponden solamente a valores de límite de aire fresco. Las advertencias por exceder los umbrales personalizados son diferentes a las advertencias asociados a exceder los umbrales de aire fresco.

Visualización de interfaces de red disponibles en el sistema operativo host

Es posible ver la información acerca de todas las interfaces de red que se encuentran disponibles en el sistema operativo host como las direcciones IP que se han asignado al servidor. El módulo de servicio de iDRAC proporciona estos datos al iDRAC. La información de direcciones IP para el sistema operativo incluye las direcciones IPv4 e IPv6, la dirección MAC, la longitud de la máscara o el prefijo de subred y el FQDD para el dispositivo de red.

 **NOTA:** Esta función está disponible con las licencias iDRAC Express y Enterprise.

Para ver la información del sistema operativo, asegúrese de que:

- Tiene privilegios de inicio de sesión.
- El módulo de servicio de iDRAC se ha instalado y se ejecuta en el sistema operativo host.
- La opción Información de sistema operativo se encuentra activada en la página **Descripción general** → **Servidor** → **Módulo de servicio**.


iDRAC puede mostrar las direcciones IPv4 e IPv6 para todas las interfaces configuradas en el sistema operativo host.

Según la forma en que el sistema operativo host detecta el servidor DHCP, es posible que no se muestre la dirección IPv4 o IPv6 correspondiente para el servidor DHCP. Por lo general, una dirección IPv4 o IPv6 para DHCP es visible cuando DHCP se encuentra activado.

Visualización de interfaces de red disponibles en el sistema operativo host mediante la interfaz web

Para ver las interfaces de red disponibles en el sistema operativo host mediante la interfaz web:

1. Vaya a **Descripción general** → **SO host** → **Interfaces de red**.
La página **Interfaces de red** muestra todas las interfaces de red que se encuentran disponibles en el sistema operativo host.
2. Para ver la lista de interfaces de red asociadas con un dispositivo de red, en el menú desplegable **FQDD de dispositivo de red**, seleccione un dispositivo de red y, a continuación, haga clic en **Aplicar**.
Los detalles de IP para el sistema operativo se mostrarán en la sección **Interfaces de red para sistema operativo host**.

3. En la columna **FQDD de dispositivo**, haga clic en el vínculo para el dispositivo de red.
Se mostrará la página para el dispositivo correspondiente desde la sección **Hardware** → **Dispositivos de red**, donde se pueden ver los detalles del dispositivo. Para obtener más información acerca de estas propiedades, consulte la *Ayuda en línea de iDRAC*.
4. Para cada dispositivo de red, haga clic en el  icono para mostrar los detalles adicionales.
De forma similar, se puede ver la información de interfaces de red para el sistema operativo host asociado con un dispositivo de red desde la página **Hardware** → **Dispositivos de red**. Haga clic en **Ver interfaces de red de sistema operativo host**.

Visualización de interfaces de red disponibles en el sistema operativo host mediante RACADM

Utilice el comando `gethostnetworkinterfaces` para ver las interfaces de red disponibles en los sistemas operativos de hosts mediante RACADM. Para obtener más información, consulte *iDRAC RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de iDRAC)* disponible en dell.com/esmmanuals.


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

En los servidores Blade, 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.

Puede ver la información siguiente para cada puerto de tarjeta Ethernet incorporada y tarjeta mezzanine opcional instalada:

- Redes Fabric a las que están conectadas las tarjetas
- Tipo de red Fabric.
- Direcciones MAC asignadas por el servidor, asignadas por el chasis o asignadas de manera remota.

Para ver la información de FlexAddress en iDRAC, configure y active la función FlexAddress en Chassis Management Controller (CMC). Para obtener más información, consulte *Dell Chassis Management Controller User Guide (Guía del usuario de Dell Chassis Management Controller)* disponible en dell.com/support/manuals. Las sesiones de consola virtual o medios virtuales existentes se cerrarán si se activa o desactiva la configuración FlexAddress.

 **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 función FlexAddress reemplaza las direcciones MAC asignadas por el servidor con las direcciones MAC asignadas por el chasis y se implementa para iDRAC junto con los LOM de servidores blade, las tarjetas mezzanine y los módulos de E/S. La función FlexAddress de iDRAC admite la conservación de una dirección MAC específica de ranura para iDRACs en un chasis. La dirección MAC asignada por el chasis se almacenan en memoria no volátil de CMC y se envía a iDRAC durante un inicio de iDRAC o cuando se activa CMC FlexAddress.

Si CMC activa direcciones MAC asignadas por el chasis, iDRAC muestra la **Dirección MAC** en cualquiera de las páginas siguientes:

- **Descripción general** → **Servidor** → **Propiedades Detalles** → **Información de iDRAC**.

- **Descripción general** → **Servidor** → **Propiedades WWN/MAC**.
- **Información general** → **Configuración de iDRAC** → **Propiedades Información iDRAC** → **Configuración de red actual**.
- **Descripción general** → **Configuración de iDRAC** → **Red Red** → **Configuración de la 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 de iDRAC también cambia.

Visualización o terminación de sesiones iDRAC

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

Terminación de las sesiones de iDRAC mediante la interfaz web

Los usuarios que no tienen privilegios administrativos deben tener privilegios de configuración de iDRAC para terminar sesiones iDRAC mediante la interfaz web de iDRAC.

Para ver y terminar las sesiones iDRAC:

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Configuración de iDRAC** → **Sesiones**. La página **Sesiones** muestra el ID de la sesión, la dirección IP y el tipo de sesión. Para obtener más información acerca de estas propiedades, consulte la *Ayuda en línea de iDRAC*.
2. Para terminar la sesión, en la columna **Terminar**, haga clic en el icono de papelera de reciclaje de una sesión.

Terminación de las sesiones de iDRAC mediante RACADM

Es necesario disponer de privilegios de administrador para terminar las sesiones iDRAC mediante RACADM.

Para ver las sesiones de usuario actual, utilice el comando **getssninfo**.

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

Para obtener más información sobre estos comandos, consulte *iDRAC8 RACADM Command Line Interface Reference Guide (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8)* disponible en dell.com/support/manuals.

Configuración de la comunicación de iDRAC

Es posible comunicarse con iDRAC mediante cualquiera de los modos siguientes:

- Interfaz web del iDRAC
- Conexión serie mediante un cable DB9 (comunicación en serie RAC o comunicación en serie IPMI): solo para servidores tipo bastidor y torre
- Comunicación en serie IPMI en la LAN
- IPMI en la LAN
- RACADM remoto
- RACADM local
- Servicios remotos

Para obtener información general acerca de los protocolos compatibles, los comandos admitidos y los prerequisites, consulte la tabla siguiente.

Tabla 10. Modos de comunicación: resumen

Modos de comunicación	Protocolo compatible	Comandos admitidos	Prerrequisito
Interfaz web del iDRAC	Protocolo de Internet (https)	NA	Web Server
Comunicación en serie mediante un cable DB9 de módem nulo	Protocolo de comunicación en serie	RACADM SMCLP IPMI	Parte del firmware iDRAC Comunicación en serie RAC o IPMI activada.
Comunicación en serie IPMI en la LAN	Protocolo de bus de administración de plataforma inteligente SSH Telnet	IPMI	IPMITool se instala y la Comunicación en serie IPMI en la LAN está activada.
IPMI en la LAN	Protocolo de bus de administración de plataforma inteligente	IPMI	IPMITool se instala y la configuración IPMI se activa.
SMCLP	SSH Telnet	SMCLP	SSH o Telnet en iDRAC se activa.

Modos de comunicación	Protocolo compatible	Comandos admitidos	Prerrequisito
RACADM remoto	HTTPS	RACADM remoto	RACADM remoto se instala y activa.
Firmware RACADM	SSH Telnet	Firmware RACADM	Firmware RACADM se instala y se activa.
RACADM local	IPMI	RACADM local	Local RACADM se instala.
Servicios remotos [1]	WS-MAN	WinRM (Windows) OpenWSMAN (Linux)	WinRM se instala (Windows) o OpenWSMAN se instala (Linux).

[1] Para obtener más información, consulte *Lifecycle Controller Remote Services User's Guide* (Guía del usuario de Lifecycle Controller Remote Services) disponible en dell.com/support/manuals.


Enlaces relacionados

- [Comunicación con iDRAC a través de una conexión serie mediante un cable DB9](#)
- [Cambio entre la comunicación en serie RAC y la consola de comunicación en serie mediante el cable DB9](#)
- [Comunicación con iDRAC mediante IPMI SOL](#)
- [Comunicación con iDRAC mediante IPMI en la LAN](#)
- [Activación o desactivación de RACADM remoto](#)
- [Desactivación de RACADM local](#)
- [Activación de IPMI en Managed System](#)
- [Configuración de Linux para la consola de comunicación en serie durante el inicio](#)
- [Esquemas de criptografía SSH compatibles](#)

Comunicación con iDRAC a través de una conexión serie mediante un cable DB9

Puede utilizar cualquiera de los métodos de comunicación para realizar tareas de administración del sistema a través de una conexión serie a servidores tipo bastidor y torre:

- Comunicación en serie RAC
- Comunicación en serie IPMI: modo básico de conexión directa y modo de terminal de conexión directa

 **NOTA:** En el caso de los servidores blade, la conexión serie se establece a través del chasis. Para obtener más información, consulte *Chassis Management Controller User's Guide* (Guía del usuario de Chassis Management Controller) disponible en dell.com/support/manuals.

Para establecer una conexión serie:

1. Configure el BIOS para activar conexiones serie:
2. Conecte el cable DB9 de módem nulo desde el puerto serie de la estación de administración hasta el conector serie externo del sistema administrado.

3. Asegúrese de que el software de emulación de terminal de la estación de administración se haya configurado para conexiones serie utilizando cualquiera de los métodos siguientes:
 - Linux Minicom en Xterm
 - HyperTerminal Private Edition (versión 6.3) de Hilgraeve

Según dónde se encuentra el sistema administrado en el proceso de inicio, aparecerá la pantalla POST o la pantalla del sistema operativo. Esto depende de la configuración: SAC para Windows y pantallas de modo de texto Linux para Linux.

4. Active las conexiones RAC serie o IPMI serie en iDRAC.

Enlaces relacionados


[Configuración del BIOS para la conexión serie](#)

[Activación de la conexión serie RAC](#)

[Activación de los modos básicos y de terminal de la conexión serie básica IPMI](#)

Configuración del BIOS para la conexión serie


Para configurar el BIOS para la conexión serie:

 **NOTA:** Esto es aplicable solamente para iDRAC en servidores tipo bastidor y torre.

1. Encienda o reinicie el sistema.
2. Presione <F2>.
3. Vaya a **Configuración del BIOS del sistema** → **Comunicación en serie**.
4. Seleccione **Conector serie externo** en **Dispositivo de acceso remoto**.
5. Haga clic en **Atrás**, en **Terminar** y, a continuación, en **Sí**.
6. Presione <Esc> para salir de **Configuración del sistema**.

Activación de la conexión serie RAC

Después de configurar la conexión serie en el BIOS, active la comunicación en serie RAC en iDRAC.

 **NOTA:** Esto es aplicable solamente para iDRAC en servidores tipo bastidor y torre.

Activación de la conexión serie RAC mediante la interfaz web

Para activar la conexión serie RAC:

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Configuración de iDRAC** → **Red** → **Comunicación en serie**.
Se mostrará la página **Comunicación en serie**.
2. En **Comunicación en serie RAC**, seleccione **Activado** y especifique los valores de los atributos.
3. Haga clic en **Apply (Aplicar)**.
Se habrán configurado los valores de la comunicación en serie RAC.


Activación de la conexión serie RAC mediante RACADM

Para activar la conexión serie RAC mediante RACADM, utilice una de las siguientes opciones:

- Utilice los objetos del grupo **cfgSerial** con el comando **config**.
- Utilice el objeto del grupo **iDRAC.Serial** con el comando **set**.

Activación de los modos básicos y de terminal de la conexión serie básica IPMI

Para activar el enrutamiento de comunicación en serie IPMI del BIOS en iDRAC, configure la comunicación en serie IPMI en cualquiera de los modos siguientes en iDRAC:

 **NOTA:** Esto es aplicable solamente para iDRAC en servidores tipo bastidor y torre.

- En modo IPMI básico: admite una interfaz binaria para el acceso al programa, tal como el shell de IPMI (ipmish) que se incluye con la utilidad de administración de placa base (BMU). Por ejemplo, para imprimir el registro de sucesos del sistema mediante ipmish a través del modo básico IPMI, ejecute el comando siguiente:

```
ipmish -com 1 -baud 57600 -flow cts -u root -p calvin sel get
```

- Modo de terminal IPMI: admite comandos ASCII que se envían desde una terminal de comunicación en serie. Este modo admite un número limitado de comandos (incluido el control de alimentación) y comandos IPMI sin formato que se escriben como caracteres ASCII hexadecimales. Esto permite ver las secuencias de inicio del sistema operativo hasta el BIOS, cuando se inicia sesión en iDRAC a través de SSH o Telnet.

Enlaces relacionados

[Configuración del BIOS para la conexión serie](#)

[Configuración adicional para el modo de terminal de la comunicación en serie IPMI](#)

Activación de la conexión serie mediante la interfaz web

Asegúrese de desactivar la interfaz serie RAC para activar la comunicación en serie IPMI.

Para configurar los valores de la comunicación en serie IPMI:

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Configuración de iDRAC** → **Red** → **Comunicación en serie**.
2. Bajo **Comunicación en serie IPMI**, especifique los valores de los atributos. Para obtener más información acerca de estas opciones, consulte la *Ayuda en línea de iDRAC*.
3. Haga clic en **Apply (Aplicar)**.

Activación del modo de comunicación en serie de IPMI mediante RACADM

Para configurar el modo de IPMI, desactive la interfaz de serie RAC y, a continuación, active el modo de IPMI mediante una de las siguientes opciones:

- Mediante el comando **config**:

```
racadm config -g cfgSerial -o cfgSerialConsoleEnable 0
```

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialConnectionMode < 0 o 1>
```

donde, *0* indica el modo de terminal y *1* indica el modo básico.

- Mediante el comando **set**:

```
racadm set iDRAC.Serial.Enable 0
```

```
racadm set iDRAC.IPMISerial.ConnectionMode < 0 o 1>
```

donde, *0* indica el modo de terminal y *1* indica el modo básico.

Activación de la configuración de la comunicación en serie de IPMI mediante RACADM

Para configurar los valores de la conexión serie de IPMI, se utiliza el comando **set** o **config**:

1. Cambie el modo de conexión serie IPMI al valor adecuado mediante el comando:
 - Mediante el comando **config**: `racadm config -g cfgSerial -o cfgSerialConsoleEnable 0`
 - Mediante el comando **set**: `racadm set iDRAC.Serial.Enable 0`
 2. Establezca la velocidad en baudios de la conexión serie de IPMI:
 - Mediante el comando **config**: `racadm config -g cfgIpmiSerial -o cfgIpmiSerialBaudRate <baud_rate>`
 - Mediante el comando **set**: `racadm set iDRAC.IPMSerial.BaudRate <baud_rate>`

donde <baud_rate> es 9600, 19200, 57600 o 115200 bps.
 3. Active el control de flujo del hardware de la conexión serie de IPMI.
 - Mediante el comando **config**: `racadm config -g cfgIpmiSerial -o cfgIpmiSerialFlowControl 1`
 - Mediante el comando **set**: `racadm set iDRAC.IPMSerial.FlowControl 1`
 4. Establezca el nivel mínimo de privilegios del canal de la conexión serie de IPMI.
 - Mediante el comando **config**: `racadm config -g cfgIpmiSerial -o cfgIpmiSerialChanPrivLimit <nivel>`
 - Mediante el comando **set**: `racadm set iDRAC.IPMSerial.ChanPrivLimit <level>`

donde <nivel> es 2 (Usuario), 3 (Operador) o 4 (Administrador).
 5. Asegúrese de que el MUX de comunicación en serie (conector serie externo) se ha establecido correctamente al dispositivo de acceso remoto en el programa de configuración del BIOS para configurar el BIOS para la conexión serie.
- Para obtener más información sobre estas propiedades, consulte la especificación IPMI 2.0.

Configuración adicional para el modo de terminal de la comunicación en serie IPMI

En esta sección se proporcionan valores de configuración adicionales para el modo de terminal de la comunicación en serie IPMI.

Configuración de valores adicionales para el modo de terminal de comunicación en serie IPMI mediante la interfaz web

Para configurar los valores del modo de terminal:

1. En la interfaz web de iDRAC, vaya a **Información general** → **Configuración de iDRAC** → **Red** → **Comunicación en serie**
Aparecerá la página **Comunicación en serie**.
2. Active la comunicación en serie IPMI.
3. Haga clic en **Configuración del modo de terminal** .
Se muestra la página **Configuración del modo de terminal**.
4. Especifique los valores siguientes:
 - Edición de línea
 - Control de eliminación
 - Control del eco

- Control del protocolo de enlace
- Nueva secuencia de línea
- Entrada de nuevas secuencias de línea

Para obtener más información acerca de estas opciones, consulte la *Ayuda en línea de iDRAC*.

5. Haga clic en **Apply (Aplicar).**

Se configuran los valores del modo de terminal.

6. Asegúrese de que el MUX de comunicación en serie (conector serie externo) se ha establecido correctamente al dispositivo de acceso remoto en el programa de configuración del BIOS para configurar el BIOS para la conexión serie.

Configuración de valores adicionales para el modo de terminal de comunicación en serie IPMI mediante RACADM

Para configurar los valores del modo de terminal, ejecute el comando: `racadm config cfgIpmiSerial`

Cambio entre la comunicación en serie RAC y la consola de comunicación en serie mediante el cable DB9

iDRAC admite secuencias de tecla de escape que permiten cambiar entre una comunicación de interfaz en serie RAC y una consola de comunicación en serie en servidores tipo bastidor y torre.

Cambio de una consola de comunicación en serie a la comunicación en serie RAC

Para cambiar al modo de comunicación de interfaz serie del RAC desde el modo de consola de comunicación en serie, utilice la siguiente secuencia de teclas:

`<Esc> +<Shift> <9>`

Esta secuencia activa la petición de "Inicio de sesión de iDRAC" (si iDRAC está configurado en modo de comunicación en serie RAC) o bien el modo de conexión serie en el que pueden emitirse comandos de terminal si iDRAC se encuentra en modo de terminal de comunicación en serie directa de IPMI.

Cambio de una comunicación en serie RAC a consola de comunicación en serie

Para cambiar al modo de consola de comunicación en serie desde el modo de comunicación de interfaz serie del RAC, use la siguiente secuencia de teclas:

`<Esc> +<Shift> <q>`

En modo de terminal, para cambiar la conexión al modo de consola de comunicación en serie utilice:

`<Esc> +<Shift> <q>`

Para volver al uso de modo de terminal, cuando esté conectado en el modo de consola de comunicación en serie:

`<Esc> +<Shift> <9>`

Comunicación con iDRAC mediante IPMI SOL

La comunicación en serie IPMI en la LAN (SOL) permite el redireccionamiento de los datos de comunicación en serie de la consola basada en texto del sistema administrador a través de la red Ethernet de administración fuera de banda (dedicada o compartida) de iDRAC. Mediante SOL se puede realizar lo siguiente:

- Acceder a los sistemas operativos de manera remota sin tiempo de espera.
- Realizar diagnósticos de sistemas host en servicios de administración de emergencia (EMS) o en la consola administrativa especial (SAC) para un shell de Windows o Linux.
- Ver el progreso de los servidores durante POST y reconfigurar el programa de configuración del BIOS.

Para configurar el modo de comunicación SOL:

1. Configure el BIOS para la conexión serie.
2. Configure iDRAC para utilizar SOL.
3. Active un protocolo compatible (SSH, Telnet, IPMItool).

Enlaces relacionados


[Configuración del BIOS para la conexión serie](#)

[Configuración de iDRAC para usar SOL](#)


[Activación del protocolo compatible](#)

Configuración del BIOS para la conexión serie


Para configurar el BIOS para la conexión serie:

 **NOTA:** Esto es aplicable solamente para iDRAC en servidores tipo bastidor y torre.

1. Encienda o reinicie el sistema.
2. Presione <F2>.
3. Vaya a **Configuración del BIOS del sistema** → **Comunicación en serie**.
4. Especifique los valores siguientes:
 - Comunicación en serie: con Redirección de consola
 - Dirección de puerto serie: COM2.

 **NOTA:** Se puede configurar el campo de **comunicación serie** en **Activado con redirección serie a través de com1** si **dispositivo serie2** en el campo de **dirección del puerto serie** también está configurado en com1.

- Conector serie externo: dispositivo serie2
 - Velocidad en baudios a prueba de fallas: 115200
 - Tipo de terminal remota: VT100/VT220
 - Redirección después de inicio: activado
5. Haga clic en **Atrás** y luego en **Terminar**.
 6. Haga clic en **Sí** para guardar los cambios.
 7. Presione <Esc> para salir de **Configuración del sistema**.

 **NOTA:** El BIOS envía los datos serie de la pantalla en formato 25 x 80. La ventana SSH que se utiliza para invocar el comando `console com2` debe estar configurada en el formato 25 x 80. De esta manera, la pantalla redirigida se mostrará correctamente.

Configuración de iDRAC para usar SOL

Puede especificar la configuración de SOL en iDRAC mediante la interfaz web, RACADM o la utilidad de configuración de iDRAC.

Configuración de iDRAC para usar SOL mediante la interfaz web iDRAC

Para configurar la comunicación en serie IPMI en la LAN (SOL).

1. En la interfaz web de iDRAC, vaya a **Información general** → **Configuración de iDRAC** → **Red** → **Comunicación en serie en la LAN**
Aparecerá la página **Comunicación en serie en la LAN**.
2. Active SOL, especifique los valores y haga clic en **Aplicar**.
Se habrán configurado los valores de IPMI SOL.
3. Para configurar el intervalo de acumulación de caracteres y el umbral de envío de caracteres, seleccione **Configuración avanzada**.
Aparecerá la página **Configuración avanzada de la comunicación en serie en la LAN**.
4. Especifique los valores de los atributos y haga clic en **Aplicar**.
Se configuran la configuración avanzada de IPMI SOL. Estos valores ayudan a mejorar el rendimiento.

Para obtener más información acerca de estas opciones, consulte la *Ayuda en línea de iDRAC*.

Configuración de iDRAC para usar SOL mediante RACADM

Para configurar la comunicación en serie IPMI en la LAN (SOL).

1. Active la comunicación en serie IPMI en la LAN:
 - Mediante el comando **config**: `racadm config -g cfgIpmiSol -o cfgIpmiSolEnable 1`
 - Mediante el comando **set**: `racadm set iDRAC.IPMISol.Enable 1`
2. Actualice el nivel de privilegios mínimo de SOL de IPMI.
 - Mediante el comando **config**: `racadm config -g cfgIpmiSol o cfgIpmiSolMinPrivilege <level>`
 - Mediante el comando **set**: `racadm set iDRAC.IPMISol.MinPrivilege 1`

donde <level> es 2 (Usuario), 3 (Operador), 4 (Administrador).



NOTA: El nivel de privilegio mínimo IPMI SOL determina el privilegio mínimo para activar IPMI SOL. Para obtener más información, consulte la especificación IPMI 2.0.

3. Actualice la velocidad en baudios de SOL de IPMI.
 - Mediante el comando **config**: `racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate <baud_rate>`
 - Mediante el comando **set**: `racadm set iDRAC.IPMISol.BaudRate <baud_rate>`

donde <baud_rate> es 9600, 19200, 57600 o 115200 bps.



NOTA: Para redirigir la consola de comunicación en serie en la LAN, asegúrese de que la velocidad en baudios de la comunicación en serie en la LAN sea idéntica a la velocidad en baudios del sistema administrado.

4. Desactive SOL para cada usuario:
 - Mediante el comando **config**: `racadm config -g cfgUserAdmin -o cfgUserAdminSolEnable -i <id> 2`

- Mediante el comando **set**: `racadm set iDRAC.Users.<id>.SolEnable 2`

donde <id> es la identificación única del usuario.



NOTA: Para redirigir la consola de comunicación en serie en la LAN, asegúrese de que la velocidad en baudios de la comunicación en serie en la LAN sea idéntica a la velocidad en baudios del sistema administrado.

Activación del protocolo compatible

Los protocolos admitidos son IPMI, SSH y Telnet.

Activación del protocolo admitido mediante la interfaz web

Para activar SSH o Telnet, vaya a **Información general** → **Configuración de iDRAC** → **Red** → **Servicios** y seleccione **Activado** para SSH o Telnet, respectivamente.

Para activar IPMI, vaya a **Descripción general** → **Configuración de iDRAC** → **Red** y seleccione **Activar IPMI en la LAN**. Asegúrese de que el valor **Clave de cifrado** sea todos ceros o pulse la tecla de retroceso para borrar y cambiar el valor a caracteres NULOS.

Activación del protocolo admitido mediante RACADM

Para activar SSH o Telnet, ejecute el comando:

- Telnet:
 - Mediante el comando **config**: `racadm config -g cfgSerial -o cfgSerialTelnetEnable 1`
 - Mediante el comando **set**: `racadm set iDRAC.Telnet.Enable 1`
- SSH:
 - Mediante el comando **config**: `racadm config -g cfgSerial -o cfgSerialSshEnable 1`
 - Mediante el comando **set**: `racadm set iDRAC.SSH.Enable 1`

Para cambiar el puerto SSH, escriba:

- Mediante el comando **config**: `racadm config -g cfgRacTuning -o cfgRacTuneSshPort <port number>`
- Mediante el comando **set**: `racadm set iDRAC.SSH.Port <port number>`

Puede utilizar las herramientas siguientes:

- IPMItool para utilizar el protocolo IPMI
- Putty/OpenSSH para utilizar el protocolo SSH o Telnet

Enlaces relacionados

[SOL mediante el protocolo IPMI](#)

[SOL mediante el protocolo SSH o Telnet](#)

SOL mediante el protocolo IPMI

IPMItool <--> Conexión LAN/WAN <--> iDRAC


La utilidad SOL basada en IPMI y la herramienta IPMItool utilizan RMCP+ que se entrega mediante datagramas UDP al puerto 623. RMCP+ proporciona opciones mejoradas de autenticación, comprobación de integridad de datos, cifrado y capacidad para transportar varios tipos de cargas cuando

se utiliza IPMI 2.0. Para obtener más información, consulte <http://ipmitool.sourceforge.net/manpage.html>.


RMCP+ utiliza una clave de cifrado de cadena hexadecimal de 40 caracteres (0-9, a-f y A-F) para la autenticación. El valor predeterminado de una cadena es 40 ceros.

Una conexión RMCP+ a iDRAC debe cifrarse mediante la clave de cifrado (clave de generador de clave (KG)). Se puede configurar la clave de cifrado mediante la interfaz web de iDRAC o la utilidad de configuración de iDRAC.

Para iniciar una sesión SOL mediante IPMItool desde una estación de administración:

 **NOTA:** Si fuera necesario, se puede cambiar el tiempo de espera predeterminado de la sesión SOL en **Descripción general** → **Configuración de iDRAC** → **Red** → **Servicios**.

1. Instale IPMITool desde el DVD *Herramientas y documentación para administración de sistemas Dell*. Para obtener las instrucciones de instalación, consulte la *Guía de instalación rápida de software*.
2. En el símbolo del sistema (Windows o Linux), ejecute el comando para iniciar SOL desde iDRAC:
`ipmitool -H <iDRAC-ip-address> -I lanplus -U <login name> -P <login password> sol activate.`
De este modo, la estación de administración se conectará al puerto serie del sistema administrado.
3. Para salir de una sesión SOL desde IPMItool, pulse <~> y <. > consecutivamente. Se cerrará la sesión SOL.


 **NOTA:** Si una sesión SOL no termina, restablezca iDRAC y deje pasar al menos dos minutos para completar el inicio.

SOL mediante el protocolo SSH o Telnet

Shell seguro (SSH) y Telnet son protocolos de red que se usan para establecer comunicaciones de línea de comandos a iDRAC. Es posible analizar comandos RACADM y SMCLP remotos a través de cualquiera de estas interfaces.

SSH es más seguro que Telnet. iDRAC solo admite SSH versión 2 con autenticación de contraseñas, el cual se encuentra activado de manera predeterminada. iDRAC admite hasta dos sesiones SSH y dos sesiones Telnet a la vez. Es recomendable utilizar SSH, ya que Telnet no es un protocolo seguro. Se debe utilizar Telnet solamente si no se puede instalar un cliente SSH o si la infraestructura de la red es segura.

Para conectarse a iDRAC, utilice programas de código abierto, tal como PuTTY u OpenSSH que admitan los protocolos de red SSH y Telnet en una estación de administración.

 **NOTA:** Ejecute OpenSSH desde un emulador de terminal VT100 o ANSI en Windows. Ejecutar OpenSSH en el símbolo del sistema de Windows no ofrece funcionalidad completa (es decir, algunas teclas no responden y no se muestra gráficos).

Antes de utilizar SSH o Telnet para comunicarse con iDRAC, asegúrese de realizar lo siguiente:

1. Configurar el BIOS para activar la consola de comunicación en serie.
2. Configurar SOL en iDRAC.
3. Activar SSH o Telnet mediante la interfaz web de iDRAC o RACADM.
Cliente Telnet (puerto 23)/SSH (puerto 22) <---> Conexión WAN <---> iDRAC

SOL basado en IPMI que utiliza el protocolo SSH o Telnet elimina la necesidad de utilidades adicionales, ya que la traslación de comunicación en serie a la red se realiza en iDRAC. La consola SSH o Telnet que utilice debe poder interpretar y responder a los datos que lleguen del puerto serie del sistema administrado. El puerto serie normalmente se conecta a un shell que emula una terminal ANSI o VT100/VT220. La consola de comunicación en serie se redirige automáticamente a la consola SSH o Telnet.


Enlaces relacionados

[Uso de SOL desde PuTTY en Windows](#)


[Uso de SOL desde OpenSSH o Telnet en Linux](#)

Uso de SOL desde PuTTY en Windows

Para iniciar IPMI SOL desde PuTTY en una estación de trabajo de Windows:

 **NOTA:** Si fuera necesario, puede cambiar el tiempo de espera de la sesión SSH o Telnet predeterminado en **Información general** → **Configuración de iDRAC** → **Red** → **Servicios**.

1. Ejecute el comando para conectarse a iDRAC: `putty.exe [-ssh | -telnet] <login name>@<iDRAC-ip-address> <port number>`

 **NOTA:** El número de puerto es opcional. Solo se necesita cuando el número de puerto se ha reasignado.


2. Ejecute el comando `console com2` o `connect` para iniciar SOL e iniciar el sistema administrado. Se abre una sesión SOL desde la estación de administración al sistema administrado mediante el protocolo SSH o Telnet. Para acceder a la consola de línea de comandos de iDRAC, siga la secuencia de teclas ESC. El comportamiento de conexión Putty y SOL es el siguiente:
 - Al acceder al sistema administrado a través de Putty durante el proceso POST, si la opción Teclas de función y teclado en Putty está establecido del modo siguiente:
 - VT100+: F2 pasa, pero F12 no pasa.
 - ESC[n~: F12 pasa, pero F2 no pasa.
 - En Windows, si se abre la consola del sistema de administración de emergencia (EMS) inmediatamente después de un reinicio del host, es posible que se dañe la terminal de la consola de administración especial (SAC). Cierre la sesión SOL, cierre la terminal, abra otra terminal e inicie la sesión SOL mediante el mismo comando.

Enlaces relacionados


[Desconexión de la sesión SOL en la consola de línea de comandos de iDRAC](#)

Uso de SOL desde OpenSSH o Telnet en Linux

Para iniciar SOL desde OpenSSH o Telnet en una estación de trabajo de Linux:

 **NOTA:** Si fuera necesario, puede cambiar el tiempo de espera predeterminado de la sesión SSH o Telnet en **Descripción general** → **Configuración de iDRAC** → **Red** → **Servicios**.

1. Inicie una ventana de shell.
2. Conéctese a iDRAC mediante el comando siguiente:
 - Para SSH: `ssh <iDRAC-ip-address> -l <login name>`
 - Para Telnet: `telnet <iDRAC-ip-address>`

 **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 uno de los comandos siguientes en el símbolo del sistema para iniciar SOL:

- `connect`
- `console com2`

Esto conecta iDRAC al puerto SOL del sistema administrado. Una vez establecida la sesión SOL, la consola de línea de comandos de iDRAC dejará de estar disponible. Siga la secuencia de escape correctamente para abrir la consola de línea de comandos de iDRAC. La secuencia de comandos también se imprime en la pantalla tan pronto se conecta la sesión SOL. Cuando el sistema administrado está desactivado, lleva algo de tiempo para establecer la sesión SOL.



NOTA: Puede utilizar `console com1` o `console com2` para iniciar SOL. Reinicie el servidor para establecer la conexión.

El comando `console -h com2` muestra el contenido del búfer de historial de la conexión serie antes de esperar información proveniente del teclado o nuevos caracteres provenientes del puerto serie.

El tamaño predeterminado (y máximo) del búfer del historial es de 8192 caracteres. Puede establecer este número en un valor menor mediante el comando:

```
racadm config -g cfgSerial -o cfgSerialHistorySize <number>
```

4. Cierre la sesión SOL para cerrar la sesión SOL activa.

Enlaces relacionados

[Uso de la consola virtual de Telnet](#)

[Configuración de la tecla de retroceso para la sesión de Telnet](#)

[Desconexión de la sesión SOL en la consola de línea de comandos de iDRAC](#)

Uso de la consola virtual de Telnet

Es posible que algunos clientes Telnet en los sistemas operativos de Microsoft no muestren correctamente la pantalla de configuración del BIOS cuando la consola virtual del BIOS se ha configurado para la emulación VT100/VT220. En este caso, cambie la consola del BIOS al modo ANSI para actualizar la pantalla. Para realizar este procedimiento, seleccione **Consola virtual** → **Tipo de terminal remoto** → **ANSI**.

Al configurar la ventana de emulación de cliente VT100, defina la ventana o la aplicación que está mostrando la consola virtual redirigida en 25 filas x 80 columnas, para garantizar que el texto se muestre correctamente; de lo contrario, es posible que algunas pantallas de texto aparezcan ilegibles.

Para utilizar la consola virtual Telnet:

1. Active **Telnet** en **Servicios de componentes de Windows**.
2. Conéctese a iDRAC mediante el comando: `telnet <IP address>:<port number>`, donde `IP address` es la dirección IP de iDRAC y `port number` es el número de puerto Telnet (si utiliza un puerto nuevo).

Configuración de la tecla de retroceso para la sesión de Telnet

Según el cliente Telnet, el uso de la tecla <Retroceso> podría producir resultados inesperados. Por ejemplo, la sesión podría producir un eco `^h`. Sin embargo, la mayoría de los clientes Telnet de Microsoft y Linux puede configurarse para utilizar la tecla <Retroceso>.

Para configurar la sesión Telnet de Linux para que utilice la tecla <Retroceso>, abra un símbolo del sistema y escriba `stty erase ^h`. En la petición, escriba `telnet`.

Para configurar los clientes Telnet de Microsoft para usar la tecla <Retroceso>:

1. Abra una ventana de símbolo del sistema (si es necesario).
2. Si no está ejecutando una sesión Telnet, escriba `telnet`. Si está ejecutando una, presione <Ctrl><J>.
3. En la petición, escriba `set bsasdel`.
Se muestra el mensaje `Backspace will be sent as delete`.

Desconexión de la sesión SOL en la consola de línea de comandos de iDRAC

Los comandos para desconectar una sesión SOL dependen de la utilidad. Puede salir de la utilidad solamente cuando la sesión SOL se ha terminado por completo.

Para desconectar una sesión SOL, finalice la sesión SOL desde la consola de línea de comandos de iDRAC.

- Para salir del redireccionamiento SOL, presione <Intro>, <Esc> y luego <t>. Se cierra la sesión de SOL.
- Para salir de una sesión SOL desde Telnet en Linux, mantenga presionado <Ctrl>+]. Se muestra una petición de Telnet. Introduzca `quit` para salir de Telnet.
- Si una sesión SOL no se termina completamente en la utilidad, es posible que no haya otras sesiones SOL disponibles. Para solucionar esto, cierre la consola de línea de comandos en la interfaz web bajo **Información general** → **Configuración de iDRAC** → **Sesiones**.

Comunicación con iDRAC mediante IPMI en la LAN

Debe configurar IPMI en la LAN para iDRAC con el fin de activar o desactivar los comandos IPMI en los canales LAN hacia cualquier sistema externo. Si no se lleva a cabo esta configuración, los sistemas externos no podrán comunicarse con el servidor iDRAC mediante comandos IPMI.

Configuración de IPMI en la LAN mediante la interfaz web

Para configurar IPMI en la LAN:

1. En la interfaz web de iDRAC, vaya a **Información general** → **Configuración de iDRAC** → **Red**. Aparecerá la página **Red**.
2. En **Configuración de IPMI**, especifique los valores de los atributos y haga clic en **Aplicar**.
Para obtener más información acerca de estas opciones, consulte la *Ayuda en línea de iDRAC*.

Se habrán configurado los valores de IPMI en la LAN.

Configuración de IPMI en la LAN mediante la utilidad de configuración de iDRAC

Para configurar IPMI en la LAN:

1. En **Utilidad de configuración de iDRAC**, vaya a **Red**. Aparece la pantalla **Red de configuración de iDRAC**.
2. Para **Configuración de IPMI**, especifique los valores.
Para obtener información acerca de las opciones, consulte la *Ayuda en línea de la utilidad de configuración de iDRAC*.
3. Haga clic en **Atrás**, en **Terminar** y, a continuación, en **Sí**.
Se habrán configurado los valores de IPMI en la LAN.

Configuración de IPMI en la LAN mediante RACADM

Para configurar IPMI en la LAN mediante el comando **set** o **config**:

1. Active la IPMI en la LAN:

- Mediante el comando **config**: `racadm config -g cfgIpmiLan -o cfgIpmiLanEnable 1`
- Mediante el comando **set**: `racadm set iDRAC.IPMILan.Enable 1`



NOTA: Este valor determina los comandos IPMI que se ejecutan mediante la interfaz IPMI en la LAN. Para obtener más información, consulte las especificaciones de IPMI 2.0 en intel.com.

2. Actualice los privilegios de canal de IPMI:

- Mediante el comando **config**: `racadm config -g cfgIpmiLan -o cfgIpmiLanPrivilegeLimit <level>`
- Mediante el comando **set**: `racadm set iDRAC.IPMILan.PrivLimit <level>`

donde <level> es uno de los siguientes: 2 (Usuario), 3 (Operador) o 4 (Administrador)

3. Establezca la clave de cifrado del canal de LAN de IPMI (si es necesario):

- Mediante el comando **config**: `racadm config -g cfgIpmiLan -o cfgIpmiEncryptionKey <key>`
- Mediante el comando **set**: `racadm set iDRAC.IPMILan.EncryptionKey <key>`

donde <key> es una clave de cifrado de 20 caracteres en un formato hexadecimal válido.



NOTA: IPMI de iDRAC admite el protocolo RMCP+. Para obtener más información, consulte las especificaciones de IPMI 2.0 en intel.com.

Activación o desactivación de RACADM remoto

Es posible activar o desactivar RACADM remoto mediante la interfaz web de iDRAC o RACADM y ejecutar hasta cinco sesiones de RACADM remoto simultáneamente.

Activación o desactivación de RACADM remoto mediante la interfaz web

Para activar o desactivar RACADM remoto:

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Configuración de iDRAC** → **Red** → **Servicios**.

Aparecerá la página **Servicios**.

2. En **RACADM remoto**, seleccione **Activado**. De lo contrario, seleccione **Desactivado**.

3. Haga clic en **Apply (Aplicar)**.

RACADM remoto se activa o desactiva según la opción seleccionada.


Activación o desactivación de RACADM remoto mediante RACADM

La capacidad remota de RACADM está activada de forma predeterminada. En caso de estar desactivada, escriba uno de los siguientes comandos:

- Mediante el comando **config**: `racadm config -g cfgRacTuning -o cfgRacTuneRemoteRacadmEnable 1`
- Mediante el comando **set**: `racadm set iDRAC.Racadm.Enable 1`

Para desactivar la capacidad remota, escriba uno de los siguientes comandos:

- Mediante el comando **config**: `racadm config -g cfgRacTuning -o cfgRacTuneRemoteRacadmEnable 0`
- Mediante el comando **set**: `racadm set iDRAC.Racadm.Enable 0`

 **NOTA:** Es recomendable ejecutar estos comandos en el sistema local.

Desactivación de RACADM local


RACADM local está activado de manera predeterminada. Para desactivarlo, consulte [Desactivación del acceso para modificar la configuración de iDRAC en el sistema host](#).

Activación de IPMI en Managed System

En un sistema administrado, utilice Dell Open Manage Server Administrator para activar o desactivar IPMI. Para obtener más información, consulte *Dell Open Manage Server Administrator's User Guide* (Guía del usuario de Dell Open Manage Server Administrator) disponible en dell.com/support/manuals.

Configuración de Linux para la consola de comunicación en serie durante el inicio

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

 **NOTA:** Al configurar la ventana de emulación de cliente VT100, defina la ventana o la aplicación que está mostrando la consola virtual redirigida en 25 filas x 80 columnas, para garantizar que el texto se muestre correctamente; de lo contrario, es posible que algunas pantallas de texto aparezcan ilegibles.

Modifique el archivo `/etc/grub.conf` según se indica a continuación:

1. Localice las secciones de configuración general dentro del archivo y agregue lo siguiente:


```
serial --unit=1 --speed=57600 terminal --timeout=10 serial
```
2. Anexe dos opciones a la línea de núcleo:


```
kernel ..... console=ttyS1,115200n8r console=tty1
```
3. Desactive la interfaz gráfica de GRUB y utilice la interfaz basada en texto. De lo contrario, la pantalla de GRUB no se mostrará en la consola virtual de RAC. Para desactivar la interfaz gráfica, coloque un comentario en la línea que comience con `splashimage`.

En el ejemplo siguiente se proporciona un archivo `/etc/grub.conf` que muestra los cambios que se describen en este procedimiento.

```
# grub.conf generated by anaconda # Note that you do not have to rerun grub
after making changes to this file # NOTICE: You do not have a /boot
partition. This means that all # kernel and initrd paths are relative to /,
e.g. # root (hd0,0) # kernel /boot/vmlinuz-version ro root=/dev/sda1 #
initrd /boot/initrd-version.img #boot=/dev/sda default=0 timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz serial --unit=1 --speed=57600
terminal --timeout=10 serial title Red Hat Linux Advanced Server (2.4.9-e.
3smp) root (hd0,0) kernel /boot/vmlinuz-2.4.9-e.3smp ro root=/dev/sda1
hda=ide-scsi console=ttyS0 console=ttyS1,115200n8r initrd /boot/
initrd-2.4.9-e.3smp.img title Red Hat Linux Advanced Server-up (2.4.9-e.3)
root (hd0,00) kernel /boot/vmlinuz-2.4.9-e.3 ro root=/dev/sda1 s initrd /
boot/initrd-2.4.9-e.3.im
```

4. Para activar varias opciones de GRUB para iniciar sesiones en la consola virtual mediante la conexión serie del RAC, agregue la siguiente línea a todas las opciones:

```
console=ttyS1,115200n8r console=tty1
```

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

Activación del inicio de sesión en la consola virtual después del inicio

En el archivo `/etc/inittab`, agregue una línea nueva para configurar `agetty` en el puerto serie COM2:

```
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
```

El siguiente ejemplo muestra un archivo con la nueva línea.


```
#inittab This file describes how the INIT process should set up #the system in
a certain run-level. #Author:Miquel van Smoorenburg #Modified for RHS Linux by
Marc Ewing and Donnie Barnes #Default runlevel. The runlevels used by RHS are:
#0 - halt (Do NOT set initdefault to this) #1 - Single user mode #2 -
Multiuser, without NFS (The same as 3, if you do not have #networking) #3 -
Full multiuser mode #4 - unused #5 - X11 #6 - reboot (Do NOT set initdefault to
this) id:3:initdefault: #System initialization. si::sysinit:/etc/rc.d/
rc.sysinit 10:0:wait:/etc/rc.d/rc 0 11:1:wait:/etc/rc.d/rc 1 12:2:wait:/etc/
rc.d/rc 2 13:3:wait:/etc/rc.d/rc 3 14:4:wait:/etc/rc.d/rc 4 15:5:wait:/etc/
rc.d/rc 5 16:6:wait:/etc/rc.d/rc 6 #Things to run in every runlevel. ud::once:/
sbin/update ud::once:/sbin/update #Trap CTRL-ALT-DELETE ca::ctrlaltdel:/sbin/
shutdown -t3 -r now #When our UPS tells us power has failed, assume we have a
few #minutes of power left. Schedule a shutdown for 2 minutes from now. #This
does, of course, assume you have power installed and your #UPS is connected and
working correctly. pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure; System
Shutting Down" #If power was restored before the shutdown kicked in, cancel it.
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored; Shutdown Cancelled"

#Run gettys in standard runlevels co:2345:respawn:/sbin/agetty -h -L 57600
ttyS1 ansi 1:2345:respawn:/sbin/mingetty tty1 2:2345:respawn:/sbin/mingetty
tty2 3:2345:respawn:/sbin/mingetty tty3 4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5 6:2345:respawn:/sbin/mingetty tty6 #Run xdm
in runlevel 5 #xdm is now a separate service x:5:respawn:/etc/X11/prefdm -
nodaemon
```

En el archivo `/etc/securetty`, agregue una línea nueva con el nombre de la conexión tty serie para COM2:

```
ttyS1
```

El siguiente ejemplo muestra un archivo con la nueva línea.

 **NOTA:** Utilice la secuencia de teclas de interrupción (`~B`) para ejecutar los comandos clave de Linux **Magic SysRq** en la consola de comunicación en serie utilizando la herramienta IPMI.

```
vc/1 vc/2 vc/3 vc/4 vc/5 vc/6 vc/7 vc/8 vc/9 vc/10 vc/11 tty1 tty2 tty3 tty4
tty5 tty6 tty7 tty8 tty9 tty10 tty11 ttyS1
```

Esquemas de criptografía SSH compatibles

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

Tabla 11. Esquemas de criptografía SSH

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

Uso de la autenticación de clave pública para SSH

iDRAC admite la autenticación de claves públicas (PKA) sobre SSH. Esta es una función con licencia. Cuando la PKA sobre SSH se configura y utiliza correctamente, no es necesario introducir el nombre de usuario y la contraseña al iniciar sesión en iDRAC. Esto es de utilidad a la hora de configurar secuencia de comandos automatizadas que realizan distintas funciones. Las claves cargadas deben tener el formato RFC 4716 u openssh. De lo contrario, deberá convertir las claves a ese formato.

En cualquier situación, un par de claves privada y pública se debe generar en la estación de administración. La clave pública se carga en el usuario local de iDRAC y la clave privada la utiliza el cliente SSH para establecer la relación de confianza entre la estación de administración e iDRAC.

Puede generar el par de claves pública o privada mediante los elementos siguientes:

- La aplicación *Generador de clave PuTTY* para clientes que ejecutan Windows
- La CLI *ssh-keygen* para clientes que ejecutan Linux.

△ PRECAUCIÓN: Este privilegio normalmente se reserva para los usuarios que son miembros del grupo de usuarios Administrador en iDRAC. No obstante, los usuarios del grupo Personalizado pueden recibir este privilegio. Un usuario con este privilegio puede configurar la configuración de cualquier usuario. Esto incluye la creación o eliminación de usuarios, la administración de claves SSH para usuarios, etc. Por estos motivos, tenga cuidado a la hora de asignar este privilegio.

△ PRECAUCIÓN: La capacidad para cargar, ver o eliminar las claves SSH se basa en el privilegio 'Configurar usuarios'. Este privilegio permite a los usuarios configurar la clave SSH de otros usuarios. Debe tener cuidado a la hora de otorgar este privilegio.

Generación de claves públicas para Windows


Para usar la aplicación *generador de claves PuTTY* y crear la clave básica:

1. Inicie la aplicación y seleccione SSH-2 RSA o SSH-2 DSA como tipo de clave para generar (SSH-1 no se admite). Los algoritmos de generación de clave admitidos son RSA y DSA únicamente.
2. Introduzca el número de bits para la clave. Para RSA, introduzca entre 768 y 4096 bits y para DSA, introduzca 1024.
3. Haga clic en **Generar** y mueva el mouse dentro de la ventana como se indica.
Se generan las claves.
4. Puede modificar el campo de comentario de la clave.
5. Introduzca una frase de contraseña para proteger la clave.
6. Guarde la clave pública y privada.


Generación de claves públicas para Linux


Para utilizar la aplicación *ssh-keygen* y crear la clave básica, abra la ventana de terminal y en el símbolo del sistema del shell, introduzca `ssh-keygen -t rsa -b 1024 -C testing` donde:

- `-t` es *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.

 **NOTA:** Las opciones distinguen entre mayúsculas y minúsculas.

Siga las instrucciones. Una vez que se ejecute el comando, cargue el archivo público.

 **PRECAUCIÓN:** Las claves generadas desde la estación de administración de Linux management mediante *ssh-keygen* tienen un formato distinto de 4716. Convierta las claves al formato 4716 mediante `ssh-keygen -e -f /root/.ssh/id_rsa.pub > std_rsa.pub`. No cambie los permisos del archivo de clave. La conversión debe realizarse con los permisos predeterminados.

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

Carga de claves SSH

Puede cargar hasta cuatro claves públicas *por usuario* para utilizar sobre una interfaz SSH. Antes de agregar las claves públicas, asegúrese de comprobar que las claves están configuradas, de modo que la clave no se sobrescriba accidentalmente.

Al agregar claves públicas nuevas, asegúrese de que las claves existentes no se encuentren en el índice en el que se agrega la clave nueva. iDRAC no realiza ninguna comprobación para asegurarse de que las claves anteriores se eliminen antes de agregar claves nuevas. Cuando se agrega una clave nueva, se puede utilizar si la interfaz SSH está activada.

Carga de claves SSH mediante la interfaz web

Para cargar las claves SSH:


1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Configuración de iDRAC** → **Red** → **Autenticación de usuario** → **Usuarios locales**.

Se muestra la página **Users (Usuarios)**.

2. En la columna **Identificación de usuario**, haga clic en un número de identificación de usuario. Aparece la página **Menú principal de usuarios**.
 3. En **Configuración de claves SSH**, seleccione **Cargar claves SSH** y haga clic en **Siguiente**. Aparece la página **Cargar claves SSH**.
 4. Cargue las claves SSH de una de las maneras siguientes:
 - Cargue el archivo clave.
 - Copie del contenido del archivo de claves en el cuadro de texto
- Para obtener más información, consulte la Ayuda en línea de iDRAC.
5. Haga clic en **Apply (Aplicar)**.

Carga de claves SSH mediante RACADM


Para cargar las claves SSH, ejecute el siguiente comando:

 **NOTA:** No es posible cargar y copiar una clave al mismo tiempo.

- Para RACADM local: `racadm sshpkauth -i <2 to 16> -k <1 to 4> -f <filename>`
- Desde RACADM remoto mediante Telnet o SSH: `racadm sshpkauth -i <2 to 16> -k <1 to 4> -t <key-text>`

Por ejemplo, para cargar una clave válida al ID 2 de usuario de iDRAC en el primer espacio de clave mediante un archivo, ejecute el comando siguiente:

```
$ racadm sshpkauth -i 2 -k 1 -f pkkey.key
```

 **NOTA:** La opción `-f` no se admite en RACADM Telnet/SSH/serie.

Visualización de claves SSH

Es posible ver las claves cargadas en iDRAC.

Visualización de claves SSH mediante la interfaz web

Para ver las claves SSH:

1. En la interfaz web, vaya a **Información general** → **Configuración de iDRAC** → **Red** → **Autenticación de usuario** → **Usuarios locales**. Se muestra la página **Users (Usuarios)**.
2. En la columna **Identificación de usuario**, haga clic en un número de identificación de usuario. Aparece la página **Menú principal de usuarios**.
3. En **Configuración de claves SSH**, seleccione **Ver o quitar las claves SSH** y haga clic en **Siguiente**. Se muestra la página **Ver o quitar las claves SSH** con los detalles de la clave.

Visualización de claves SSH mediante RACADM

Si desea ver las claves SSH, ejecute el siguiente comando:

- Clave específica: `racadm sshpkauth -i <2 a 16> -v -k <1 a 4>`
- Todas las claves: `racadm sshpkauth -i <2 a 16> -v -k all`

Eliminación de claves SSH

Antes de eliminar las claves públicas, asegúrese de visualizarlas para comprobar que están configuradas, de modo que no se eliminen accidentalmente.

Eliminación de claves SSH mediante la interfaz web

Para eliminar las claves SSH

1. En la interfaz web, vaya a **Información general** → **Configuración de iDRAC** → **Red** → **Autenticación de usuario** → **Usuarios locales**.
Se muestra la página **Users (Usuarios)**.
2. En la columna **Identificación de usuario**, haga clic en un número de identificación de usuario.
Aparece la página **Menú principal de usuarios**.
3. En **Configuración de claves SSH**, seleccione **Ver o quitar las claves SSH** y haga clic en **Siguiente**.
Se muestra la página **Ver o quitar las claves SSH** con los detalles de la clave.
4. Seleccione **Quitar** para las claves que desea eliminar y haga clic en **Aplicar**.
Se eliminan las claves seleccionadas.

Eliminación de claves SSH mediante RACADM

Para eliminar las claves SSH, ejecute los comandos siguientes:

- Clave específica: `racadm sshpkauth -i <2 to 16> -d -k <1 to 4>`
- Todas las claves: `racadm sshpkauth -i <2 to 16> -d -k all`

Configuración de cuentas de usuario y privilegios

Puede configurar las cuentas de usuario con privilegios específicos (*autoridad basada en roles*) para administrar el sistema mediante iDRAC y mantener la seguridad del sistema. De manera predeterminada, iDRAC está configurado con una cuenta de administrador local. Este nombre de usuario predeterminado es *root* y la contraseña es *calvin*. Como administrador, puede configurar cuentas de usuario para permitir que otros usuarios accedan a iDRAC.

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

iDRAC admite el acceso basado en roles para los usuarios con un conjunto de privilegios asociados. Los roles son: administrador, operador, solo lectura o ninguno. El rol define los privilegios máximos disponibles.

Enlaces relacionados


[Configuración de usuarios locales](#)

[Configuración de usuarios de Active Directory](#)

[Configuración de los usuarios LDAP genéricos](#)


Configuración de usuarios locales

Puede configurar hasta 16 usuarios locales en iDRAC con permisos de acceso específicos. Antes de crear un usuario de iDRAC, compruebe si existen usuarios actuales. Puede establecer los nombres de usuario, las contraseñas y las funciones con privilegios para estos usuarios. Los nombres de usuario y las contraseñas se pueden cambiar mediante cualquiera de las interfaces seguras de iDRAC (es decir, la interfaz web, RACADM o WS-MAN). También puede activar o desactivar la autenticación de SNMPv3 para cada usuario.

 **NOTA:** La función de SNMPv3 requiere una licencia y está disponible con la licencia Enterprise de iDRAC.

Configuración de usuarios locales mediante la interfaz web de iDRAC

Para agregar y configurar usuarios de iDRAC locales:

 **NOTA:** Debe tener el permiso Configurar usuarios para poder crear usuarios en iDRAC.

1. En la interfaz web de iDRAC, vaya a **Información general** → **Configuración de iDRAC** → **Autenticación de usuario** → **Usuarios locales**.

Aparece la página **Usuarios**.

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



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

Aparece la página **Menú principal de usuarios**.

3. Seleccione **Configurar** y luego haga clic en **Siguiente**.

Se muestra la página **Configuración de usuario**.

4. Active la identificación de usuario y especifique el nombre de usuario, la contraseña y los privilegios de acceso del usuario. También es posible activar la autenticación de SNMPv3 para el usuario. Para obtener más información sobre las opciones, consulte la *Ayuda en línea de iDRAC*.
5. Haga clic en **Aplicar**. El usuario se crea con los privilegios necesarios.

Configuración de los usuarios locales mediante RACADM



NOTA: Se debe haber iniciado sesión como usuario **root** para ejecutar los comandos de RACADM en un sistema remoto con Linux.

Puede configurar uno o varios usuarios de iDRAC mediante RACADM.

Para configurar varios usuarios de iDRAC con valores de configuración idénticos, realice uno de los siguientes procedimientos:

- Use los ejemplos de RACADM de esta sección como guía para crear un archivo de proceso por lotes de comandos RACADM y después ejecute el archivo de proceso por lotes en cada sistema administrado.
- Cree el archivo de configuración de iDRAC y ejecute el subcomando **racadm config** o **racadm set** en cada sistema administrado con el mismo archivo de configuración.

Si está configurando un nuevo iDRAC o ha utilizado el comando **racadm racresetcfg**, el único usuario actual es el usuario `root` con la contraseña `calvin`. El subcomando **racresetcfg** restablece iDRAC a los valores predeterminados.



NOTA: Los usuarios se pueden activar o desactivar con el transcurso del tiempo. Por este motivo, un usuario puede tener un número de índice diferente en cada iDRAC.

Para verificar si el usuario existe, escriba el comando siguiente en el símbolo del sistema:

- Mediante el comando **config**: `racadm getconfig -u <username>`

o

Escriba el siguiente comando una vez para cada índice (de 1 a 16):

- Mediante el comando **config**: `racadm getconfig -g cfgUserAdmin -i <index>`
- Mediante el comando **get**: `racadm get iDRAC.Users.<index>.UserName`



NOTA: También puede escribir `racadm getconfig -f <myfile.cfg>` o `racadm get -f <myfile.cfg>` y ver o editar el archivo **myfile.cfg**, que incluye todos los parámetros de configuración de iDRAC.

Varios parámetros e ID de objeto se muestran con sus valores actuales. Los objetos importantes son los siguientes:

- Si ha utilizado el comando **getconfig**:

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

- Si ha utilizado el comando **get**:

```
iDRAC.Users.UserName=
```

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

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

Tenga en cuenta que el objeto **cfgUserAdminIndex** que aparece en el ejemplo anterior contiene el carácter '#'. Esto indica que es un objeto de solo lectura. Asimismo, si utiliza el comando **racadm config -f racadm.cfg** para especificar cualquier número de grupos u objetos para escritura, el índice no se puede especificar. Este comportamiento permite una mayor flexibilidad a la hora de configurar varios iDRAC con los mismos valores.

Para activar la autenticación de SNMPv3 para un usuario, use objetos **SNMPv3AuthenticationType**, **SNMPv3Enable** y **SNMPv3PrivacyType**. Para obtener más información, consulte *RACADM Command Line Interface Guide* (Guía de referencia de la interfaz de línea de comandos RACADM), disponible en dell.com/esmanuals.

Si utiliza el archivo XML de configuración, utilice los atributos **AuthenticationProtocol**, **ProtocolEnable** y **PrivacyProtocol** para activar la autenticación de SNMPv3.

Cómo agregar un usuario iDRAC mediante RACADM

Para agregar un nuevo usuario a la configuración RAC, realice los pasos siguientes:

1. Establezca el nombre de usuario.
2. Establezca la contraseña.
3. Establezca los siguientes privilegios del usuario:
 - iDRAC
 - LAN
 - Serial Port
 - Comunicación en serie en la LAN
4. Active el usuario.

Ejemplo:

El siguiente ejemplo describe cómo agregar un nuevo usuario de nombre "John" con la contraseña "123456" y privilegios de inicio de sesión en el RAC.

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i 3 john
racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i 3 123456
racadm config -g cfgUserAdmin -i 3 -o cfgUserAdminPrivilege 0x00000001
racadm config -g cfgUserAdmin -i 3 -o cfgUserAdminIpmiLanPrivilege 2
racadm config -g cfgUserAdmin -i 3 -o cfgUserAdminIpmiSerialPrivilege 2
racadm config -g cfgUserAdmin -i 3 -o cfgUserAdminSolEnable 1
racadm config -g cfgUserAdmin -i 3 -o cfgUserAdminEnable 1
```


Para verificarlo, use uno de los siguientes comandos:

```
racadm getconfig -u john
racadm getconfig -g cfgUserAdmin -i 3
```


Para obtener más información sobre los comandos RACADM, consulte *iDRAC8 RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8), disponible en dell.com/support/manuals.

Activación del usuario iDRAC mediante permisos

Para activar un usuario con permisos administrativos específicos (autoridad basada en funciones):


 **NOTA:** Puede utilizar los comandos **getconfig** y **config** o los comandos **get** y **set**.

1. Busque un índice de usuario disponible mediante la sintaxis de comando siguiente:
 - Mediante el comando **getconfig**: `racadm getconfig -g cfgUserAdmin -i <index>`
 - Mediante el comando **get**: `racadm get iDRAC.Users <index>`
2. Escriba los comandos siguientes con el nombre de usuario y la contraseña nuevos.
 - Mediante el comando **config**: `racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i <index> <user privilege bitmask value>`
 - Mediante el comando **set**: `racadm set iDRAC.Users.<index>.Privilege <user privilege bitmask value>`

 **NOTA:** Para obtener una lista de los valores de máscara de bits válidos para privilegios de usuario específicos, consulte *iDRAC8 RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8) disponible en dell.com/support/manuals. El valor de privilegio predeterminado es 0, lo que indica que el usuario no tiene activado ningún privilegio.

Configuración de usuarios de Active Directory

Si la empresa utiliza el software Microsoft Active Directory, puede configurarlo para proporcionar acceso a iDRAC, lo que permite agregar y controlar los privilegios de usuario iDRAC para los usuarios existentes en el servicio de directorio. Esta función requiere una licencia.

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

Puede configurar la autenticación de usuario a través de Active Directory para iniciar sesión en el iDRAC. También puede proporcionar autorización basada en roles, lo que permite a un administrador configurar privilegios específicos para cada usuario.

Los nombres de roles y privilegios de iDRAC han cambiado de la generación anterior de servidores. Los nombres de rol son los siguientes:

Tabla 12. Roles de iDRAC

Generación actual	Generación anterior	Privilegios
Administrador	Administrador	Inicio de sesión, Configurar, Configurar usuarios, Registros, Control del sistema, Acceder a la consola virtual, Acceder a medios virtuales, Operaciones del sistema, Depuración
Operador	Usuario avanzado	Inicio de sesión, Configurar, Control del sistema, Acceder a la consola virtual, Acceder a medios virtuales, Operaciones del sistema, Depuración
Read Onlu (Solo lectura)	Usuario invitado	Inicio de sesión
Ninguno	Ninguno	Ninguno

Tabla 13. Privilegios del usuario del iDRAC

Generación actual	Generación anterior	Descripción
Inicio de sesión	Inicio de sesión en iDRAC	Permite al usuario iniciar sesión en el iDRAC.
Configurar	Configurar iDRAC	Permite al usuario configurar el iDRAC.
Configurar usuarios	Configurar usuarios	Permite activar la capacidad del usuario de otorgar permisos de acceso al sistema a usuarios específicos.
Registros	Borrar registros	Permite al usuario borrar el registro de sucesos del sistema (SEL).
Control del sistema	Ejecutar comandos de control del servidor	Permite ejecutar un ciclo de energía en el sistema host.
Acceder a la consola virtual	Redirección de acceso a la consola virtual (para servidores Blade) Acceder a la consola virtual (para servidores tipo bastidor y torre)	Permite al usuario ejecutar la consola virtual.
Acceder a los medios virtuales	Acceder a los medios virtuales	Permite al usuario ejecutar y usar los medios virtuales.

Generación actual	Generación anterior	Descripción
Operaciones del sistema	Probar alertas	Permite sucesos iniciados y generados por usuario. La información se envía como una notificación asincrónica y registrada.
Depuración	Ejecutar comandos de diagnóstico	Permite al usuario ejecutar comandos de diagnóstico.

Enlaces relacionados

- [Prerrequisitos del uso de la autenticación de Active Directory para iDRAC](#)
- [Mecanismos de autenticación compatibles de Active Directory](#)

Prerrequisitos del uso de la autenticación de Active Directory para iDRAC

Para utilizar la función de autenticación de Active Directory de iDRAC, asegúrese de haber realizado lo siguiente:

- Implementado una infraestructura de Active Directory. Consulte el sitio web de Microsoft para obtener más información.
- Incorporado PKI en la infraestructura de Active Directory. iDRAC utiliza el mecanismo de infraestructura de claves públicas (PKI) estándar para la autenticación segura en Active Directory. Consulte el sitio web de Microsoft para obtener más información.
- Activado Capa de sockets seguros (SSL) en todas las controladoras de dominio a las que se conecta iDRAC para la autenticación en todas las controladoras de dominio.

Enlaces relacionados

- [Activación de SSL en una controladora de dominio](#)

Activación de SSL en una controladora de dominio

Cuando iDRAC autentica los usuarios en una controladora de dominio de Active Directory, inicia una sesión SSL en la controladora de dominio. En este momento, la controladora debe publicar un certificado firmado por la autoridad de certificados (CA), el certificado raíz que también se carga en iDRAC. Para que iDRAC autentique *cualquier* controladora de dominio (ya sea la raíz o la controladora de dominio secundaria), dicha controladora de dominio debe tener un certificado habilitado para SSL firmado por la CA del dominio.

Si utiliza la CA raíz empresarial de Microsoft para asignar *automáticamente* todas las controladoras de dominio a un certificado SSL, deberá realizar lo siguiente:

1. Instalar el certificado SSL en cada controladora de dominio.
2. Exportar el certificado de CA raíz de la controladora de dominio a iDRAC.
3. Importar el certificado SSL del firmware de iDRAC.

Enlaces relacionados


- [Instalación de un certificado SSL para cada controladora de dominio](#)
- [Exportación de un certificado de CA raíz de la controladora de dominio a iDRAC](#)
- [Importación del certificado SSL de firmware de iDRAC](#)

Instalación de un certificado SSL para cada controladora de dominio

Para instalar el certificado SSL para cada controladora:

1. Haga clic en **Inicio** → **Herramientas administrativas** → **Política de seguridad de dominio**.
2. Expanda la carpeta **Políticas 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**.
Aparece el **Asistente para instalación de petición automática de certificado**.
3. Haga clic en **Siguiente** y seleccione **Controladora de dominio**.
4. Haga clic en **Siguiente** y seleccione **Terminar**. Se instala el certificado SSL.

Exportación de un certificado de CA raíz de la controladora de dominio a iDRAC

 **NOTA:** Si el sistema ejecuta Windows 2000 o si está utilizando una CA independiente, los siguientes pasos pueden variar.

Para exportar el certificado de CA raíz de la controladora de dominio a iDRAC.

1. Localice la controladora de dominio que ejecuta el servicio de CA de Microsoft Enterprise.
2. Haga clic en **Inicio** → **Ejecutar**.
3. 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 o quitar complemento**.
5. En la ventana **Agregar o quitar complemento**, haga clic en **Agregar**.
6. En la ventana **Complemento independiente**, seleccione **Certificados** y haga clic en **Agregar**.
7. Seleccione el **Equipo** y haga clic en **Siguiente**.
8. Seleccione **Equipo local**, haga clic en **Terminar** y, a continuación, en **Aceptar**.
9. En la ventana **Consola 1**, vaya a la carpeta **Certificados Personal Certificados**.
10. Localice el certificado de CA raíz y haga clic con el botón derecho del mouse sobre ese elemento. Seleccione **Todas las tareas** y haga clic en **Exportar...**
11. En el **Asistente de exportación de certificados**, haga clic en **Siguiente** y seleccione **No exportar la clave privada**.
12. Haga clic en **Siguiente** y seleccione **Codificado en base 64 X.509 (.cer)** como el formato.
13. Haga clic en **Siguiente** y guarde el certificado en un directorio del sistema.
14. Cargue el certificado guardado en el paso 13 en iDRAC.

Importación del certificado SSL de firmware de iDRAC

El certificado SSL de iDRAC es el certificado idéntico que se utiliza para el servidor web iDRAC. Todas las controladoras iDRAC se entregan con un certificado autofirmado predeterminado.

Si el servidor de Active Directory no se ha configurado para autenticar el cliente durante la inicialización de una sesión SSL, deberá cargar el certificado del servidor de iDRAC en la controladora de dominio de Active Directory. Este paso adicional no es necesario si Active Directory no realiza la autenticación 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 del firmware de iDRAC es firmado por una CA y el certificado de esta ya se encuentra en la lista Entidades emisoras raíz de confianza de la controladora de dominio, no realice los pasos que se describen en esta sección.

Para importar el certificado SSL del firmware iDRAC en todas las listas de certificado seguras de la controladora de dominio:

1. Descargue el certificado SSL de iDRAC mediante el comando RACADM siguiente:
`racadm sslcertdownload -t 0x1 -f <RAC SSL certificate>`
2. En la controladora de 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 de iDRAC en la lista **Autoridades de certificación raíz de confianza** de cada controladora de dominio.
Si ha instalado un certificado propio, asegúrese de que la CA que lo firma figure en la lista **Entidades emisoras raíz de confianza**. De lo contrario, deberá instalarlo en todas las controladoras 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, a continuación, en **Aceptar**. El certificado SSL del firmware de iDRAC se importa a todas las listas de certificado de confianza de controladoras de dominio.

Mecanismos de autenticación compatibles de Active Directory

Es posible utilizar Active Directory para definir el acceso de usuario a iDRAC mediante dos métodos:

- La solución del *esquema estándar*, que solo utiliza objetos de grupo de Active Directory.
- La solución del *esquema extendido*, que contiene objetos de Active Directory personalizados. Todos los objetos de control de acceso se mantienen en Active Directory. Esto proporciona una flexibilidad máxima a la hora de configurar el acceso de usuario en distintos iDRAC con niveles de privilegios variados.

Enlaces relacionados

[Descripción general del esquema estándar de Active Directory](#)

[Descripción general del esquema extendido de Active Directory](#)

Descripción general del esquema estándar de Active Directory

Como se muestra en la figura a continuación, el uso del esquema estándar para la integración de Active Directory requiere la configuración tanto en Active Directory como en el iDRAC.

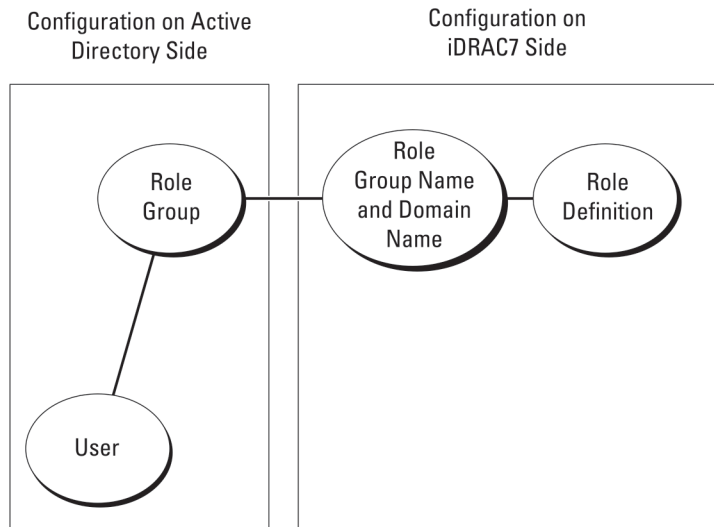



Ilustración 1. Configuración de iDRAC con el esquema estándar de Active Directory

En Active Directory, un objeto de grupo estándar se utiliza como grupo de funciones. Un usuario con acceso a iDRAC es miembro del grupo de funciones. Para conceder a este usuario acceso a un iDRAC específico, el nombre del grupo de funciones y su nombre de dominio deben configurarse en el iDRAC específico. La función y el nivel de privilegios se definen en cada iDRAC y no en Active Directory. Es posible configurar hasta cinco grupos de funciones en cada iDRAC. En la tabla de referencia se muestran los privilegios predeterminados del grupo de funciones.

Tabla 14. Privilegios predeterminados del grupo de roles

Grupos de funciones	Nivel predeterminado de privilegios	Permisos otorgados	Máscara de bits
Grupo de roles 1	Ninguno	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 roles 2	Ninguno	Iniciar sesión en el iDRAC, Configurar el iDRAC, Ejecutar comandos de control del servidor, Acceder a la consola virtual, Acceder a los medios virtuales, Probar alertas, Ejecutar comandos de diagnóstico	0x000000f9

Grupos de funciones	Nivel predeterminado de privilegios	Permisos otorgados	Máscara de bits
Grupo de roles 3	Ninguno	Inicio de sesión en iDRAC	0x00000001
Grupo de roles 4	Ninguno	Sin permisos asignados	0x00000000
Grupo de roles 5	Ninguno	Sin permisos asignados	0x00000000

 **NOTA:** Los valores de la máscara de bits se utilizan únicamente cuando se establece el esquema estándar con RACADM.

Casos de dominio único y dominio múltiple

Si todos los usuarios y grupos de roles de inicio de sesión, incluidos los grupos anidados, se encuentran en el mismo dominio, solamente es necesario configurar las direcciones de las controladoras de dominio en iDRAC. En este caso de dominio único, se admite cualquier tipo de grupo.

Si todos los usuarios o grupos de roles de inicio de sesión, o cualquiera de los grupos anidados, provienen de dominios múltiples, se deberán configurar las direcciones del servidor de catálogo global en iDRAC. En este caso de dominio múltiple, todos los grupos de roles y grupos anidados, si los hay, deben ser del tipo Grupo universal.

Configuración del esquema estándar de Active Directory


Si desea configurar iDRAC para un acceso de inicio de sesión de Active Directory:

1. En un servidor de Active Directory (controladora de dominio), abra el complemento Usuarios y equipos de Active Directory.
2. Cree un grupo o seleccione un grupo existente. Agregue el usuario de Active Directory como miembro del grupo de Active Directory para acceder a iDRAC.
3. Configure el nombre del grupo, el nombre del dominio y los privilegios de rol en iDRAC mediante la interfaz web de iDRAC Web o RACADM.

Enlaces relacionados

- [Configuración de Active Directory con el esquema estándar mediante la interfaz web de iDRAC](#)
- [Configuración de Active Directory con esquema estándar vía RACADM](#)

Configuración de Active Directory con el esquema estándar mediante la interfaz web de iDRAC

 **NOTA:** Para obtener información acerca de los distintos campos, consulte la *Ayuda en línea de iDRAC*.

1. En la interfaz web de iDRAC, vaya a **Información general** → **Configuración de iDRAC** → **Autenticación de usuario** → **Servicios de directorio** → **Microsoft Active Directory**. Aparece la página de resumen de **Active Directory**.
2. Haga clic en **Configurar Active Directory**. Aparece la página **Paso 1 de 4 de Configuración y administración de Active Directory**.
3. Opcionalmente, active la validación de certificados y cargue el certificado digital firmado por la CA que se ha utilizado durante la instalación de las conexiones SSL al comunicarse con el servidor de Active Directory (AD). Para ello, se deben especificar las controladoras de dominio y el FQDN de

catálogo global. Esto se realiza en los próximos pasos. Por tanto, el DNS debería configurarse correctamente en la configuración de red.

4. Haga clic en **Siguiente**.

Aparece la página **Paso 2 de 4 de Configuración y administración de Active Directory**.

5. Active Active Directory y especifique la información de ubicación acerca de los servidores y las cuentas de usuario de Active Directory. Asimismo, especifique el tiempo que iDRAC debe esperar para recibir las respuestas de Active Directory durante el inicio de sesión de iDRAC.



NOTA: Si está activada la validación de certificados, especifique las direcciones de servidor de controladora de dominio y el FQDN de catálogo global. Asegúrese de que el DNS está configurado correctamente bajo **Información general** → **Configuración de iDRAC** → **Red**.

6. Haga clic en **Siguiente**. Aparece la página **Paso 3 de 4 de Configuración y administración de Active Directory**.

7. Seleccione **Esquema estándar** y haga clic en **Siguiente**.

Aparece la página **Paso 4a de 4 de Configuración y administración de Active Directory**.

8. Introduzca la ubicación de los servidores de catálogo global de Active Directory y especifique los grupos de privilegios que se utilizan para autorizar a los usuarios.

9. Haga clic en **Grupo de roles** para configurar la política de autorización de control para los usuarios bajo el modo de esquema estándar.

Aparece la página **Paso 4b de 4 de Configuración y administración de Active Directory**.

10. Especifique los privilegios y haga clic en **Aplicar**.

Se aplica la configuración y aparece la página **Paso 4a de 4 de Configuración y administración de Active Directory**.

11. Haga clic en **Terminar**. Se habrán configurado los valores de Active Directory para el esquema estándar.

Configuración de Active Directory con esquema estándar vía RACADM

Para configurar iDRAC Active Directory con esquema estándar a través de RACADM:

1. En el símbolo del sistema racadm, ejecute los comandos siguientes:

- Mediante el comando **config**:

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1 racadm config -g
cfgActiveDirectory -o cfgADType 2 racadm config -g cfgStandardSchema -i
<index> -o cfgSSADRoleGroupName <common name of the role group> racadm
config -g cfgStandardSchema -i <index> -o cfgSSADRoleGroupDomain <fully
qualified domain name> racadm config -g cfgStandardSchema -i <index> -o
cfgSSADRoleGroupPrivilege <Bit Mask Value for specific RoleGroup
permissions> racadm config -g cfgActiveDirectory -o
cfgADDomainController1 <fully qualified domain name or IP address of the
domain controller> racadm config -g cfgActiveDirectory -o
cfgADDomainController2 <fully qualified domain name or IP address of the
domain controller> racadm config -g cfgActiveDirectory -o
cfgADDomainController3 <fully qualified domain name or IP address of the
domain controller> racadm config -g cfgActiveDirectory -o
cfgADGlobalCatalog1 <fully qualified domain name or IP address of the
domain controller> racadm config -g cfgActiveDirectory -o
cfgADGlobalCatalog2 <fully qualified domain name or IP address of the
domain controller> racadm config -g cfgActiveDirectory -o
cfgADGlobalCatalog3 <fully qualified domain name or IP address of the
domain controller>
```

- Mediante el comando **set**:

```
racadm set iDRAC.ActiveDirectory.Enable 1 racadm set
iDRAC.ActiveDirectory.Schema 2 racadm set iDRAC.ADGroup.Name <common name
of the role group> racadm set iDRAC.ADGroup.Domain <fully qualified
domain name> racadm set iDRAC.ADGroup.Privilege <Bit Mask Value for
specific RoleGroup permissions> racadm set
iDRAC.ActiveDirectory.DomainController1 <fully qualified domain name or
IP address of the domain controller> racadm set
iDRAC.ActiveDirectory.DomainController2 <fully qualified domain name or
IP address of the domain controller> racadm set
iDRAC.ActiveDirectory.DomainController3 <fully qualified domain name or
IP address of the domain controller> racadm set
iDRAC.ActiveDirectory.GlobalCatalog1 <fully qualified domain name or IP
address of the domain controller> racadm set
iDRAC.ActiveDirectory.GlobalCatalog2 <fully qualified domain name or IP
address of the domain controller> racadm set
iDRAC.ActiveDirectory.GlobalCatalog3 <fully qualified domain name or IP
address of the domain controller>
```

Para valores de máscara de bit para permisos de grupo de roles específicos, consulte [Privilegios predeterminados del grupo de roles](#).

Introduzca el FQDN de la controladora de dominio, no el FQDN del dominio. Por ejemplo, introduzca `servername.dell.com` en lugar de `dell.com`.

Al menos una de las tres direcciones se debe configurar. iDRAC intenta conectar cada una de las direcciones configuradas una a la vez hasta que establezca una conexión correcta. Con el esquema estándar, estas son las direcciones de las controladoras de dominio en las que se encuentran las cuentas de usuario y los grupos de roles.

El servidor de catálogo global solo se requiere para el esquema estándar cuando las cuentas de usuario y los grupos de roles se encuentran en dominios distintos. En el caso de dominio múltiple, solamente se puede usar el grupo universal.

La dirección IP o el FQDN que especifique en este campo debe concordar con el campo Sujeto o Nombre alternativo de sujeto del certificado de controladora de dominio si tiene activada la validación de certificados.

Si desea desactivar la validación del certificado durante el protocolo de enlace con SSL, ingrese el siguiente comando de RACADM:

- Mediante el comando **config**: `racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0`
- Mediante el comando **set**: `racadm set iDRAC.ActiveDirectory.CertValidationEnable 0`

En este caso, no es necesario cargar ningún certificado de CA.

Para aplicar la validación de certificado durante el protocolo de enlace SSL (opcional):

- Mediante el comando **config**: `racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1`
- Mediante el comando **set**: `racadm set iDRAC.ActiveDirectory.CertValidationEnable 1`

En este caso, también debe cargar el certificado de CA con el siguiente comando de RACADM:

```
racadm sslcertupload -t 0x2 -f <ADS root CA certificate>
```



NOTA: Si la validación de certificados está activada, especifique las direcciones del servidor de la controladora de dominio y el FQDN de catálogo global. Asegúrese de que el DNS esté configurado correctamente en **Descripción general** → **Configuración de iDRAC** → **Red**.

El siguiente comando de RACADM es opcional.

```
racadm sslcertdownload -t 0x1 -f <RAC SSL certificate>
```

2. Si DHCP está activado en el iDRAC y desea utilizar el DNS proporcionado por el servidor DHCP, introduzca los siguientes comandos de RACADM:

- Mediante el comando **config**: `racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 1`
- Mediante el comando **set**: `racadm set iDRAC.IPv4.DNSFromDHCP 1`

3. Si DHCP está desactivado en iDRAC o si desea introducir manualmente la dirección IP de DNS, introduzca los siguientes comandos RACADM:

- Mediante el comando **config**:

```
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0 racadm config -g cfgLanNetworking -o cfgDNSServer1 <primary DNS IP address> racadm config -g cfgLanNetworking -o cfgDNSServer2 <secondary DNS IP address>
```
- Mediante el comando **set**:

```
racadm set iDRAC.IPv4.DNSFromDHCP 0 racadm set iDRAC.IPv4.DNSFromDHCP.DNS1 <primary DNS IP address> racadm set iDRAC.IPv4.DNSFromDHCP.DNS2 <secondary DNS IP address>
```

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:

- Mediante el comando **config**: `racadm config -g cfgUserDomain -o cfgUserDomainName <fully qualified domain name or IP Address of the domain controller> -i <index>`
- Mediante el comando **set**: `racadm set iDRAC.UserDomain.<index>.Name <fully qualified domain name or IP Address of the domain controller>`

Puede configurar hasta 40 dominios de usuario con números de índice entre 1 y 40.

Descripción general del esquema extendido de Active Directory

El uso del esquema extendido requiere la extensión del esquema de Active Directory.

Extensiones de esquema de Active Directory

Los datos de Active Directory constituyen 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. Entre algunos ejemplos de atributos de clase de usuario se encuentran el nombre del usuario, sus apellidos, su número de teléfono. etc. Puede extender la base de datos de Active Directory si agrega sus propios *atributos* y *clases* únicos para satisfacer requisitos específicos. Dell ha extendido el esquema para incluir los cambios necesarios y admitir la autenticación y la autorización de la administración remota mediante Active Directory.

Cada *atributo* o *clase* que se agrega a un esquema de Active Directory debe definirse con un ID único. Para mantener los ID únicos en todo el sector, Microsoft mantiene una base de datos de identificadores de objetos de Active Directory (OID) de modo que cuando las empresas agregan extensiones al esquema,

pueden tener la garantía de que serán únicos y no entrarán en conflicto entre sí. Para extender el esquema en Microsoft Active Directory, Dell recibe OID únicos, extensiones de nombre únicas e ID de atributos con vínculos únicos para los atributos y las clases que se agregan al servicio de directorio:

- La extensión es: `dell`
- El OID base es: `1.2.840.113556.1.8000.1280`
- El rango del LinkID de RAC es: `12070` a `12079`

Descripción general sobre las extensiones de esquema de iDRAC

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

Para cada dispositivo iDRAC físico en la red que desee integrar con Active Directory para la autenticación y autorización, cree al menos un objeto de asociación y un objeto de dispositivo iDRAC. Puede crear varios objetos de asociación y cada uno de ellos se puede vincular a varios usuarios, grupos de usuarios u objetos de dispositivo iDRAC, según sea necesario. Los usuarios y los grupos de usuarios de iDRAC pueden ser miembros de cualquier dominio en la empresa.

No obstante, cada objeto de asociación se puede vincular (puede vincular usuarios, grupos de usuarios u objetos de dispositivo de iDRAC) a un solo objeto de privilegio. Este ejemplo permite al administrador controlar los privilegios de cada usuario sobre dispositivos iDRAC específicos.

El objeto del dispositivo iDRAC es el vínculo al firmware de iDRAC para consultar Active Directory para la autenticación y autorización. Cuando iDRAC se agrega a la red, el administrador debe configurar iDRAC y su objeto de dispositivo con su nombre de Active Directory de modo que los usuarios puedan realizar la autenticación y autorización con Active Directory. Asimismo, el administrador debe agregar iDRAC al menos a un objeto de asociación para que se autentifiquen los usuarios.

En la figura siguiente se muestra que el objeto de asociación proporciona la conexión necesaria para la autenticación y la autorización.

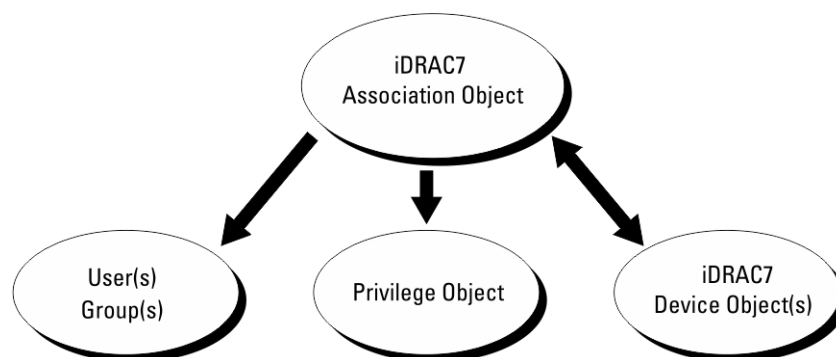


Ilustración 2. Configuración típica de los objetos de Active Directory

Puede crear el número de objetos de asociación necesario. Sin embargo, debe crear al menos un objeto de asociación y debe tener al menos un objeto de dispositivo de iDRAC para cada dispositivo de iDRAC en la red que desee integrar con Active Directory para la autenticación y autorización con iDRAC.

El objeto de asociación permite el número de usuario o grupos necesario, así como objetos de dispositivo de iDRAC. No obstante, el objeto de asociación solo incluye un único objeto de privilegio por objeto de asociación. Este último conecta los usuarios con privilegios en los dispositivos de iDRAC.

La extensión de Dell al complemento ADUC MMC solo permite asociar el objeto de privilegio y objetos iDRAC desde el mismo dominio con el objeto de asociación. La extensión de Dell no permite que un grupo o un objeto iDRAC de otros dominios se agreguen como miembro del producto del objeto de asociación.

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

Los usuarios, los grupos de usuarios o los grupos de usuarios anidados de otros dominios se pueden agregar al objeto de asociación. Las soluciones de esquema extendido admiten cualquier tipo de grupo de usuarios y el anidado de grupos de usuarios entre varios dominios permitidos por Microsoft Active Directory.

Acumulación de privilegios con el esquema extendido

El mecanismo de autenticación de esquema extendido admite la acumulación de privilegios desde distintos objetos de privilegio asociados con el mismo usuario a través de distintos objetos de asociación. Es decir, la autenticación de esquema extendido acumula los privilegios para permitir al usuario disponer del superconjunto de todos los privilegios asignados que correspondan a los objetos de privilegio asociados con el mismo usuario.

En la figura siguiente se proporciona un ejemplo de la acumulación de privilegios mediante el esquema extendido.

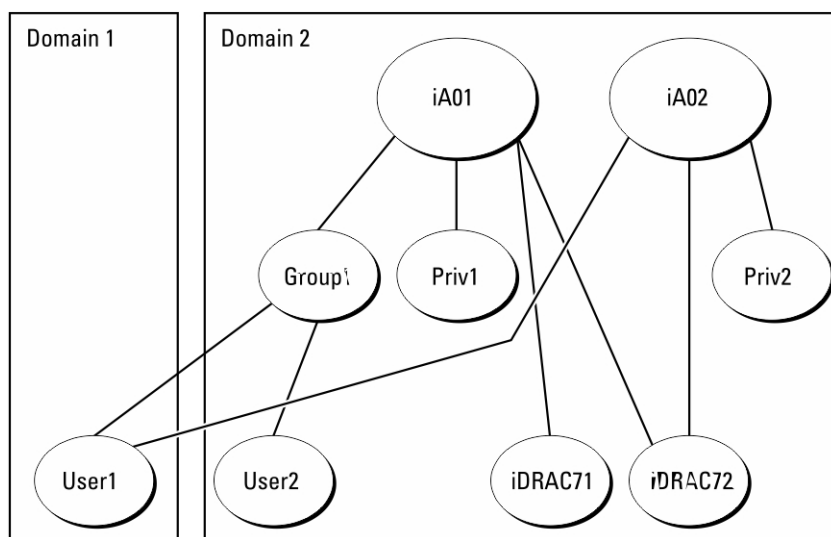


Ilustración 3. Acumulación de privilegios para un usuario

En la figura se muestran dos objetos de asociación, A01 y A02. User1 está asociado a iDRAC2 a través de ambos objetos de asociación.

La autenticación 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 este ejemplo, User1 dispone de los privilegios Priv1 y Priv2 en iDRAC2. User1 dispone de privilegios Priv1 solo en iDRAC1. User2 dispone de privilegios Priv1 en iDRAC1 y en iDRAC2. Asimismo, en esta figura se muestra que User1 puede estar en un dominio diferente y puede ser miembro de un grupo.

Configuración del esquema extendido de Active Directory

Si desea configurar Active Directory para acceder a iDRAC:

1. Amplíe el esquema de Active Directory.
2. Amplíe el complemento Usuarios y equipos de Active Directory.
3. Agregue usuarios iDRAC y sus privilegios en Active Directory.
4. Configure las propiedades de Active Directory de iDRAC mediante la interfaz web de iDRAC o RACADM.

Enlaces relacionados

[Descripción general del esquema extendido de Active Directory](#)

[Instalación de Dell Extension para el complemento Usuarios y equipos de Active Directory](#)


[Cómo agregar usuarios y privilegios de iDRAC a Active Directory](#)


[Configuración de Active Directory con esquema extendido mediante la interfaz web de iDRAC](#)

[Configuración de Active Directory con esquema extendido mediante RACADM](#)

Extensión del esquema de Active Directory

Extender el esquema de Active Directory agrega una unidad organizacional de Dell, clases y atributos de esquema y privilegios y objetos de asociación de ejemplo al esquema de Active Directory. Antes de extender el esquema, asegúrese de disponer los privilegios de administrador de esquemas en propietario del rol FSMO (operación maestra única flexible del esquema maestro) del bosque de dominios.

 **NOTA:** Asegúrese de utilizar la extensión de esquema para este producto que sea diferente de las generaciones anteriores de los productos RAC. El esquema anterior no funciona con este producto.

 **NOTA:** La extensión del nuevo esquema no afecta las versiones anteriores del producto

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 *Herramientas y documentación de Dell Systems Management*, en los siguientes directorios respectivos:

- Unidad de DVD: `\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\LDIF_Files`
- <Unidad 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**.

Puede copiar y ejecutar Schema Extender o los archivos LDIF desde cualquier ubicación.

Uso de Dell Schema Extender

 **PRECAUCIÓN:** Dell Schema Extender utiliza el archivo **SchemaExtenderOem.ini**. Para asegurarse de que la utilidad Dell Schema Extender funcione correctamente, no modifique el nombre de este archivo.

1. En la 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 **Finish (Finalizar)**.

El esquema se extiende. Para comprobar la extensión del esquema, utilice el MMC y el complemento de esquema de Active Directory para verificar que las clases y los atributos [Clases y atributos](#) existen. Consulte la documentación de Microsoft para obtener detalles acerca del uso de MMC y el complemento de esquema de Active Directory.

Clases y atributos

Tabla 15. Definiciones de clases para las clases agregadas al esquema de Active Directory

Nombre de la clase	Número de identificación de objeto asignado (OID)
delliDRACDevice	1.2.840.113556.1.8000.1280.1.7.1.1
delliDRACAssociation	1.2.840.113556.1.8000.1280.1.7.1.2
dellRAC4Privileges	1.2.840.113556.1.8000.1280.1.1.1.3
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5

Tabla 16. Clase dellRacDevice

OID	1.2.840.113556.1.8000.1280.1.7.1.1
Descripción	Representa el dispositivo Dell iDRAC. iDRAC debe configurarse como delliDRACDevice en Active Directory. Esta configuración permite a iDRAC enviar solicitudes LDAP a Active Directory.
Tipo de clase	Clase estructural
SuperClasses	dellProduct
Atributos	dellSchemaVersion

OID	1.2.840.113556.1.8000.1280.1.7.1.1
	dellRacType

Tabla 17. Clase dellDRACAssociationObject

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

Tabla 18. Clase dellRAC4Privileges

OID	1.2.840.113556.1.8000.1280.1.1.1.3
Descripción	Define los privilegios (derechos de autorización) para iDRAC
Tipo de clase	Clase auxiliar
SuperClasses	Ninguno
Atributos	dellIsLoginUser dellIsCardConfigAdmin dellIsUserConfigAdmin dellIsLogClearAdmin dellIsServerResetUser dellIsConsoleRedirectUser dellIsVirtualMediaUser dellIsTestAlertUser dellIsDebugCommandAdmin

Tabla 19. Clase dellPrivileges

OID	1.2.840.113556.1.8000.1280.1.1.1.4
Descripción	Esta clase se usa como una clase de contenedor para los privilegios de Dell (derechos de autorización).
Tipo de clase	Clase estructural
SuperClasses	User (Usuario)
Atributos	dellRAC4Privileges

Tabla 20. Clase dellProduct

OID	1.2.840.113556.1.8000.1280.1.1.1.5
Descripción	La clase principal de la que se derivan todos los productos Dell.
Tipo de clase	Clase estructural
SuperClasses	Equipo
Atributos	dellAssociationMembers

Tabla 21. Lista de atributos agregados al esquema de Active Directory

Nombre del atributo/ Descripción	OID asignado/Identificador de objeto de sintaxis	Con un solo valor
dellPrivilegeMember	1.2.840.113556.1.8000.1280.1.1.2.1	FALSO
Lista de los objetos dellPrivilege que pertenecen a este atributo.	Nombre distintivo (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	
dellProductMembers	1.2.840.113556.1.8000.1280.1.1.2.2	FALSO
Lista de objetos dellRacDevice y DelliDRACDevice que pertenecen a este rol. Este atributo es el vínculo de avance al vínculo de retroceso de dellAssociationMembers.	Nombre distintivo (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	
Identificación de vínculo: 12070		
dellIsLoginUser	1.2.840.113556.1.8000.1280.1.1.2.3	VERDADERO
TRUE si el usuario tiene derechos de inicio de sesión en el dispositivo.	Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	

Nombre del atributo/ Descripción	OID asignado/Identificador de objeto de sintaxis	Con un solo valor
dellIsCardConfigAdmin	1.2.840.113556.1.8000.1280.1.1.2.4	VERDADERO
TRUE si el usuario tiene derechos de configuración de tarjeta en el dispositivo.	Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellIsUserConfigAdmin	1.2.840.113556.1.8000.1280.1.1.2.5	VERDADERO
TRUE si el usuario tiene derechos de configuración de usuario en el dispositivo.	Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellIsLogClearAdmin	1.2.840.113556.1.8000.1280.1.1.2.6	VERDADERO
TRUE si el usuario tiene derechos de borrado de registro en el dispositivo.	Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellIsServerResetUser	1.2.840.113556.1.8000.1280.1.1.2.7	VERDADERO
TRUE si el usuario tiene derechos de restablecimiento de servidor en el dispositivo.	Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellIsConsoleRedirectUser	1.2.840.113556.1.8000.1280.1.1.2.8	VERDADERO
TRUE si el usuario tiene derechos de consola virtual en el dispositivo.	Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellIsVirtualMediaUser	1.2.840.113556.1.8000.1280.1.1.2.9	VERDADERO
TRUE si el usuario tiene derechos de medios virtuales en el dispositivo.	Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellIsTestAlertUser	1.2.840.113556.1.8000.1280.1.1.2.1	VERDADERO
TRUE si el usuario tiene derechos de usuario de alertas de prueba en el dispositivo.	Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	0
dellIsDebugCommandAdmin	1.2.840.113556.1.8000.1280.1.1.2.1	VERDADERO
TRUE si el usuario tiene derechos de administrador de comando de depuración en el dispositivo.	Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	1
dellSchemaVersion	1.2.840.113556.1.8000.1280.1.1.2.1	VERDADERO
La versión del esquema actual se usa para actualizar el esquema.	Cadena de no distinguir mayúsculas de minúsculas	2

Nombre del atributo/ Descripción	OID asignado/Identificador de objeto de sintaxis	Con un solo valor
	(LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	
dellRacType Este atributo es el tipo de RAC actual para el objeto dellIDRACDevice y el vínculo de retroceso al vínculo de avance de dellAssociationObjectMembers .	1.2.840.113556.1.8000.1280.1.1.2.1 3 Cadena de no distinguir mayúsculas de minúsculas (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	VERDADERO
dellAssociationMembers Lista de objetos dellRacDevice y DellIDRACDevice que pertenecen a este rol. Este atributo es el vínculo de avance al vínculo de retroceso dellAssociationMembers. Identificación de vínculo: 12071	1.2.840.113556.1.8000.1280.1.1.2.1 4 Nombre distintivo (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSO

Instalación de Dell Extension para el complemento Usuarios y equipos de Active Directory

Cuando se extiende el esquema en Active Directory, también se debe extender el complemento Usuarios y equipos de Active Directory para que el administrador pueda administrar los dispositivos iDRAC, los usuarios y grupos de usuarios, las asociaciones y los privilegios para iDRAC.

Cuando instala el software de administración de sistemas mediante el DVD *Herramientas y documentación de Dell Systems Management*, puede extender el complemento seleccionando la opción **Complemento Usuarios y equipos de Active Directory** durante el procedimiento de instalación. Consulte la Guía de instalación rápida del software Dell OpenManage para obtener instrucciones adicionales acerca de la instalación del software de administración de sistemas. Para los sistemas operativos de Windows de 64 bits, el instalador del complemento se encuentra en el directorio siguiente:

<Unidad DVD>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_SnapIn64

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

Cómo agregar usuarios y privilegios de iDRAC a Active Directory

Con el complemento Usuarios y equipos de Active Directory extendido de Dell, puede agregar usuarios y privilegios de iDRAC mediante la creación de objetos de dispositivo, asociación y privilegios. Para agregar cada objeto, siga estos pasos:

- Cree un objeto de dispositivo iDRAC
- Cree un objeto de privilegio
- Cree un objeto de asociación

- Agregue los objetos a un objeto de asociación

Enlaces relacionados

- [Adición de objetos a un objeto de asociación](#)
- [Creación de un objeto de dispositivo de iDRAC](#)
- [Creación de un objeto de privilegio](#)
- [Creación de un objeto de asociación](#)


Creación de un objeto de dispositivo de iDRAC

Para crear un objeto de dispositivo de iDRAC:

1. En la ventana **Raíz de consola** de MMC, haga clic con el botón derecho del mouse en un contenedor.
2. Seleccione **Nuevo** → **Opciones avanzadas del objeto Dell Remote Management**.
Se abre la ventana **Nuevo objeto**.
3. Introduzca un nombre para el objeto nuevo. El nombre debe ser idéntico al nombre de iDRAC que se introduce al configurar las propiedades de Active Directory mediante la interfaz web de iDRAC.
4. Seleccione **Objeto de dispositivo de iDRAC** y haga clic en Aceptar.

Creación de un objeto de privilegio


Para crear un objeto de privilegio:

 **NOTA:** Debe crear un objeto de privilegio en el mismo dominio que el objeto de asociación relacionado.

1. En la ventana **Raíz de consola** (MMC), haga clic con el botón derecho del mouse en un contenedor.
2. Seleccione **Nuevo** → **Opciones avanzadas del objeto Dell Remote Management**.
Se abre la ventana **Nuevo objeto**.
3. Introduzca un nombre para el nuevo objeto.
4. Seleccione **Objeto de privilegio** y haga clic en Aceptar.
5. Haga clic con el botón derecho del mouse en el objeto de privilegio que creó y seleccione **Propiedades**.
6. Haga clic en la ficha **Privilegios de administración remota** y asigne los privilegios para el usuario o grupo.

Creación de un objeto de asociación

Para crear un objeto de asociación:

 **NOTA:** El objeto de asociación de iDRAC se deriva de un grupo y su alcance está configurado como 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** → **Opciones avanzadas del objeto Dell Remote Management**.
Se abre la ventana **Nuevo objeto**.
3. Introduzca un nombre para el nuevo objeto y seleccione **Objeto de asociación**.
4. Seleccione el ámbito para el **Objeto de asociación** y haga clic en Aceptar.
5. Proporcione privilegios de acceso a los usuarios autenticados para acceder al objeto de asociación creado.

Enlaces relacionados

- [Concesión de privilegios de acceso a los usuarios para los objetos de asociación](#)

Concesión de privilegios de acceso a los usuarios para los objetos de asociación

Para proporcionar privilegios de acceso a los usuarios autenticados para acceder al objeto de asociación creado:

1. Vaya a **Herramientas administrativas** → **Edición ADSI**. Se muestra la ventana **Edición ADSI**.
2. En el panel derecho, navegue al objeto de asociación creado, haga clic con el botón derecho del mouse y seleccione **Propiedades**.
3. En la ficha **Seguridad**, haga clic en **Agregar**.
4. Escriba `Authenticated Users`, haga clic en **Comprobar nombres** y haga clic en **Aceptar**. Los usuarios autenticados se agregan a la lista **Grupos y nombres de usuario**.
5. Haga clic en **Aceptar**.

Adición de 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 iDRAC o grupos de dispositivos iDRAC.

Puede agregar grupos de usuarios y dispositivos de iDRAC.

Enlaces relacionados

[Adición de usuarios o grupos de usuarios](#)

[Adición de privilegios](#)

[Cómo agregar dispositivos iDRAC o grupos de dispositivos iDRAC](#)

Adición de usuarios o grupos de usuarios

Para agregar usuarios o grupos de usuarios:

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

Adición de privilegios

Para agregar privilegios:

Haga clic en la ficha **Objeto de privilegio** para agregar el objeto de privilegio a la asociación que define los privilegios del usuario o del grupo de usuarios al autenticar un dispositivo iDRAC. Solo se puede agregar un objeto de privilegio a un objeto de asociación.

1. Seleccione la ficha **Objeto de privilegios** y haga clic en **Agregar**.
2. Introduzca el nombre del objeto de privilegio y haga clic en **Aceptar**.
3. Haga clic en la ficha **Objeto de privilegio** para agregar el objeto de privilegio a la asociación que define los privilegios del usuario o del grupo de usuarios al autenticar un dispositivo iDRAC. Solo se puede agregar un objeto de privilegio a un objeto de asociación.

Cómo agregar dispositivos iDRAC o grupos de dispositivos iDRAC


Para agregar dispositivos iDRAC o grupos de dispositivos iDRAC:

1. Seleccione la ficha **Productos** y haga clic en **Agregar**.
2. Introduzca el nombre de los dispositivos iDRAC o de los grupos de dispositivos iDRAC 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 iDRAC conectado a la red que está disponible para los usuarios o los grupos de usuarios definidos. Puede agregar varios dispositivos iDRAC a un objeto de asociación.

Configuración de Active Directory con esquema extendido mediante la interfaz web de iDRAC

Para configurar Active Directory con esquema extendido mediante la interfaz web:

 **NOTA:** Para obtener información acerca de los distintos campos, consulte la *Ayuda en línea de iDRAC*.

- En la interfaz web de iDRAC, vaya a **Información general** → **Configuración de iDRAC** → **Autenticación de usuario** → **Servicios de directorio** → **Microsoft Active Directory**. Aparece la página de resumen de **Active Directory**.
- Haga clic en **Configurar Active Directory**. Aparece la página **Paso 1 de 4 de Configuración y administración de Active Directory**.
- Opcionalmente, active la validación de certificados y cargue el certificado digital firmado por la CA que se utilizó durante la iniciación de las conexiones SSL al comunicarse con el servidor de Active Directory (AD).
- Haga clic en **Siguiente**. Aparece la página **Paso 2 de 4 de Configuración y administración de Active Directory**.
- Especifique la información de ubicación acerca de los servidores y las cuentas de usuario de Active Directory (AD). Asimismo, especifique el tiempo que iDRAC debe esperar para las respuestas de AD durante el proceso de inicio de sesión.

 **NOTA:**

- Si está activada la validación de certificados, especifique las direcciones de servidor de controladora de dominio y el FQDN. Asegúrese de que el DNS está configurado correctamente en **Información general** → **Configuración de iDRAC** → **Red**
- Si el usuario y los objetos de iDRAC se encuentran en dominios diferentes, no seleccione la opción **Dominio de usuario desde inicio de sesión**. En su lugar, seleccione la opción **Especificar un dominio** e introduzca el nombre del dominio donde el objeto de iDRAC está disponible.

- Haga clic en **Siguiente**. Aparece la página **Paso 3 de 4 de Configuración y administración de Active Directory**.
- Seleccione **Esquema extendido** y haga clic en **Siguiente**. Aparece la página **Paso 4 de 4 de Configuración y administración de Active Directory**.
- Introduzca el nombre y la ubicación del objeto de dispositivo de iDRAC en Active Directory (AD) y haga clic en **Terminar**. Se habrán configurado los valores de Active Directory para el modo de esquema extendido.

Configuración de Active Directory con esquema extendido mediante RACADM

Para configurar Active Directory con esquema estándar a través de RACADM:

- Abra un símbolo del sistema e introduzca los siguientes comandos de RACADM:
 - Mediante el comando **config**:

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1 racadm config -g  
cfgActiveDirectory -o cfgADType 1 racadm config -g cfgActiveDirectory -o
```

```

cfgADracName <RAC common name> racadm config -g cfgActiveDirectory -o
cfgADracDomain <fully qualified rac domain name> racadm config -g
cfgActiveDirectory -o cfgADDomainController1 <fully qualified domain name
or IP Address of the domain controller> racadm config -g
cfgActiveDirectory -o cfgADDomainController2 <fully qualified domain name
or IP Address of the domain controller> racadm config -g
cfgActiveDirectory -o cfgADDomainController3 <fully qualified domain name
or IP Address of the domain controller>

```

- Mediante el comando **set**:

```

racadm set iDRAC.ActiveDirectory.Enable 1 racadm set
iDRAC.ActiveDirectory.Schema 2 racadm set iDRAC.ActiveDirectory.RacName
<RAC common name> racadm set iDRAC.ActiveDirectory.RacDomain <fully
qualified rac domain name> racadm set
iDRAC.ActiveDirectory.DomainController1 <fully qualified domain name or
IP address of the domain controller> racadm set
iDRAC.ActiveDirectory.DomainController2 <fully qualified domain name or
IP address of the domain controller> racadm set
iDRAC.ActiveDirectory.DomainController3 <fully qualified domain name or
IP address of the domain controller>

```

- ✎ **NOTA:** Debe configurar al menos una de las tres direcciones. iDRAC intenta conectarse a cada una de las direcciones configuradas una a la vez hasta que establezca correctamente una conexión. Con el esquema extendido, estas son las direcciones FQDN o IP de las controladoras de dominio donde se encuentra este dispositivo iDRAC.

Para desactivar la validación de certificado durante el protocolo de enlace SSL (opcional):

- Mediante el comando **config**: `racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0`
- Mediante el comando **set**: `racadm set iDRAC.ActiveDirectory.CertValidationEnable 0`

- ✎ **NOTA:** En este caso, no tiene que cargar un certificado de CA.

Para aplicar la validación de certificado durante el protocolo de enlace SSL (opcional):

- Mediante el comando **config**: `racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1`
- Mediante el comando **set**: `racadm set iDRAC.ActiveDirectory.CertValidationEnable 1`

En este caso, debe cargar un certificado de CA.

```
racadm sslcertupload -t 0x2 -f <ADS root CA certificate>
```

- ✎ **NOTA:** Si la validación de certificados está activada, especifique las direcciones del servidor de la controladora de dominio y el FQDN. Asegúrese de que el DNS esté configurado correctamente en **Información general** → **Configuración de iDRAC** → **Red**.

El siguiente comando de RACADM es opcional:

```
racadm sslcertdownload -t 0x1 -f <RAC SSL certificate>
```

2. Si DHCP está activado en iDRAC y desea utilizar el DNS proporcionado por el servidor DHCP, introduzca el siguiente comando de RACADM:
 - Mediante el comando **config**: `racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 1`
 - Mediante el comando **set**: `racadm set iDRAC.IPv4.DNSFromDHCP 1`

3. Si DHCP está desactivado en iDRAC o si desea introducir manualmente la dirección IP de DNS, introduzca los siguientes comandos de RACADM:

- Mediante el comando **config**:

```
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0 racadm
config -g cfgLanNetworking -o cfgDNSServer1 <primary DNS IP address>
racadm config -g cfgLanNetworking -o cfgDNSServer2 <secondary DNS IP
address>
```

- Mediante el comando **set**:

```
racadm set iDRAC.IPv4.DNSFromDHCP 0 racadm set
iDRAC.IPv4.DNSFromDHCP.DNS1 <primary DNS IP address> racadm set
iDRAC.IPv4.DNSFromDHCP.DNS2 <secondary DNS IP address>
```

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 de iDRAC, introduzca el siguiente comando:

- Mediante el comando **config**: `racadm config -g cfgUserDomain -o cfgUserDomainName <fully qualified domain name or IP Address of the domain controller> -i <index>`

- Mediante el comando **set**: `racadm set iDRAC.UserDomain.<index>.Name <fully qualified domain name or IP Address of the domain controller>`

Puede configurar hasta 40 dominios de usuario con números de índice entre 1 y 40.

5. Presione **Intro** para completar la configuración de Active Directory con esquema extendido.

Prueba de la configuración de Active Directory

Puede probar la configuración de Active Director para comprobar si es correcta o para diagnosticar el problema con un inicio de sesión de Active Directory fallido.

Prueba de la configuración de Active Directory mediante una interfaz web de iDRAC

Para probar la configuración de Active Directory:

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Configuración de iDRAC** → **Autenticación de usuario** → **Servicios de directorio** → **Microsoft Active Directory**. Aparece la página de resumen de **Active Directory**.
2. Haga clic en **Probar la configuración**.
3. Introduzca el nombre de usuario de la prueba (por ejemplo, **nombreDeUsuario@domain.com**) y la contraseña, y haga clic en **Iniciar prueba**. Se obtienen resultados de prueba detallados y se muestra el registro de la prueba.

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.



NOTA: Al realizar la prueba de la configuración de Active Directory con la opción Activar la validación de certificados seleccionada, iDRAC requiere que el FQDN y no una dirección IP identifique el servidor de Active Directory. Si el servidor de Active Directory lo identifica una dirección IP, fallará la validación del certificado porque iDRAC no puede comunicarse con el servidor Active Directory.


Prueba de la configuración de Active Directory mediante RACADM

Para probar la configuración de Active Directory, utilice el comando `testfeature`. Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8) disponible en dell.com/support/manuals.

Configuración de los usuarios LDAP genéricos

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

Para hacer que la implementación LDAP de iDRAC sea genérica, los elementos comunes entre los distintos servicios de directorio se utilizan para agrupar usuarios y asignar la relación usuario-grupo. La acción específica del servicio de directorio es el esquema. Por ejemplo, pueden tener nombres de atributo diferentes para el grupo, el usuario y el vínculo entre el usuario y el grupo. Estas acciones se configuran en iDRAC.

 **NOTA:** Los inicios de sesión de autenticación de dos factores (TFA) basada en tarjeta inteligente e inicio de sesión único (SSO) no se admiten para el servicio de directorio de LDAP genérico.


Enlaces relacionados

[Configuración del servicio de directorio de LDAP genérico mediante la interfaz basada en web de iDRAC](#)


[Configuración del servicio de directorio LDAP genérico mediante RACADM](#)

Configuración del servicio de directorio de LDAP genérico mediante la interfaz basada en web de iDRAC


Para configurar el del servicio de directorio de LDAP genérico mediante la interfaz web:


 **NOTA:** Para obtener información acerca de los distintos campos, consulte la *Ayuda en línea de iDRAC*.

1. En la interfaz web de iDRAC, vaya a **Información general** → **Configuración de iDRAC** → **Autenticación de usuario** → **Servicios de directorio** → **Servicios de directorio LDAP genérico**. La página **Configuración y administración de LDAP genérico** muestra la configuración actual del LDAP genérico.
2. Haga clic en **Configurar LDAP genérico**.
3. De manera opcional, active la validación de certificados y cargue el certificado digital que se utilizó durante la iniciación de las conexiones SSL al comunicarse con un servidor LDAP genérico.

 **NOTA:** En esta versión, no se admite el enlace LDAP basado en puertos no SSL. Solo se admite LDAP sobre SSL.

4. Haga clic en **Siguiente**. Aparece la página **Paso 2 de 3 de Configuración y administración de LDAP genérico**.
5. Active la autenticación LDAP genérica y especifique la información de ubicación sobre los servidores LDAP genéricos y las cuentas de usuario.

 **NOTA:** Si se ha activado la validación de certificados, especifique el FQDN del servidor LDAP y asegúrese de que DNS se ha configurado correctamente en **Información general** → **Configuración de iDRAC** → **Red**.

 **NOTA:** En esta versión, no se admiten grupos anidados. El firmware busca el miembro directo del grupo para que coincida con el DN del usuario. Asimismo, solo se admiten un único dominio. No se admiten dominios cruzados.


6. Haga clic en **Siguiente**.

Aparece la página **Paso 3a de 3 de Configuración y administración de LDAP genérico**.

7. Haga clic en **Grupo de roles**.

Aparece la página **Paso 3b de 3 de Configuración y administración de LDAP genérico**.

8. Especifique el nombre distintivos del grupo y los privilegios asociados con este. A continuación, haga clic en **Aplicar**.

 **NOTA:** Si utiliza Novell eDirectory y ha utilizado los caracteres # (numeral), " (comillas dobles), ; (punto y coma), > (mayor que), , (coma) o <(menor que) para el nombre DN del grupo, estos debe ser escapados.

Se guardará la configuración del grupo de roles, que se mostrará en la página **Paso 3a de 3 de Configuración y administración de LDAP genérico**.

9. Si desea configurar grupos de roles adicionales, repita los pasos 7 y 8.

10. Haga clic en **Terminar**. Se habrá configurado el servicio de directorio LDAP.

Configuración del servicio de directorio LDAP genérico mediante RACADM

Para configurar el servicio de directorio LDAP:

- Utilice los objetos de los grupos **cfgLdap** y **cfgLdapRoleGroup** con el comando **config**.
- Utilice los objetos de los grupos **iDRAC.LDAP** e **iDRAC.LDAPRole** con el comando **set**.

Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8), disponible en dell.com/support/manuals.



Prueba de la configuración del servicio de directorio de LDAP

Puede probar la configuración del servicio de directorio de LDAP para comprobar si es correcta o para diagnosticar la falla de la sesión de inicio de LDAP.

Prueba de la configuración del servicio de directorio de LDAP mediante una interfaz web de iDRAC

Para probar la configuración del servicio de directorio LDAP:

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Configuración de iDRAC** → **Autenticación de usuario** → **Servicios de directorio** → **Servicios de directorio LDAP genérico**.
La página **Configuración y administración de LDAP genérico** muestra la configuración actual del LDAP genérico.
2. Haga clic en **Probar la configuración**.
3. Introduzca el nombre de usuario y la contraseña de un usuario de directorio elegido para probar la configuración de LDAP. El formato depende en el valor de *Atributo del inicio de sesión de usuario* que se utiliza y el nombre de usuario introducido debe coincidir con el valor del atributo elegido.

-  **NOTA:** Al realizar la prueba de LDAP con la opción **Activar la validación de certificados** seleccionada, iDRAC requiere que el FQDN y no una dirección IP identifique el servidor de LDAP. Si el servidor de LDAP lo identifica una dirección IP, fallará la validación del certificado porque iDRAC no puede comunicarse con el servidor LDAP.
-  **NOTA:** Cuando está habilitado LDAP genérico, iDRAC primero intenta iniciar la sesión del usuario como un usuario de directorio. Si falla, se activa la búsqueda de usuario local.

Aparecen los resultados de la prueba y el registro de la misma.

Prueba de la configuración del servicio de directorio LDAP mediante RACADM

Para probar la configuración del servicio de directorio LDAP, utilice el comando `testfeature`. Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8)* disponible en dell.com/support/manuals.

Configuración de iDRAC para inicio de sesión único o inicio de sesión mediante tarjeta inteligente

En esta sección se proporciona información para configurar iDRAC con el inicio de sesión mediante tarjeta inteligente (para usuarios locales y usuarios de Active Directory) y el inicio de sesión único (SSO) (para usuarios de Active Directory). SSO y el inicio de sesión único son funciones con licencia.

iDRAC admite la autenticación de Active Directory basada en Kerberos para admitir inicios de sesión mediante tarjeta inteligente y SSO. Para obtener más información acerca de Kerberos, consulte el sitio web de Microsoft.


Enlaces relacionados

- [Configuración del inicio de sesión SSO de iDRAC para usuarios de Active Directory](#)
- [Configuración del inicio de sesión mediante tarjeta inteligente de iDRAC para usuarios locales](#)
- [Configuración del inicio de sesión mediante tarjeta inteligente de iDRAC para usuarios de Active Directory](#)

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

A continuación se indican los prerrequisitos de inicios de sesión SSO y mediante tarjeta inteligente basados en Active Directory:

- Sincronice la hora de iDRAC con la hora de la controladora de dominio de Active Directory. Si no lo hace, la autenticación de kerberos en iDRAC fallará. Es posible usar la zona horaria y la función de NTP para sincronizar la hora. Para ello, consulte [Configuración de zona horaria y NTP](#).
- Registre el iDRAC como equipo en el dominio raíz de Active Directory.
- Genere un archivo keytab mediante la herramienta ktpass.
- Para activar el inicio de sesión único para el esquema extendido, asegúrese de que la opción **Confiar en este usuario para la delegación a cualquier servicio (solo Kerberos)** está activada en la ficha **Delegación** del usuario keytab. Esta ficha solo está disponible tras crear el archivo keytab mediante la utilidad ktpass.
- Configure el explorador para activar el inicio de sesión SSO.
- Cree los objetos de Active Directory y proporcione los privilegios necesarios.
- Para SSO, configure la zona de búsqueda invertida en los servidores DNS para la subred en la que reside iDRAC.

 **NOTA:** Si el nombre del host no coincide con la búsqueda de DNS invertida, fallará la autenticación de Kerberos.

Enlaces relacionados

- [Configuración del explorador para activar el inicio de sesión único de Active Directory](#)

[Registro de iDRAC como equipo en el dominio raíz de Active Directory](#)
[Generación del archivo Keytab de Kerberos](#)
[Creación de objetos de Active Directory y establecimiento de privilegios](#)

Registro de iDRAC como equipo en el dominio raíz de Active Directory

Para registrar iDRAC en el dominio raíz de Active Directory:

1. Haga clic en **Información general** → **Configuración de iDRAC** → **Red** → **Red**. Aparecerá la página **Red**.
2. Proporciona una dirección IP válida en **Servidor DNS preferido/Servidor DNS alternativo**. Este valor es una dirección IP de servidor DNS válido que forma parte del dominio raíz.
3. Seleccione **Registrar el iDRAC en DNS**.
4. Indique un **nombre de dominio DNS** válido.
5. Verifique que la configuración de DNS de la red coincida con la información de DNS de Active Directory.

Para obtener más información acerca de estas opciones, consulte la *Ayuda en línea de iDRAC*.

Generación del archivo Keytab de Kerberos

Para compatibilidad con la autenticación de inicio de sesión mediante SSO y tarjeta inteligente, iDRAC permite que la configuración se active como un servicio Kerberos en una red de Windows Kerberos. La configuración de Kerberos en iDRAC implica los mismos pasos que la configuración de un servicio que no sea de Windows Server Kerberos como elemento principal de seguridad en Windows Server Active Directory.

La herramienta *ktpass* (disponible de Microsoft como parte del CD/DVD de instalación del servidor) se utiliza para crear los enlaces de nombre principal del servicio (SPN) a una cuenta de usuario y exportar la información de confianza en un archivo *keytab* de Kerberos tipo MIT, 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 utiliza para cifrar la información entre el servidor y el KDC. La herramienta *ktpass* permite servicios basados en UNIX que admiten la autenticación de Kerberos utilizar las funciones de interoperabilidad que proporciona un servicio Windows Server Kerberos KDC. Para obtener más información acerca de la utilidad **ktpass**, consulte el sitio web de Microsoft en: [technet.microsoft.com/en-us/library/cc779157\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc779157(WS.10).aspx)


Antes de generar un archivo *keytab*, debe crear una cuenta de usuario de Active Directory para utilizar con la opción **-mapuser** del comando *ktpass*. Asimismo, debe tener el mismo nombre que el nombre DNS de iDRAC DNS al que cargará el archivo *keytab* generado.

Para generar un archivo *keytab* mediante la herramienta *ktpass*:

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

```
C:\> ktpass.exe -princ HTTP/idrac7name.domainname.com@DOMAINNAME.COM -  
mapuser DOMAINNAME\username -mapOp set -crypto AES256-SHA1 -ptype  
KRB5_NT_PRINCIPAL -pass [password] -out c:\krbkeytab
```


El tipo de cifrado es AES256-SHA1. El tipo principal es KRB5_NT_PRINCIPAL. Las propiedades de la cuenta de usuario a la que se asigna el nombre principal del servicio debe tener activada la propiedad **Utilizar tipos de cifrado AES 256 para esta cuenta**.

 **NOTA:** Utilice letras en minúsculas para **iDRACname** y **Nombre principal del servicio**. Utilice letras en mayúsculas para el nombre de dominio, tal como se muestra en el ejemplo.

3. Ejecute el comando siguiente:

```
C:\>setspn -a HTTP/iDRACname.domainname.com username
```

Se genera un nuevo archivo keytab.

 **NOTA:** Si encuentra problemas con el usuario de iDRAC para el que se crea el archivo keytab, cree un nuevo usuario y un nuevo archivo keytab. Si se vuelve a ejecutar el mismo archivo keytab que se había creado originalmente, no se configurará correctamente.

Creación de objetos de Active Directory y establecimiento de privilegios

Realice los pasos a continuación para el inicio de sesión SSO basado en el esquema extendido de Active Directory:

1. Cree el objeto de dispositivo, el objeto de privilegio y el objeto de asociación en el servidor de Active Directory.
2. Establezca los privilegios de acceso al objeto de privilegio creado. Es recomendable no proporcionar privilegios de administrador, ya que esto podría omitir algunas comprobaciones de seguridad.
3. Asocie el objeto de dispositivo y el objeto de privilegio con el objeto de asociación.
4. Agregue el usuario de SSO (usuario con acceso) anterior al objeto de dispositivo.
5. Proporcione privilegio de acceso a *Usuarios autenticados* para acceder al objeto de asociación creado.

Enlaces relacionados

[Cómo agregar usuarios y privilegios de iDRAC a Active Directory](#)

Configuración del explorador para activar el inicio de sesión único de Active Directory

En esta sección se proporciona la configuración de explorador de Internet Explorer y Firefox para activar el inicio de sesión único de Active Directory.

 **NOTA:** Google Chrome y Safari no admiten Active Directory para realizar el inicio de sesión SSO.

Configuración de Internet Explorer para activar el inicio de sesión único de Active Directory

Para configurar los valores del explorador para Internet Explorer:

1. En Internet Explorer, vaya a **Intranet local** y haga clic en **Sitios**.
2. 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.
3. Haga clic en **Avanzado**.
4. Agregue todos los nombres de dominio relativos que se usarán en instancias de iDRAC y que forman parte de la configuración del SSO (por ejemplo: **myhost.example.com**).
5. Haga clic en **Cerrar** y luego en **Aceptar** dos veces.

Configuración de Firefox para activar el inicio de sesión único de Active Directory

Para configurar los valores del explorador para Firefox:

1. En la barra de dirección, introduzca `about:config`.
2. En **Filtro**, introduzca `network.negotiate`.
3. Agregue el nombre de iDRAC a `network.negotiate-auth.trusted-uris` (con una lista de valores separados por comas).
4. Agregue el nombre de iDRAC a `network.negotiate-auth.delegation-uris` (con una lista de valores separados por comas).

Configuración del inicio de sesión SSO de iDRAC para usuarios de Active Directory

Antes de configurar iDRAC para el inicio de sesión SSO de Active Directory, asegúrese de satisfacer todos los prerequisites.

Puede configurar iDRAC para SSO de Active Directory cuando configura una cuenta de usuario basada en Active Directory.

Enlaces relacionados

[Prerequisites para el inicio de sesión único de Active Directory o el inicio de sesión mediante tarjeta inteligente](#)

[Configuración de Active Directory con el esquema estándar mediante la interfaz web de iDRAC](#)


[Configuración de Active Directory con esquema estándar vía RACADM](#)

[Configuración de Active Directory con esquema extendido mediante la interfaz web de iDRAC](#)

[Configuración de Active Directory con esquema extendido mediante RACADM](#)

Configuración del inicio de sesión SSO de iDRAC para usuarios de Active Directory mediante la interfaz web

Para configurar iDRAC para un inicio de sesión SSO de Active Directory:

 **NOTA:** Para obtener más información acerca de estas opciones, consulte la *Ayuda en línea de iDRAC*.

1. Verifique si el nombre DNS de iDRAC coincide con el nombre de dominio completo de iDRAC. Para ello, en la interfaz web de iDRAC, vaya a **Información general** → **Configuración de iDRAC** → **Red** → **Red** y consulte la propiedad **Nombre de dominio DNS**.
2. Al configurar Active Directory para configurar una cuenta de usuario basada en el esquema estándar o el esquema extendido, realice los dos pasos adicionales siguientes para configurar SSO:
 - Cargue el archivo keytab en la página **Paso 1 de 4 de Configuración y administración de Active Directory**.
 - Seleccione **Activar inicio de sesión único** en la página **Paso 2 de 4 de Configuración y administración de Active Directory**.

Configuración del inicio de sesión SSO de iDRAC para usuarios de Active Directory mediante RACADM

Además de los pasos que se realizan durante la configuración de Active Directory, para activar SSO, se debe ejecutar uno de los comandos siguientes:

- Mediante el comando **config**:

```
racadm config -g cfgActiveDirectory -o cfgADSSOEnable 1
```
- Mediante el comando **set**:

```
racadm set iDRAC.ActiveDirectory.SSOEnable 1
```

Configuración del inicio de sesión mediante tarjeta inteligente de iDRAC para usuarios locales

Para configurar el usuario local de iDRAC para inicio de sesión mediante tarjeta inteligente:

1. Cargue el certificado de usuario de tarjeta inteligente y el certificado de CA de confianza en iDRAC.
2. Active el inicio de sesión mediante tarjeta inteligente.

Enlaces relacionados

[Obtención de certificados](#)

[Carga del certificado de usuario de tarjeta inteligente](#)

[Activación o desactivación del inicio de sesión mediante tarjeta inteligente](#)

Carga del certificado de usuario de tarjeta inteligente

Antes de cargar el certificado de usuario, asegúrese de que el certificado de usuario del proveedor de la tarjeta inteligente se ha exportado en el formato Base64. También se admiten los certificados SHA-2.

Enlaces relacionados

[Obtención de certificados](#)

Carga del certificado de usuario de tarjeta inteligente mediante la interfaz web

Para cargar el certificado de usuario de tarjeta inteligente:

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Configuración de iDRAC** → **Red** → **Autenticación de usuario** → **Usuarios locales**.
Se muestra la página **Users (Usuarios)**.
2. En la columna **Identificación de usuario**, haga clic en un número de identificación de usuario.
Aparece la página **Menú principal de usuarios**.
3. En **Configuraciones de tarjeta inteligente**, seleccione **Cargar certificado de usuario** y haga clic en **Siguiente**.
Aparece la página **Carga del certificado de usuario**.
4. Busque y seleccione el certificado de usuario Base64 y haga clic en **Aplicar**.

Carga del certificado de usuario de tarjeta inteligente mediante RACADM

Para cargar el certificado de usuario de tarjeta inteligente, utilice el objeto **usercertupload**. Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8)* disponible en dell.com/support/manuals.

Carga del certificado de CA de confianza para tarjeta inteligente

Antes de cargar el certificado de CA, asegúrese de disponer de un certificado firmado por la CA.

Enlaces relacionados

[Obtención de certificados](#)

Carga del certificado de CA de confianza para tarjeta inteligente mediante la interfaz web

Para cargar el certificado de CA de confianza para el inicio de sesión mediante tarjeta inteligente:

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Configuración de iDRAC** → **Red** → **Autenticación de usuario** → **Usuarios locales**.
Se muestra la página **Users (Usuarios)**.
2. En la columna **Identificación de usuario**, haga clic en un número de identificación de usuario.
Aparece la página **Menú principal de usuarios**.
3. En **Configuraciones de tarjeta inteligente**, seleccione **Cargar certificado de CA de confianza** y haga clic en **Siguiente**.
Aparece la página **Carga del certificado de CA de confianza**.
4. Busque y seleccione el certificado de CA de confianza y haga clic en **Aplicar**.

Carga del certificado de CA de confianza para tarjeta inteligente mediante RACADM

Para cargar el certificado de CA de confianza para el inicio de sesión mediante tarjeta inteligente, utilice el objeto **usercertupload**. Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8)* disponible en dell.com/support/manuals.

Configuración del inicio de sesión mediante tarjeta inteligente de iDRAC para usuarios de Active Directory

Antes de configurar el inicio de sesión mediante tarjeta inteligente de iDRAC para los usuarios de Active Directory, asegúrese de haber cumplido los requisitos necesarios.

Para configurar el inicio de sesión mediante tarjeta inteligente de iDRAC:

1. En la interfaz web de iDRAC, al configurar Active Directory para establecer una cuenta de usuario basada en el esquema estándar o el esquema extendido, en la página **Paso 1 de 4 de Configuración y administración de Active Directory** realice lo siguiente:
 - Active la validación de certificados.
 - Cargue un certificado firmado por la CA de confianza.
 - Cargue el archivo keytab.
2. Active el inicio de sesión mediante tarjeta inteligente. Para obtener más información acerca de estas opciones, consulte la *Ayuda en línea de iDRAC*.

Enlaces relacionados

[Activación o desactivación del inicio de sesión mediante tarjeta inteligente](#)

[Obtención de certificados](#)

[Generación del archivo Keytab de Kerberos](#)

[Configuración de Active Directory con el esquema estándar mediante la interfaz web de iDRAC](#)

[Configuración de Active Directory con esquema estándar vía RACADM](#)


[Configuración de Active Directory con esquema extendido mediante la interfaz web de iDRAC](#)

[Configuración de Active Directory con esquema extendido mediante RACADM](#)

Activación o desactivación del inicio de sesión mediante tarjeta inteligente

Antes de activar o desactivar el inicio de sesión mediante tarjeta inteligente para iDRAC, asegúrese de haber realizado lo siguiente:

- Configurar los permisos iDRAC.
- Completar la configuración de usuario local de iDRAC o la configuración de usuario de Active Directory con los certificados adecuados.

 **NOTA:** Si se activa el inicio de sesión mediante tarjeta inteligente, SSH, Telnet, IPMI en la LAN, Comunicación en serie en la LAN y RACADM remoto se desactivan. Si desactiva el inicio de sesión mediante tarjeta inteligente, las interfaces no se activan automáticamente.

Enlaces relacionados

[Obtención de certificados](#)

[Configuración del inicio de sesión mediante tarjeta inteligente de iDRAC para usuarios de Active Directory](#)

[Configuración del inicio de sesión mediante tarjeta inteligente de iDRAC para usuarios locales](#)

Activación o desactivación del inicio de sesión mediante tarjeta inteligente utilizando la interfaz web

Para activar o desactivar la función de inicio de sesión mediante tarjeta inteligente:

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Configuración de iDRAC** → **Autenticación de usuario** → **Tarjeta inteligente**.
Se muestra la página **Tarjeta inteligente**.
2. En el menú desplegable **Configurar inicio de sesión mediante tarjeta inteligente**, seleccione **Activado** para activar el inicio de sesión mediante tarjeta inteligente o seleccione **Activado con RACADM remoto**. De lo contrario, seleccione **Desactivado**.
Para obtener más información acerca de estas opciones, consulte la *Ayuda en línea de iDRAC*.
3. Haga clic en **Aplicar** para aplicar la configuración.
Se le solicitará un inicio de sesión mediante tarjeta inteligente durante todos los intentos de inicio de sesión subsiguientes mediante la interfaz web de iDRAC.

Activación o desactivación del inicio de sesión mediante tarjeta inteligente utilizando RACADM

Para activar el inicio de sesión mediante una tarjeta inteligente, utilice una de las siguientes opciones:

- Utilice los objetos del grupo **cfgSmartCard** con el comando **config**.
- Utilice los objetos del grupo **iDRAC.SmartCard** con el comando **set**.

Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide* (*Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8*) disponible en dell.com/support/manuals.

Activación o desactivación del inicio de sesión mediante tarjeta inteligente mediante la utilidad de configuración de iDRAC

Para activar o desactivar la función de inicio de sesión mediante tarjeta inteligente:

1. En la utilidad de configuración de iDRAC, vaya a **Tarjeta inteligente**.
Se muestra la página **Tarjeta inteligente de la configuración de iDRAC**.
2. Seleccione **Activado** para activar el inicio de sesión mediante tarjeta inteligente. De lo contrario, seleccione **Desactivar**. Para obtener más información acerca de estas opciones, consulte la *Ayuda en línea de la utilidad de configuración de iDRAC*.
3. Haga clic en **Atrás**, en **Terminar** y, a continuación, en **Sí**.
La función de inicio de sesión mediante tarjeta inteligente se activa o desactiva según la opción seleccionada.

Configuración de iDRAC para enviar alertas

Puede establecer alertas y acciones para determinados sucesos que se producen en el sistema administrado. Un suceso se produce cuando el estado de un componente del sistema es mayor que la condición predefinida. Si un suceso coincide con un filtro de suceso y se ha configurado este filtro para generar una alerta (por correo electrónico, captura SNMP, alerta IPMI, registros del sistema remoto o sucesos de WS), se envía una alerta a uno o más destinos configurados. Si el mismo filtro de suceso también está configurado para realizar una acción (como reinicio, ciclo de encendido o apagado del sistema), la acción se llevará a cabo. Puede configurar una sola acción para cada suceso.

Si desea configurar iDRAC para enviar alertas:

1. Active las alertas.
2. De manera opcional, puede filtrar las alertas en función de la categoría o la gravedad.
3. Configure los valores de alerta por correo electrónico, alerta IPMI, captura SNMP, registro del sistema remoto, registro del sistema operativo y/o sucesos de WS.
4. Active las alertas y las acciones de suceso, como por ejemplo:
 - Envíe una alerta por correo electrónico, alerta IPMI, capturas SNMP, registros del sistema remoto, registro del sistema operativo o sucesos de WS a los destinos configurados.
 - Realice un reinicio, un apagado o un ciclo de encendido del sistema administrado.

Enlaces relacionados

[Activación o desactivación de alertas](#)

[Filtrado de alertas](#)

[Configuración de alertas de suceso](#)

[Configuración de suceso de periodicidad de alertas](#)

[Configuración de alertas por correo electrónico, capturas SNMP o capturas IPMI](#)

[Configuración del registro del sistema remoto](#)

[Configuración de sucesos de WS](#)

[Id. de mensaje de alertas](#)

Activación o desactivación de alertas

Para enviar una alerta a destinos configurados o para realizar una acción de suceso, deberá activar la opción de alertas globales. Esta propiedad invalida las alertas individuales o las acciones de suceso establecidas.

Enlaces relacionados

[Filtrado de alertas](#)

[Configuración de alertas por correo electrónico, capturas SNMP o capturas IPMI](#)

Activación o desactivación de alertas mediante la interfaz web

Para activar o desactivar la generación de alertas:

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Servidor** → **Alertas**. Aparecerá la página **Alertas**.
2. En la sección **Alertas**, realice lo siguiente:
 - Seleccione **Activar** para activar la generación de alertas o realizar una acción de suceso.
 - Seleccione **Desactivar** para desactivar la generación de alertas o realizar una acción de suceso.
3. Haga clic en **Aplicar** para guardar la configuración.

Activación o desactivación de alertas mediante RACADM

Para activar o desactivar la generación de alertas o acciones de sucesos mediante el comando **config**:

```
racadm config -g cfgIpmiLan -o cfgIpmiLanAlertEnable 1
```

Para activar o desactivar la generación de alertas o acciones de sucesos mediante el comando **set**:

```
racadm set iDRAC.IPMILan.AlertEnable 1
```

Activación o desactivación de alertas mediante la utilidad de configuración de iDRAC

Para activar o desactivar la generación de alertas o acciones de suceso:

1. En la utilidad de configuración de iDRAC, vaya a **Alertas**. Aparece la pantalla **Alertas de configuración de iDRAC**.
2. En **Sucesos de plataforma**, seleccione **Activado** para activar la generación de alertas o acciones de suceso. De lo contrario, seleccione **Desactivado**. Para obtener más información acerca de las opciones, consulte la *Ayuda en línea de la utilidad de configuración de iDRAC*.
3. Haga clic en **Atrás**, en **Terminar** y, a continuación, en **Sí**. Se habrán configurado los valores de alerta.

Filtrado de alertas

Puede filtrar las alertas en función de la categoría o la gravedad.


Enlaces relacionados

[Activación o desactivación de alertas](#)

[Configuración de alertas por correo electrónico, capturas SNMP o capturas IPMI](#)

Filtrado de alertas mediante la interfaz web de iDRAC

Para filtrar alertas en función de la categoría o la gravedad:

 **NOTA:** Es posible filtrar alertas incluso con privilegios de solo lectura.

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Servidor** → **Alertas**. Aparecerá la página **Alertas**.
2. En la sección **Filtro de alertas**, seleccione una o más de las categorías siguientes:
 - Condición del sistema

- Almacenamiento
 - Configuración
 - Auditorías
 - Actualizaciones
 - Notas de trabajo
3. Seleccione uno o más de los niveles de gravedad siguientes:
 - Informativo
 - Aviso
 - Crítico
 4. Haga clic en **Apply (Aplicar)**.

En la sección **Resultados de la alerta** se muestran los resultados en función de la categoría y la gravedad seleccionadas.

Filtrado de alertas mediante RACADM

Para filtrar las alertas, utilice el comando **eventfilters**. Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8)* disponible en dell.com/support/manuals.

Configuración de alertas de suceso

Puede configurar alertas de sucesos como alertas por correo electrónico, alertas IPMI, capturas SNMP, registros del sistema remoto, registros del sistema operativo y sucesos WS para que se envíen a los destinos configurados.

Enlaces relacionados

[Activación o desactivación de alertas](#)

[Configuración de alertas por correo electrónico, capturas SNMP o capturas IPMI](#)

[Filtrado de alertas](#)

[Configuración del registro del sistema remoto](#)

[Configuración de sucesos de WS](#)

Configuración de alertas de suceso mediante la interfaz web

Para establecer una alerta de suceso mediante la interfaz web:

1. Asegúrese de tener configuradas las alertas por correo electrónico, las alertas IPMI, las capturas SNMP y/o los parámetros de registro del sistema remoto.
2. Vaya a **Descripción general** → **Servidor** → **Alertas**.

Se muestra la página **Alerts (Alertas)**.
3. Bajo **Resultados de las alertas**, seleccione una o todas las alertas siguientes para los sucesos necesarios:
 - Alerta por correo electrónico
 - Captura SNMP
 - Alerta IPMI
 - Registro del sistema remoto
 - Registro del sistema operativo


- Sucesos de WS
4. Haga clic en **Apply (Aplicar)**.
La configuración se guarda.
 5. En la sección **Alertas**, seleccione la opción **Activar** para enviar las alertas a los destinos configurados.
 6. De manera opcional, puede enviar un suceso de prueba. En el campo **ID del mensaje para suceso de prueba**, introduzca la identificación del mensaje para probar si se generó la alerta y haga clic en **Prueba**. Para la lista de identificaciones de mensajes, consulte *Event Messages Guide* (Guía de mensajes de sucesos) disponible en dell.com/support/manuals.

Configuración de alertas de suceso mediante RACADM

Para establecer alertas de suceso, utilice el comando **eventfilters**. Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8) disponible en dell.com/support/manuals.

Configuración de suceso de periodicidad de alertas

Es posible configurar iDRAC para generar sucesos adicionales en intervalos específicos si el sistema continúa funcionando a una temperatura mayor que el límite de umbral de temperatura de entrada. El intervalo predeterminado es 30 días. El rango válido es de 0 a 366 días. Un valor de 0 indica que no se han producido sucesos.

 **NOTA:** Debe tener privilegio para configurar iDRAC para que establezca el valor de periodicidad de alertas.

Configuración de sucesos de periodicidad de alertas mediante la interfaz web de iDRAC

Para configurar el valor de periodicidad de alertas:

1. En la interfaz web de iDRAC, diríjase a **Descripción general** → **Servidor** → **Alertas** → **Periodicidad de alertas**.
Aparecerá la página **Periodicidad de alertas**.
2. En la columna **Periodicidad**, introduzca el valor de frecuencia de alertas para la categoría, alerta y tipos de gravedad requeridos.
Para obtener más información, consulte la *Ayuda en línea de iDRAC*.
3. Haga clic en **Apply (Aplicar)**.
Se guarda la configuración de periodicidad de alertas.

Configuración de sucesos de periodicidad de alertas mediante RACADM

Para configurar el suceso de periodicidad de alertas mediante RACADM, utilice el subcomando **eventfilters**. Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8).

Configuración de acciones del suceso

Puede establecer acciones de sucesos, tal como un reinicio del sistema, un ciclo de encendido o un apagado del sistema, o no realizar ninguna acción.

Enlaces relacionados

[Filtrado de alertas](#)

[Activación o desactivación de alertas](#)

Configuración de acciones del suceso mediante la interfaz web

Para configurar una acción de suceso:

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Servidor** → **Alertas**. Aparecerá la página **Alertas**.
2. Bajo **Resultados de alertas**, en el menú desplegable **Acciones**, seleccione una acción para cada suceso:
 - Reboot (Reiniciar)
 - Ciclo de encendido
 - Apagado
 - Sin acción
3. Haga clic en **Apply (Aplicar)**.
La configuración se guarda.

Configuración de acciones del suceso mediante RACADM

Para configurar una acción de suceso, utilice una de las siguientes opciones:

- Comando **eventfilters**
- Objeto **cfgIpmiPefAction** con el comando **config**

Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8)* disponible en dell.com/support/manuals.

Configuración de alertas por correo electrónico, capturas SNMP o capturas IPMI

Management Station utiliza capturas de protocolo simple de administración de red (SNMP) y de interfaz de administración de plataforma inteligente (IPMI) para recibir datos de iDRAC. Para los sistemas con un gran número de nodos, es posible que no sea eficiente que una estación de administración sondee cada iDRAC para cada condición que pueda producirse. Por ejemplo, las capturas de suceso pueden ayudar a una estación de administración con el equilibrio de carga entre nodos o emitir una alerta si se produce un fallo de autenticación. Se admiten los formatos de SNMP v1, v2 y v3.

Es posible configurar los destinos de alerta IPv4 e IPv6, los valores de correo electrónico y los valores del servidor SMTP, así como probar estos valores de configuración. También se puede especificar el usuario SNMP v3 al que se desea enviar las capturas de SNMP.

Antes de configurar los valores de correo electrónico o capturas SNMP/IPMI, asegúrese de lo siguiente:

- Dispone de permisos Configurar el RAC.
- Ha configurado los filtros de sucesos.

Enlaces relacionados

[Configuración de destinos de alerta IP](#)

[Configuración de los valores de alertas por correo electrónico](#)

Configuración de destinos de alerta IP

Es posible configurar las direcciones IPv6 o IPv4 para recibir las alertas IPMI o las capturas SNMP. Para obtener más información sobre los valores de MIB de iDRAC necesarios para supervisar los servidores mediante SNMP, consulte *SNMP Reference Guide for iDRAC8 (Guía de referencia de SNMP para iDRAC8)* disponible en dell.com/support/manuals.

Configuración de destinos de alerta IP mediante la interfaz web

Para configurar destinos de alerta mediante la interfaz web:

1. Vaya a **Descripción general** → **Servidor** → **Alertas** → **Configuración de SNMP y correo electrónico**.
2. Seleccione la opción **Estado** para activar un destino de alerta [dirección IPv4, dirección IPv6 o nombre de dominio completo (FQDN)] para recibir las capturas.
Es posible especificar hasta ocho direcciones de destino. Para obtener más información sobre las opciones, consulte la *Ayuda en línea de iDRAC*.
3. Seleccione el usuario SNMP v3 al que desea enviar la captura SNMP.
4. Introduzca la cadena de comunidad SNMP de iDRAC (solo se aplica a SNMPv1 y SNMPv2) y el número de puerto de la alerta SNMP.

Para obtener más información acerca de estas opciones, consulte la *Ayuda en línea de iDRAC*.



NOTA: El valor de cadena de comunidad indica la cadena de comunidad que se debe utilizar como una captura de alerta SNMP enviada desde iDRAC. Asegúrese de que la cadena de comunidad de destino sea igual a la de iDRAC. El valor predeterminado es Público.

5. Para comprobar que la dirección IP está recibiendo las capturas IPMI o SNMP, haga clic en **Enviar** bajo **Probar captura IPMI** y **Probar captura SNMP**, respectivamente.
6. Haga clic en **Apply (Aplicar)**.
Se configurarán los destinos de alerta.
7. En la sección **Formato de captura SNMP**, seleccione la versión de protocolo que se utilizará para enviar las capturas en los destinos de captura: **SNMP v1**, **SNMP v2** o **SNMP v3**, y haga clic en **Aplicar**.



NOTA: La opción **Formato de captura SNMP** se aplica solo a capturas SNMP y no a capturas IPMI. Las capturas IPMI siempre se envían en formato SNMP v1 y no están basadas en la opción configurada **Formato de captura SNMP**.

Se configurará el formato de captura SNMP.

Configuración de destinos de alerta IP mediante RACADM

Para configurar los valores de alerta de captura, siga los pasos siguientes:

1. Para activar capturas:
 - Dirección IPv4:

```
racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i (index) (0|1)
```
 - Dirección IPv6:

```
racadm config -g cfgIpmiPetIpv6 -o cfgIpmiPetIpv6AlertEnable -i (index) (0|1)
```donde, (index) es el índice de destino y 0 o 1 desactiva o activa la captura, respectivamente.

Por ejemplo, para activar una captura con índice 4, introduzca el comando siguiente:

```
racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 4 1
```

2. Para configurar la dirección de destino de la captura, siga los pasos siguientes:

```
racadm config -g cfgIpmiPetIpv6 -o cfgIpmiPetIpv6AlertDestIPAddr -i [index] [IP-address]
```

donde [index] es el índice del destino de la captura de y [IP-address] es la dirección IP del sistema que recibe las alertas de sucesos de plataforma.

3. Configure la cadena de nombre de comunidad SNMP:

```
racadm config -g cfgIpmiLan -o cfgIpmiPetCommunityName [name]
```

donde [name] es el nombre de comunidad SNMP.

4. Para configurar un destino de SNMP:

- Para configurar el destino de la captura SNMP para SNMPv3:

```
racadm set idrac.SNMP.Alert.[index].DestAddr [Ip address]
```

Por ejemplo:

```
racadm set idrac.SNMP.Alert.1.DestAddr 1.2.3.4
```

- Para configurar los usuarios SNMPv3 para los destinos de captura:

```
racadm set idrac.SNMP.Alert.1.SNMPv3Username root
```

- Para activar SNMPv3 para un usuario:

```
racadm set idrac.users.2.SNMPv3Enable Enabled
```

5. Para probar la captura, si fuera necesario:

```
racadm testtrap -i [index]
```

donde [index] es el índice del destino de captura que se debe probar.

Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8)* disponible en dell.com/support/manuals.


Configuración de destinos de alerta IP mediante la utilidad de configuración de iDRAC


Es posible configurar destinos de alerta (IPv4, IPv6 o FQDN) mediante la utilidad de configuración de iDRAC. Para realizar esta acción:

1. En la **utilidad de configuración de iDRAC**, vaya a **Alertas**. Aparece la pantalla **Alertas de configuración de iDRAC**.
2. En **Valores de captura**, active las direcciones IP para recibir las capturas e introduzca las direcciones de destino IPv4, IPv6 o FQDN. Puede especificar hasta ocho direcciones.
3. Introduzca el nombre de la cadena de comunidad.
Para obtener información acerca de las opciones, consulte la *Ayuda en línea de la utilidad de configuración de iDRAC*.
4. Haga clic en **Atrás**, en **Terminar** y, a continuación, en **Sí**.
Se configurarán los destinos de alerta.

Configuración de los valores de alertas por correo electrónico

Puede configurar la dirección de correo electrónico para recibir alertas por correo electrónico. También deberá configurar los valores de la dirección del servidor SMTP.

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

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

Enlaces relacionados

[Configuración de los valores de dirección del servidor de correo electrónico SMTP](#)

Configuración de los valores de alerta por correo electrónico mediante la interfaz web

Para configurar los valores de alerta por correo electrónico mediante la interfaz web:

1. Vaya a **Descripción general** → **Servidor** → **Alertas** → **Configuración de SNMP y correo electrónico**.
2. Seleccione la opción **Estado** para activar la dirección de correo electrónico que recibirá las alertas y escriba una dirección de correo electrónico válida. Para obtener más información sobre las opciones, consulte la *Ayuda en línea de iDRAC*.
3. Haga clic en **Enviar** en **Probar correo electrónico** para probar los valores de alerta por correo electrónico configurados.
4. Haga clic en **Apply (Aplicar)**.

Configuración de los valores de alerta por correo electrónico mediante RACADM

Para configurar los valores de alerta por correo electrónico:

1. Para activar alertas por correo electrónico:

- Mediante el comando **config**:

```
racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i [índice] [0|1]
```

donde [index] es el índice del destino de correo electrónico. 0 desactiva la alerta por correo electrónico y 1 la activa.

El índice del destino de correo electrónico puede ser un valor de 1 a 4. Por ejemplo, para activar el correo electrónico con índice 4, introduzca el comando siguiente:

```
racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 4 1
```

- Mediante el comando **set**:

```
racadm set iDRAC.EmailAlert.Enable.[índice] 1
```

donde [index] es el índice del destino de correo electrónico. 0 desactiva la alerta por correo electrónico y 1 la activa.

El índice del destino de correo electrónico puede ser un valor de 1 a 4. Por ejemplo, para activar el correo electrónico con índice 4, introduzca el comando siguiente:

```
racadm set iDRAC.EmailAlert.Enable.4 1
```

2. Para configurar los valores de correo electrónico:

- Mediante el comando **config**:

```
racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 [email-address]
```

donde 1 es el índice del destino de correo electrónico y [email-address] es la dirección de correo electrónico del destino que recibe las alertas de los sucesos de plataforma.

- Mediante el comando **set**:

```
racadm set iDRAC.EmailAlert.Address.1 [email-address]
```

donde 1 es el índice del destino de correo electrónico y [email-address] es la dirección de correo electrónico del destino que recibe las alertas de los sucesos de plataforma.

3. Para configurar un mensaje personalizado:

- Mediante el comando **config**:

```
racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i [index] [custom-message]
```

donde [index] es el índice del destino de correo electrónico y [custom-message] es el mensaje personalizado.

- Mediante el comando **set**:

```
racadm set iDRAC.EmailAlert.CustomMsg.[índice] [mensaje_personalizado]
```

donde [index] es el índice del destino de correo electrónico y [custom-message] es el mensaje personalizado.

4. Para probar la alerta por correo electrónico configurada, si fuera necesario:

```
racadm testemail -i [index]
```

donde [index] es el índice del destino de correo electrónico que desea probar.

Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8)* disponible en dell.com/support/manuals.

Configuración de los valores de dirección del servidor de correo electrónico SMTP

Debe configurar la dirección del servidor SMTP para las alertas por correo electrónico de modo que se envíen a los destinos especificados.

Configuración de los valores de dirección de servidor de correo electrónico SMTP mediante la interfaz web de iDRAC

Para configurar la dirección del servidor SMTP:

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Servidor** → **Alertas** → **Configuración SNMP y de correo electrónico**.
2. Introduzca la dirección IP válida o el nombre de dominio completamente calificado (FQDN) del servidor SMTP que se va a usar en la configuración.
3. Seleccione la opción **Activar autenticación** y, a continuación, proporcione el nombre de usuario y la contraseña (de un usuario que tenga acceso al servidor SMTP).
4. Introduzca el número de puerto SMTP.
Para obtener más información acerca de los campos, consulte la *Ayuda en línea de iDRAC*.
5. Haga clic en **Apply (Aplicar)**.
Se habrán configurado los valores de SMTP.

Configuración de los valores de dirección de servidor de correo electrónico SMTP mediante RACADM

Para configurar el servidor de correo electrónico SMTP, utilice una de las siguientes opciones:

- Mediante el comando **set**:

```
racadm set iDRAC.RemoteHosts.SMTPServerIPAddress <SMTP E-mail Server IP Address>
```

- Mediante el comando **config**:

```
racadm config -g cfgRemoteHosts -o cfgRhostsSmtServerIpAddr <SMTP E-mail Server IP Address>
```

Configuración de sucesos de WS

El protocolo de sucesos de WS se utiliza para que un servicio cliente (suscriptor) registre el interés (suscripción) en un servidor (fuente de sucesos) para recibir mensajes que contienen los sucesos del servidor (notificaciones o mensajes de sucesos). Los clientes interesados en recibir los mensajes de sucesos de WS pueden suscribirse en iDRAC y recibir sucesos relacionados con los trabajos de Lifecycle Controller.

Los pasos necesarios para configurar la función de sucesos de WS con el fin de recibir mensajes de sucesos de WS para los cambios relacionados con los trabajos de Lifecycle Controller se describen en el documento de especificación sobre la asistencia a sucesos de servicios web para iDRAC 1.30.30. Además de esta especificación, consulte el documento DSP0226 (Especificación de administración de WS DMTF), sección 10 Notificaciones (Sucesos) para obtener la información completa sobre el protocolo de sucesos de WS. Los trabajos relacionados con Lifecycle Controller se describen en el documento de perfiles de control de trabajos de DCIM.

Id. de mensaje de alertas

En la tabla siguiente se proporciona la lista de ID de mensaje que se muestran para las alertas.

Tabla 22. ID de mensaje de alertas

| Id. de mensaje | Descripción |
|-----------------------|---|
| AMP | Amperage |
| ASR | Restablecimiento automático del sistema |
| BAR | Copia de seguridad/restauración |
| BAT | Suceso de la batería |
| BIOS | Administración del BIOS |
| BOOT | Control BOOT |
| CBL | Cable |
| CPU | Procesador |
| CPUA | Procesador ausente |
| CTL | Controladora de almacenamiento |
| DH | Administración de certificados |
| DIS | Descubrimiento automático |
| ENC | Gabinete de almacenamiento |

| Id. de mensaje | Descripción |
|-----------------------|------------------------------|
| FAN | Suceso de ventilador |
| FSD | Depuración |
| HWC | Configuración de hardware |
| IPA | Cambio de IP de DRAC |
| ITR | Intrusión |
| JCP | Control de trabajos |
| LC | Lifecycle Contr |
| LIC | Licencias |
| LNK | Estado de vínculo |
| LOG | Suceso del registro |
| MEM | Memoria |
| NDR | Controlador de SO de NIC |
| NIC | Configuración de NIC |
| OSD | Implementación de SO |
| OSE | Suceso del sistema operativo |
| PCI | Dispositivo PCI |
| PDR | Disco físico |
| PR | Intercambio de piezas |
| PST | POST del BIOS |
| la PSU | Suministro de energía |
| PSUA | PSU ausente |
| PWR | Uso de alimentación |
| RAC | Suceso RAC |
| RDU | Redundancia |
| RED | Descarga de firmware |

| Id. de mensaje | Descripción |
|---------------------------------|---------------------------------------|
| RFL | Medios IDSDM |
| RFLA | IDSDM ausente |
| RFM | SD de dirección flexible |
| RRDU | Redundancia IDSDM |
| RSI | Servicio remoto |
| SEC | Suceso de seguridad |
| Registro de sucesos del sistema | Registro de sucesos del sistema |
| SRD | RAID de software |
| SSD | SSD PCIe |
| STOR | Almacenamiento |
| SUP | Trabajo de actualización del firmware |
| SWC | Configuración de software |
| SWU | Cambio de software |
| SYS | Información del sistema |
| TMP | Temperatura |
| TST | Alerta de prueba |
| UEFI | Suceso UEFI |
| USR | Seguimiento del usuario |
| VDR | Disco virtual |
| VF | Tarjeta VFlash SD |
| VFL | Suceso de vFlash |
| VFLA | vFlash ausente |
| VLT | Tensión |
| VME | Medios virtuales |
| VRM | Consola virtual |

| Id. de mensaje | Descripción |
|----------------|-----------------|
| WRK | Nota de trabajo |

Administración de registros

iDRAC proporciona un registro de Lifecycle que contiene los sucesos relacionados con el sistema, los dispositivos de almacenamiento, los dispositivos de red, las actualizaciones de firmware, los cambios de configuración, los mensajes de licencia, etc. Sin embargo, los sucesos del sistema también están disponibles como un registro independiente denominado Registro de sucesos del sistema (SEL). El registro de Lifecycle es accesible desde la interfaz web de iDRAC, RACADM y la interfaz WS-MAN.

Cuando el tamaño del registro de lifecycle alcanza 800 KB, los registros se comprimen y se archivan. Solo puede ver las entradas de los registros no archivados y aplicar filtros y comentarios a ellos. Para ver registros de ciclos de vida archivados, deberá exportarlos a una ubicación del sistema.

Enlaces relacionados

- [Visualización del registro de sucesos del sistema](#)
- [Visualización del registro de Lifecycle](#)
- [Exportación de los registros de Lifecycle Controller](#)
- [Adición de notas de trabajo](#)
- [Configuración del registro del sistema remoto](#)

Visualización del registro de sucesos del sistema


Cuando se produce un suceso de sistema en un sistema administrado, se registra en el registro de sucesos del sistema (SEL). La misma entrada del SEL también está disponible en el registro de LC.

Visualización del registro de sucesos del sistema mediante la interfaz web

Para ver el SEL, en la interfaz web de iDRAC, vaya a **Descripción general** → **Servidor** → **Registros**.

En la página **Registro de sucesos del sistema** se muestra un indicador de la condición del sistema, una marca de hora y fecha, y una descripción de cada suceso registrado. Para obtener más información, consulte la *Ayuda en línea de iDRAC*.

Haga clic en **Guardar como** para guardar el **SEL** en una ubicación de su elección.

 **NOTA:** Si está utilizando Internet Explorer y hay un problema al guardar, descargue la actualización de seguridad acumulada para Internet Explorer. Se puede descargar desde el sitio web de asistencia de Microsoft en support.microsoft.com.

Para borrar los registros, haga clic en **Borrar registro**.

 **NOTA:** **Borrar registro** sólo aparece si tiene permiso de Borrar registros.

Después de vaciar el SEL, se registra una anotación en el registro de Lifecycle Controller. La anotación del registro incluye el nombre de usuario y la dirección IP de la ubicación desde donde se borró el SEL.

Visualización del registro de sucesos del sistema mediante RACADM

Para ver el SEL:

```
racadm getsel <options>
```

Si no se especifican argumentos, se muestra todo el registro.

Para mostrar el número de anotaciones de SEL: `racadm getsel -i`

Para borrar las anotaciones de SEL: `racadm clrsel`

Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8) disponible en dell.com/support/manuals.

Visualización del registro de sucesos del sistema mediante la utilidad de configuración de iDRAC

Es posible ver la cantidad total de registros del registro de sucesos del sistema (SEL) mediante la utilidad de configuración de iDRAC. Además es posible borrar los registros. Para realizar estas acciones:

1. En la utilidad de configuración de iDRAC, vaya a **Registro de sucesos del sistema**. La página **Configuración de iDRAC - Registro de sucesos del sistema** muestra la **cantidad total de registros**.
2. Para borrar los registros, seleccione **Sí**. De lo contrario, seleccione **No**.
3. Para ver los sucesos del sistema, haga clic en **Mostrar registro de sucesos del sistema**.
4. Haga clic en **Atrás**, en **Terminar** y, a continuación, en **Sí**.

Visualización del registro de Lifecycle

Los registros de Lifecycle Controller proporcionan un historial de los cambios relacionados con los componentes instalados en un sistema administrado y proporcionan registros acerca de los sucesos relacionados con lo siguiente:

- Dispositivos de almacenamiento
- Sucesos del sistema
- Dispositivos de red
- Configuración
- Auditorías
- Actualizaciones
- Notas de trabajo

Cuando inicia o cierra sesión en iDRAC mediante alguna de las siguientes interfaces, el inicio de sesión, el cierre de sesión o los sucesos de falla de inicio de sesión se registran en los registros de Lifecycle:

- Telnet
- SSH
- Interfaz web
- RACADM

- SM-CLP
- IPMI en la LAN
- Serie
- Consola virtual
- Medios virtuales

Puede filtrar los registros en función de la categoría y el nivel de gravedad. También puede ver, exportar y agregar notas de trabajo a un suceso del registro.

Enlaces relacionados

[Filtrado de los registros de Lifecycle](#)

[Exportación de los registros de Lifecycle Controller mediante la interfaz web](#)

[Adición de comentarios a los registros de Lifecycle.](#)

Visualización del registro de Lifecycle mediante la interfaz web

Para ver los registros de Lifecycle, haga clic en **Descripción general** → **Servidor** → **Registros** → **Registro de Lifecycle**. Se muestra la página **Registro de Lifecycle**. Para obtener más información acerca de las opciones, consulte la *Ayuda en línea de iDRAC*.

Filtrado de los registros de Lifecycle

Puede filtrar los registros según la categoría, la gravedad, una palabra clave o un intervalo de fechas.

Para filtrar los registros de lifecycle:

1. En la página **Registro de ciclos de vida**, bajo **Filtro del registro**, realice una o todas las acciones siguientes:
 - Seleccione **Tipo de registro** de la lista desplegable.
 - Seleccione el nivel de gravedad de la lista desplegable **Gravedad**.
 - Introduzca una palabra clave.
 - Especifique el intervalo de fechas.
2. Haga clic en **Apply (Aplicar)**.
Las entradas filtradas del registro se muestran en **Resultados del registro**.

Adición de comentarios a los registros de Lifecycle.

Para agregar comentarios a los registros de lifecycle:

1. En la página **Registro de Lifecycle**, haga clic en el icono de la anotación de registro deseada.
Se muestran los detalles del ID de mensaje.
2. Introduzca los comentarios para la anotación de registro en el cuadro **Comentario**.
Los comentarios se muestran en el cuadro **Comentario**.

Visualización del registro de Lifecycle mediante RACADM

Para ver los registros de Lifecycle, utilice el comando `lcllog`. Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8)* disponible en dell.com/support/manuals.

Exportación de los registros de Lifecycle Controller


Puede exportar todo el registro de Lifecycle Controller (anotaciones activas y archivadas) en un archivo XML comprimido individual a un recurso compartido de red o al sistema local. La extensión del archivo

XML comprimido es **.xml.gz**. Las anotaciones de archivo se ordenan en forma de secuencia según sus números de secuencia, desde el menor hasta el mayor.

Exportación de los registros de Lifecycle Controller mediante la interfaz web

Para exportar los registros de Lifecycle Controller mediante la interfaz web:

1. En la página **Registro de Lifecycle**, haga clic en **Exportar**.
2. Seleccione cualquiera de las opciones siguientes:
 - **Red**: exporte los registros de Lifecycle Controller a una ubicación compartida de la red.
 - **Local**: exporte los registros de Lifecycle Controller a una ubicación del sistema local.

 **NOTA:** Mientras se especifica la configuración para el recurso compartido de red, se recomienda evitar el uso de caracteres especiales en el nombre de usuario y la contraseña o codificar por porcentaje los caracteres especiales.

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


3. Haga clic en **Exportar** para exportar el registro a la ubicación especificada.

Exportación de los registros de Lifecycle Controller mediante RACADM

Para exportar los registros de Lifecycle Controller mediante RACADM, utilice el comando `lcclog export`. Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8)* disponible en dell.com/support/manuals o dell.com/esmanuals.


Adición de notas de trabajo

Todos los usuarios que inician sesión en iDRAC puede agregar notas de trabajo y estas se almacenan como un suceso en el registro de ciclos de vida. Debe disponer de privilegios para los registros de iDRAC para agregar notas de trabajo y se admite un máximo de 255 caracteres para cada una de ellas.

 **NOTA:** No es posible eliminar notas de trabajo.

Para agregar una nota de trabajo:

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Servidor** → **Propiedades** → **Resumen**. Aparecerá la página **Configuración del sistema**.
2. En **Notas de trabajo**, introduzca el texto en el cuadro de texto vacío.

 **NOTA:** Es recomendable no utilizar demasiados caracteres especiales.

3. Haga clic en **Agregar**.

La nota de trabajo se agrega al registro. Para obtener más información, consulte la *Ayuda en línea de iDRAC*.

Configuración del registro del sistema remoto

Puede enviar registros de lifecycle a un sistema remoto. Antes de hacerlo, asegúrese de lo siguiente:

- Hay conectividad de red entre iDRAC y el sistema remoto.
- El sistema remoto e iDRAC se encuentran en la misma red.

Configuración del registro del sistema remoto mediante la interfaz web

Para configurar los valores del servidor de registro del sistema remoto:

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Servidor** → **Registros** → **Configuración**. Aparece la pantalla **Configuración del registro del sistema remoto**.
2. Active el registro del sistema remoto y especifique la dirección del servidor y el número de puerto. Para obtener más información acerca de estas opciones, consulte la *Ayuda en línea de iDRAC*.
3. Haga clic en **Apply (Aplicar)**.
Se guarda la configuración. Todos los registros que se graban en el registro de lifecycle también se graban simultáneamente en los servidores remotos configurados.

Configuración del registro del sistema remoto mediante RACADM

Para configurar los valores del servidor de syslog remoto, utilice una de las siguientes opciones:

- Objetos del grupo **cfgRemoteHosts** con el comando **config**.
- Objetos del grupo **iDRAC.SysLog** con el comando **set**.

Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8)* disponible en **dell.com/support/manuals**.

Supervisión y administración de la alimentación

Puede utilizar iDRAC para supervisar y administrar los requisitos de alimentación del sistema administrado. Esto ayuda a proteger el sistema de cortes en el suministro eléctrico al distribuir y regular correctamente el consumo de alimentación del sistema.

Las características claves son las siguientes:

- **Supervisión de alimentación:** consulte el estado de alimentación, el historial de las mediciones de alimentación, los promedios actuales, los picos, etc. para el sistema administrado.
- **Límites de alimentación:** consulte y establezca los límites de alimentación del sistema administrado, incluida la visualización del consumo de alimentación potencia mínimo y máximo. Esta función requiere una licencia.
- **Control de alimentación:** permite realizar operaciones de control de alimentación de manera remota (tal como encendido, apagado, restablecimiento del sistema, ciclo de encendido y apagado ordenado) en el sistema administrado.
- **Opciones de suministro de energía:** permiten configurar las opciones de suministro de energía, tal como la política de redundancia, el repuesto dinámico y la corrección del factor de alimentación.

Enlaces relacionados

[Supervisión de la alimentación](#)

[Ejecución de las operaciones de control de alimentación](#)

[Límites de alimentación](#)

[Configuración de las opciones de suministro de energía](#)

[Activación o desactivación del botón de encendido](#)

[Configuración del umbral de advertencia para consumo de alimentación](#)

Supervisión de la alimentación

iDRAC supervisa el consumo de alimentación del sistema continuamente y muestra los siguientes valores de alimentación:

- Umbrales de advertencia y críticos del consumo de alimentación
- Valores acumulados de alimentación, alimentación pico y amperaje pico.
- Consumo de alimentación de la última hora, el último día o la última semana
- Consumo de alimentación promedio, mínimo y máximo
- Valores pico históricos y marcas de tiempo picos
- Valores espacio pico y de espacio instantáneo (para los servidores de tipo bastidor y torre).

Supervisión de la alimentación mediante la interfaz web

Para ver la información de supervisión de la alimentación, en la interfaz web de iDRAC vaya a **Descripción general** → **Servidor** → **Alimentación/Térmico** → **Supervisión de alimentación**. Se muestra la página **Supervisión de alimentación**. Para obtener más información, consulte la *Ayuda en línea de iDRAC*.

Supervisión de la alimentación mediante RACADM

Para ver la información de supervisión de la alimentación, utilice los objetos en el grupo **System.Power** con el comando **get** o el objeto **cfgServerPower** con el comando **getConfig**. Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8)* disponible en dell.com/support/manuals.

Configuración del umbral de advertencia para consumo de alimentación

Es posible establecer el valor de umbral de advertencia para el sensor de consumo de alimentación en los sistemas tipo bastidor y torre. El umbral de alimentación de advertencia/crítico para los sistemas de torre y bastidor puede cambiar en un ciclo de encendido del sistema según la capacidad de la unidad de suministro de energía y la política de redundancia. Sin embargo, el umbral de advertencia no debe exceder el umbral crítico aunque cambie la capacidad de la unidad de suministro de energía de la política de redundancia.

El umbral de alimentación de advertencia para los sistemas de tipo bastidor se establece según la asignación de alimentación para CMC.

Si se realiza una acción para restablecer los valores predeterminados, los umbrales de alimentación se establecerán en los valores predeterminados.

Es necesario tener el privilegio de usuario de configuración para establecer el valor del umbral de advertencia para el sensor de consumo de alimentación.

Configuración del umbral de advertencia para consumo de alimentación mediante la interfaz web

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Servidor** → **Alimentación/Térmico** → **Supervisión de alimentación**.
Se mostrará la página **Supervisión de alimentación**.
2. En la sección **Umbrales y lecturas de alimentación actuales**, de la columna **Umbral de advertencia**, introduzca el valor en **Vatios** o **BTU/h**.
Los valores deben ser menores que los valores de **Umbral de falla**. Los valores se redondean al valor más cercano que sea divisible por 14. Si se introducen **Vatios**, el sistema calcula y muestra automáticamente el valor en **BTU/h**. De manera similar, si se introduce **BTU/h**, se muestra el valor en **Vatios**.
3. Haga clic en **Aplicar**. Se configurarán los valores.

Ejecución de las operaciones de control de alimentación

iDRAC permite encender, apagar, restablecer, apagar de manera ordenada, realizar una interrupción sin máscara (NMI) o un ciclo de encendido del sistema de manera remota mediante la interfaz web o RACADM.

Estas operaciones también se pueden realizar mediante Lifecycle Controller Remote Services o WS Management. Para obtener más información, consulte *Lifecycle Controller Remote Services Quick Start Guide* (Guía de inicio rápido de Lifecycle Controller Remote Services) disponible en dell.com/support/manuals y el documento de perfiles de *Dell Power State Management* disponible en delltechcenter.com.

Ejecución de las operaciones de control de alimentación mediante la interfaz web

Para realizar las operaciones de control de alimentación:

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Servidor** → **Alimentación/Térmico** → **Configuración de la alimentación** → **Control de alimentación**. Se mostrará la página **Control de alimentación**.
2. Seleccione la operación de alimentación necesaria:
 - Encender el sistema
 - Apagar el sistema
 - NMI (Interrupción no enmascarable)
 - Apagado ordenado
 - Restablecer el sistema (reinicio mediante sistema operativo)
 - Realizar ciclo de encendido del sistema (reinicio mediante suministro de energía)
3. Haga clic en **Aplicar**. Para obtener más información, consulte la *Ayuda en línea de iDRAC*.

Ejecución de las operaciones de control de alimentación mediante RACADM

Para realizar acciones relacionadas con la alimentación, utilice el comando **serveraction**. Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8)* disponible en dell.com/support/manuals.

Límites de alimentación

Puede ver los límites de umbral de alimentación que cubre la gama de consumo de alimentación de CA y CC que un sistema de carga de trabajo elevada presenta al centro de datos. Esta función requiere licencia.

Límites de alimentación en servidores Blade

Antes de que se encienda el servidor blade, iDRAC proporciona a CMC sus requisitos de alimentación. Es mayor que la alimentación real que puede consumir el servidor blade y se calcula según la información sobre el inventario de hardware limitado. Es posible que al encenderse iDRAC, el servidor solicite un intervalo de alimentación mayor según la alimentación real que consuma el servidor. Si aumenta el consumo de alimentación con el tiempo y si el servidor consume una alimentación cercana a su asignación máxima, es posible que iDRAC solicite un aumento del consumo de alimentación potencial

máximo, por lo que aumentará el intervalo de alimentación. iDRAC solo aumenta su solicitud de consumo de alimentación potencial máximo a CMC. No solicita una alimentación potencial menor si el consumo disminuye. iDRAC sigue solicitando más alimentación y el consumo de alimentación supera la alimentación que asigne CMC.

Una vez encendido e inicializado el sistema, iDRAC calcula un nuevo requisito de alimentación basado en la configuración real del servidor blade. Este último permanece encendido incluso si CMC no consigue asignar una nueva solicitud de alimentación.

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 existe suficiente alimentación asignada, el servidor blade no se enciende. Si se ha asignado alimentación suficiente al servidor blade, iDRAC enciende el sistema.

Visualización y configuración de la política de límites de alimentación

Cuando está activada la política de límites de alimentación, se aplican al sistema límites de alimentación definidos por el usuario. En caso contrario, utiliza la política de protección de hardware que se implementa de manera predeterminada. Esta política de protección de la alimentación es independiente de la política definida por el usuario. el rendimiento del sistema se ajusta de manera dinámica para mantener el consumo de alimentación a un nivel cercano al umbral especificado.

El consumo de alimentación real puede ser inferior para cargas de trabajo ligeras y puede superar momentáneamente el umbral hasta que se completen los ajustes de rendimiento. Por ejemplo, para una configuración del sistema concreta, con un consumo de alimentación potencial máximo de 700W y un consumo de alimentación potencial mínimo de 500W, puede especificar y activar un umbral de presupuesto de alimentación para reducir el consumo de su 650W actual a 525W. A partir de ese momento, el rendimiento del sistema se ajusta dinámicamente para mantener el consumo de alimentación de modo que no exceda el umbral de 525W especificado por el usuario.

Si el valor de límite de alimentación se establece a un valor inferior al umbral mínimo recomendado, es posible que iDRAC no pueda mantener el límite deseado.

El valor se puede especificar en vatios, BTU/hora o como un porcentaje (%) del límite de alimentación máximo recomendado.

Cuando el umbral de límites de alimentación se establece en BTU/hora, la conversión en vatios se redondea al entero más cercano. Al volver a leer el umbral, la conversión de vatios a BTU/hora se vuelve a redondear del mismo modo. Como resultado, el valor de escritura podría ser ligeramente diferente del valor de lectura. Por ejemplo, un umbral establecido en 600 BTU/hora podría volver a leerse como 601 BTU/hora.

Configuración de la política de límites de alimentación mediante la interfaz web

Para ver y configurar las políticas de alimentación:

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Servidor** → **Alimentación/Térmico** → **Configuración de la alimentación** → **Configuración de la alimentación**. Se mostrará la página **Control de alimentación**.

Aparece la página **Configuración de alimentación**. El límite de la política de alimentación actual se muestra en la sección **Política de límites de alimentación activa actualmente**.

2. Seleccione **Activar** bajo **Política de límites de alimentación de iDRAC**.
3. En la sección **Límites definidos por el usuario**, introduzca el límite de alimentación máximo en vatios y BTU/hora o el porcentaje (%) máximo del límite de sistema recomendado.
4. Haga clic en **Aplicar** para aplicar los valores.

Configuración de la política de límites de alimentación mediante RACADM

Para ver y configurar los valores de límites de alimentación actuales:

- Utilice los objetos siguientes con el subcomando **config**:
 - cfgServerPowerCapWatts
 - cfgServerPowerCapBTUhr
 - cfgServerPowerCapPercent
 - cfgServerPowerCapEnable
- Utilice los objetos siguientes con el subcomando **set**:
 - System.Power.Cap.Enable
 - System.Power.Cap.Watts
 - System.Power.Cap.Btuhr
 - System.Power.Cap.Percent

Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8) disponible en **dell.com/support/manuals**.

Configuración de la política de límites de alimentación mediante la utilidad de configuración de iDRAC

Para ver y configurar las políticas de alimentación:

1. En la utilidad de configuración de iDRAC, vaya a **Configuración de la alimentación**.



NOTA: El vínculo **Configuración de alimentación** está disponible solo si la unidad de suministro de energía del servidor admite la supervisión de alimentación.

Se muestra la página **Configuración de alimentación de la configuración de iDRAC**.

2. Seleccione **Activado** para activar la opción **Política de límites de alimentación**. De lo contrario, seleccione **Desactivado**.
3. Utilice los valores recomendados o, en **Política de límites de alimentación definida por el usuario**, introduzca los límites necesarios.

Para obtener más información acerca de las opciones, consulte la *Ayuda en línea de la utilidad de configuración de iDRAC*.

4. Haga clic en **Atrás**, en **Terminar** y, a continuación, en **Sí**.
Se habrán configurado los valores de límites de alimentación.

Configuración de las opciones de suministro de energía

Puede configurar las opciones de suministro de energía, tal como la política de redundancia, repuesto dinámico y corrección del factor de alimentación.

El repuesto dinámico es una función de suministro de energía que configura las unidades de suministro de energía (PSU) redundantes para que se apeguen en función de la carga del servidor. Esto permite a las PSU restantes funcionar con una mayor carga y eficacia. Esto requiere PSU que admitan esta función de modo que se pueda encender rápidamente si fuera necesario.

En un sistema de dos PSU, es posible configurar PSU1 o PSU2 como la PSU principal. En un sistema de cuatro PSU, se debe establecer el par de PSU (1+1 o 2+2) como la PSU principal.

Después de activar el repuesto dinámico, las unidades de suministro de energía pueden activarse o suspenderse en función de la carga. Si Repuesto dinámico está activado, se activa la corriente eléctrica asimétrica que se comparte entre las dos unidades de suministro de energía. Una unidad de suministro de energía está *activa* y proporciona la mayoría de la corriente mientras que la otra se encuentra suspendida y proporciona una pequeña cantidad de corriente. Esto suele denominarse 1+0 con dos unidades de suministro de energía y repuesto dinámico activado. Si todas las unidades de suministro de energía 1 están en el circuito A y las unidades de suministro de energía 2 en el circuito B, con el repuesto dinámico activado (configuración de repuesto dinámico de fábrica predeterminada), el circuito B tiene mucho menos carga y dispara los avisos. Si se desactiva el repuesto dinámico, la corriente eléctrica se comparte en partes iguales (50-50) por las dos unidades de suministro de energía y los circuitos A y B generalmente tienen la misma carga.

El factor de alimentación es la relación de alimentación real consumida con respecto a la alimentación aparente. Cuando la corrección del factor de alimentación está activada, el servidor consume una pequeña cantidad de alimentación cuando el host está apagado. De forma predeterminada, la corrección del factor de alimentación está activada cuando el servidor se envía de fábrica.

Configuración de las opciones de suministro de energía mediante la interfaz web

Para configurar las opciones de suministro de energía:

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Servidor** → **Alimentación/Térmico** → **Configuración de la alimentación** → **Configuración de la alimentación**. Se mostrará la página **Configuración de la alimentación**.
2. En **Opciones de suministro de energía**, seleccione las opciones necesarias. Para obtener más información, consulte la *Ayuda en línea de iDRAC*.
3. Haga clic en **Aplicar**. Se habrán configurado los valores de suministro de energía.

Configuración de las opciones de suministro de energía mediante RACADM

Para configurar las opciones de suministro de energía, utilice los siguientes objetos con el subcomando **set**:


- System.Power.RedundancyPolicy
- System.Power.Hotspare.Enable
- System.Power.Hotspare.PrimaryPSU
- System.Power.PFC.Enable

Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8)* disponible en dell.com/support/manuals.

Configuración de las opciones de suministro de energía mediante la utilidad de configuración de iDRAC

Para configurar las opciones de suministro de energía:

1. En la utilidad de configuración de iDRAC, vaya a **Configuración de la alimentación**.

 **NOTA:** El vínculo **Configuración de alimentación** está disponible solo si la unidad de suministro de energía del servidor admite la supervisión de alimentación.

Se muestra la página **Configuración de la alimentación de la configuración de iDRAC**.

2. En **Opciones de suministro de energía**:
 - Activa o desactive la redundancia del suministro de energía.
 - Active o desactive el repuesto dinámico.
 - Establezca la unidad principal de suministro de energía.
 - Active o desactive la corrección del factor de alimentación. Para obtener más información acerca de las opciones, consulte la *Ayuda en línea de la utilidad de configuración de iDRAC*.
3. Haga clic en **Atrás**, en **Terminar** y, a continuación, en **Sí**.
Se habrán configurado los valores de suministro de energía.

Activación o desactivación del botón de encendido

Para activar o desactivar el botón de encendido del sistema administrado:

1. En la utilidad de configuración de iDRAC, vaya a **Seguridad del panel frontal**.
Se mostrará la página **Configuración de iDRAC - Seguridad del panel frontal**.
2. Seleccione **Activado** para activar el botón de encendido. de lo contrario seleccione **Desactivado**.
3. Haga clic en **Atrás**, en **Terminar** y, a continuación, en **Sí**. Se guardará la configuración

Inventario, supervisión y configuración de dispositivos de red

Es posible crear un inventario, supervisar y configurar los siguientes dispositivos de red:

- Tarjetas de interfaz de red (NIC)
- Adaptadores de red convergentes (CNA)
- LAN de la placa base (LOM)
- Tarjetas secundarias de interfaz de red (NIC)
- Tarjetas mezzanine (solo para servidores Blade)

Enlaces relacionados

[Inventario y supervisión de dispositivos HBA FC](#)

[Configuración dinámica de las direcciones virtuales, del iniciador y del destino de almacenamiento](#)

Inventario y supervisión de dispositivos de red

Es posible supervisar de manera remota la condición de los siguientes dispositivos de red en el sistema administrado y ver el inventario de los mismos:

Para cada dispositivo, puede ver la siguiente información sobre los puertos y las particiones admitidas:

- Estado de vínculo
- Propiedades
- Configuración y capacidades
- Estadísticas de recepción y transmisión


Enlaces relacionados

[Inventario, supervisión y configuración de dispositivos de red](#)

[Configuración dinámica de las direcciones virtuales, del iniciador y del destino de almacenamiento](#)

Supervisión de dispositivos de red mediante la interfaz web

Para ver la información del dispositivo de red mediante la interfaz de red, vaya a **Descripción general** → **Hardware** → **Dispositivo de red**. Se muestra la página **Dispositivos de red**. Para obtener más información acerca de las propiedades mostradas, consulte la *Ayuda en línea de iDRAC*.

 **NOTA:** Si **Estado del controlador de SO** muestra el estado como Operativo, indica el estado del controlador del sistema operativo o el estado de controlador UEFI.

Supervisión de dispositivos de red mediante RACADM

Para ver la información de un dispositivo de red, utilice los comandos **hwinventory** y **nicstatistics**. Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide (Guía de*

referencia de la interfaz de línea de comandos RACADM para iDRAC8) disponible en dell.com/support/manuals.

Pueden mostrarse propiedades adicionales cuando se utiliza RACADM o WS-MAN, además de las propiedades que se muestran en la interfaz web de iDRAC.

Inventario y supervisión de dispositivos HBA FC

Es posible supervisar de forma remota la condición y ver el inventario de los dispositivos adaptadores de bus host de Fibre Channel (HBA FC) en el sistema administrado. Se admiten HBA FC Emulex y QLogic (excepto FC8). Para cada dispositivo HBA FC, puede ver la información siguiente de los puertos:

- Información y estado del vínculo
- Propiedades de puertos
- Estadísticas de recepción y transmisión

Enlaces relacionados

[Inventario, supervisión y configuración de dispositivos de red](#)

Supervisión de dispositivos HBA FC mediante la interfaz web

Para ver la información de dispositivos HBA FC mediante la interfaz web, vaya a **Descripción general** → **Hardware** → **Fibre Channel**. Se mostrará la página de FC. Para obtener más información sobre las propiedades que se muestran, consulte la *Ayuda en línea de iDRAC*.

El nombre de la página muestra también el número de ranura en donde el dispositivo HBA FC está disponible y el tipo de dispositivo HBA FC.

Supervisión de dispositivos HBA FC mediante RACADM

Para ver la información de dispositivos HBA FC mediante racadm, utilice el subcomando **hwinventory**. Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8)* disponible en dell.com/support/manuals.


Configuración dinámica de las direcciones virtuales, del iniciador y del destino de almacenamiento

De manera dinámica, se pueden ver y configurar los valores de dirección virtual, iniciador y destino de almacenamiento, así como aplicar una política de persistencia. Esto permite que la aplicación aplique la configuración según los cambios en el estado de la alimentación (es decir, reinicio de sistema operativo, restablecimiento mediante sistema operativo, restablecimiento mediante suministro de energía o ciclo de CA) y también en función de la configuración de la política de persistencia para ese estado de la alimentación. Esto proporciona más flexibilidad en las implementaciones donde se necesita una reconfiguración rápida de las cargas de trabajo de un sistema a otro.

Las direcciones virtuales son:

- Dirección MAC virtual
- Dirección MAC de iSCSI virtual
- Dirección MAC de FIP virtual
- WWN virtual

- WWPN virtual

 **NOTA:** Al borrar la política de persistencia, todas las direcciones virtuales se restablecen a la dirección permanente predeterminada de fábrica.

Con la característica de identidad de E/S, es posible:

- Ver y configurar las direcciones virtuales para los dispositivos de red (por ejemplo, NIC, CNA, HBA de Fibre Channel)
- Configurar los valores para el iniciador (para iSCSI y FCoE) y el destino de almacenamiento (para iSCSI, FCoE y FC)
- Especificar la persistencia o la autorización de los valores configurados sobre una pérdida de alimentación de CA, un restablecimiento mediante sistema operativo y un restablecimiento mediante suministro de energía en el sistema

Los valores configurados para las direcciones virtuales, el iniciador y los destinos de almacenamiento pueden variar en función de la forma en que se maneja la alimentación eléctrica principal durante el restablecimiento del sistema y si los dispositivos NIC, CNA o HBA de FC tienen una alimentación auxiliar. La persistencia de la configuración de identidad de E/S se puede lograr en función de la configuración de políticas realizada mediante iDRAC.

Las políticas de persistencia surten efecto únicamente si la función de identidad de E/S se encuentra activada. Cada vez que el sistema se restablece o se enciende, los valores se mantienen o se borran en función de la configuración de políticas.

Enlaces relacionados

[Inventario, supervisión y configuración de dispositivos de red](#)

[Tarjetas admitidas para la optimización de la identidad de E/S](#)

[Versión del BIOS admitida para la optimización de la identidad de E/S](#)

[Versiones del firmware de la NIC admitidas para la optimización de la identidad de E/S](#)

[Activación o desactivación de la optimización de la identidad de E/S](#)


[Configuración de la política de persistencia](#)

Tarjetas admitidas para la optimización de la identidad de E/S

La siguiente tabla proporciona las tarjetas que admiten la función de optimización de la identidad de E/S.

| Fabricante | Tipo |
|------------|--|
| Broadcom | <ul style="list-style-type: none"> • 5720 PCIe de 1 GB • 5719 PCIe de 1 GB • 57810 PCIe de 10 GB • 57810 bNDC de 10 GB • 57800 rNDC de 10 GB+1 GB • 57840 rNDC de 10 GB • 57840 bNDC de 10 GB • 5720 rNDC de 1 GB • 5719 Mezz de 1 GB • 57810 Mezz de 10 GB • 5720 bNDC de 1 GB |
| Intel | <ul style="list-style-type: none"> • i350 Mezz de 1 Gb |

| Fabricante | Tipo |
|------------|---|
| | <ul style="list-style-type: none"> x520+i350 rNDC de 10 Gb+1 Gb I350 bNDC de 1 Gb x540 PCIe de 10 Gb x520 PCIe de 10 Gb i350 PCIe de 1 Gb x540+i350 rNDC de 10 Gb+1 Gb i350 rNDC de 1 Gb x520 bNDC de 10 Gb |
| QLogic | <ul style="list-style-type: none"> QME2662 Mezz FC16 FC16 PCIe QLE2660 FC16 PCIe QLE2662 |
| Emulex | <ul style="list-style-type: none"> LPM16002 Mezz FC16 FC16 PCIe LPe16000 FC16 PCIe LPe16002 LPM16002 Mezz FC16 OCm14104-UX-D rNDC de 10 Gb OCm14102-U2-D bNDC de 10 Gb OCm14102-U3-D Mezz de 10 Gb Ce14102-UX-D PCIe de 10 Gb |

 **NOTA:** La Optimización de la identidad de E/S no se admite en las siguientes tarjetas:

- Intel x520 Mezz de 10 GB
- Tarjetas Mellanox

Versión del BIOS admitida para la optimización de la identidad de E/S

En los servidores Dell PowerEdge de 13.^a generación, la versión del BIOS necesaria se encuentra disponible de manera predeterminada.

La siguiente tabla proporciona la versión mínima del BIOS admitida en los servidores PowerEdge de 12.^a generación.

| Servidores Dell PowerEdge de 12. ^o generación | Versión mínima del BIOS admitida |
|--|----------------------------------|
| R720, R720xd, R620, T620 y M620 | 2.1.0 |
| R820 | 2.0.15 |
| R520, R320, R420, T420, T320, M520 y M420 | 2.0.19 |
| M820 | 1.7.0 |

Versiones del firmware de la NIC admitidas para la optimización de la identidad de E/S

En los servidores Dell PowerEdge de 13.^a generación, el firmware de NIC necesario se encuentra disponible de manera predeterminada.

La siguiente tabla proporciona las versiones del firmware de la NIC para la función de optimización de la identidad de E/S.

| Fabricante | Versión del firmware de la NIC admitida |
|-------------------|---|
| Tarjetas Broadcom | 7.8.x |
| Tarjetas Intel | 15.0.x |
| QLogic 82xx (CNA) | 1.13.x/6.0.0.x |

Comportamiento del sistema para FlexAddress e identidad de E / S

| | Estado de la función FlexAddress en el CMC | Estado de la función de identidad de E/S en el iDRAC | ¿Dirección virtual de agente remoto disponible para este ciclo de reinicio? | Origen de programación de dirección virtual | Comportamiento de la persistencia de dirección virtual de ciclo de reinicio |
|---|--|--|---|---|---|
| Servidor con persistencia equivalente de FA | Activado | Desactivado | | FlexAddress desde el CMC | Según las especificaciones de FlexAddress |
| | N/A, Activado o Desactivado | Activado | Sí: nuevo o que persiste | Dirección virtual de agente remoto | Según las especificaciones de FlexAddress |
| | | | No | Dirección virtual borrada | |
| Servidor con función de política de persistencia de VAM | Desactivado | Desactivado | | | |
| | Activado | Desactivado | | FlexAddress desde el CMC | Según las especificaciones de FlexAddress |
| | Activado | Activado | Sí: nuevo o que persiste | Dirección virtual de agente remoto | Según la configuración de la política de agente remoto |
| | | | No | FlexAddress desde el CMC | Según las especificaciones de FlexAddress |
| | Desactivado | Activado | Sí: nuevo o que persiste | Dirección virtual de agente remoto | Según la configuración de la política de agente remoto |
| | | | No | Dirección virtual borrada | |
| Desactivado | Desactivado | | | | |

Activación o desactivación de la optimización de la identidad de E/S

Generalmente, después del inicio del sistema, los dispositivos se configuran y se inicializan después de un reinicio. Puede activar la función Optimización de la identidad de E/S para lograr la optimización del inicio. Si está activada, configura la dirección virtual, el iniciador y los atributos del destino de almacenamiento después de restablecer el dispositivo y antes de su inicialización, lo que elimina la necesidad de un segundo reinicio del BIOS. La configuración de los dispositivos y la operación de inicio se producen en un solo inicio del sistema y se optimiza para el rendimiento del tiempo de inicio.

Antes de activar la optimización de la identidad de E/S, asegúrese de que:

- Tiene privilegios de Inicio de sesión, Configurar y Control del sistema.
- BIOS, iDRAC y las tarjetas de red se actualizan al firmware más reciente. Para obtener información acerca de las versiones admitidas, consulte [Versión del BIOS admitida para la optimización de la identidad de E/S](#) y [Versión del firmware de la NIC admitida para la optimización de la identidad de E/S](#).

Después activar la función Optimización de la identidad de E/S, exporte el archivo de configuración XML de iDRAC, modifique los atributos necesarios de la identidad de E/S en el archivo de configuración XML e importe el archivo nuevamente al iDRAC.

Para obtener la lista de atributos de Optimización de la identidad de E/S que puede modificar en el archivo de configuración XML, consulte el documento *Perfil de NIC* disponible en delltechcenter.com/idrac.

 **NOTA:** No modifique los atributos que no corresponden a la optimización de la identidad de E/S.

Activación o desactivación de la optimización de la identidad de E/S mediante la interfaz web

Para activar o desactivar la optimización de la identidad de E/S:

1. En la interfaz web del iDRAC, vaya a **Descripción general** → **Hardware** → **Dispositivos de red**. Se mostrará la página **Dispositivos de red**.
2. Haga clic en la ficha **Optimización de identidad E/S**, seleccione la opción **Optimización de identidad E/S** para activar esta función. Para desactivarla, borre esta opción.
3. Haga clic en **Aplicar** para aplicar la configuración.

Activación o desactivación de la optimización de la identidad de E/S mediante RACADM

Para activar la optimización de la identidad de E/S, utilice el comando:

```
racadm set idrac.ioidopt.IOIDOptEnable Enabled
```

Después de activar esta función debe reiniciar el sistema para que la configuración surta efecto.

Para desactivar la optimización de la identidad de E/S, utilice el comando:

```
racadm set idrac.ioidopt.IOIDOptEnable Disabled
```

Para ver la configuración de la optimización de la identidad de E/S, utilice el comando:

```
racadm get iDRAC.IOIDOpt
```

Configuración de la política de persistencia

Con la identidad de E/S, es posible configurar políticas en las que se especifiquen los comportamientos de restablecimiento y ciclo de encendido del sistema con los que se determina la persistencia o la autorización de los valores de configuración de dirección virtual, iniciador y destino de almacenamiento. Cada uno de los atributos de política de persistencia se aplica a todos los puertos y las particiones de todos los dispositivos correspondientes en el sistema. El comportamiento de los dispositivos cambia según sean de alimentación auxiliar o no.

Es posible configurar los siguientes políticas de persistencia:

- Dirección virtual: dispositivos de alimentación auxiliar
- Dirección virtual: dispositivos que no son de alimentación auxiliar
- Iniciador
- Destino de almacenamiento

Antes de aplicar la política de persistencia, asegúrese de:

- Realizar el inventario de hardware de red al menos una vez, es decir, activar la opción Recopilar inventario del sistema al reinicio.
- Activar Optimización de identidad de E/S.

Los sucesos se registran en el registro de Lifecycle Controller en las siguientes situaciones:

- Se activa o desactiva la opción Optimización de identidad de E/S.
- Se modifica la política de persistencia.
- Cuando la dirección virtual, el iniciador y los valores de destino se establecen según la política. Se registra una anotación de registro única para los dispositivos configurados y los valores que se han establecido para esos dispositivos cuando se aplica la política.

Las acciones de suceso están activadas para SNMP, correo electrónico o notificaciones de sucesos de WS. Los registros también se incluyen en los registros del sistema remoto.

Valores predeterminados para la política de persistencia

| Política de persistencia | Pérdida de alimentación de CA | Reinicio mediante suministro de energía | Reinicio mediante sistema operativo |
|---|-------------------------------|---|-------------------------------------|
| Dirección virtual: dispositivos de alimentación auxiliar | No seleccionado | Seleccionado | Seleccionado |
| Dirección virtual: dispositivos que no son de alimentación auxiliar | No seleccionado | No seleccionado | Seleccionado |
| Iniciador | Seleccionado | Seleccionado | Seleccionado |
| Destino de almacenamiento | Seleccionado | Seleccionado | Seleccionado |

Enlaces relacionados

[Activación o desactivación de la optimización de la identidad de E/S](#)

Configuración de la política de persistencia mediante la interfaz web de iDRAC

Para configurar la política de persistencia:

1. En la interfaz web del iDRAC, vaya a **Descripción general** → **Hardware** → **Dispositivos de red**.
Se mostrará la página **Dispositivos de red**.
2. Haga clic en la ficha **Optimización de identidad de E/S**.
3. En la sección **Política de persistencia**, seleccione una o varias de las siguientes opciones para cada política de persistencia:
 - **Pérdida de alimentación de CA**: la dirección virtual o los valores de destino se conservan cuando se producen condiciones de pérdida de la alimentación de CA.
 - **Reinicio mediante suministro de energía**: la dirección virtual o los valores de destino se conservan cuando se producen condiciones de reinicio mediante suministro de energía.
 - **Reinicio mediante sistema operativo**: la dirección virtual o los valores de destino se conservan cuando se producen condiciones de reinicio mediante sistema operativo.
4. Haga clic en **Apply (Aplicar)**.
Se configuran las políticas de persistencia.

Configuración de la política de persistencia mediante RACADM

Para configurar la política de persistencia, use el objeto racadm siguiente con el subcomando **set**:

- Para las direcciones virtuales, utilice los objetos **iDRAC.IOIDOpt.VirtualAddressPersistencePolicyAuxPwr** e **iDRAC.IOIDOpt.VirtualAddressPersistencePolicyNonAuxPwr**
- Para el iniciador, utilice el objeto **iDRAC.IOIDOPT.InitiatorPersistencePolicy**
- Para los destinos de almacenamiento, utilice el objeto **iDRAC.IOIDOpt.StorageTargetPersistencePolicy**

Para obtener más información, consulte *iDRAC RACADM Command Line Interface Reference Guide (Guía de referencia de la interfaz de línea de comandos RACADM de iDRAC)* disponible en dell.com/esmanuals.

Valores predeterminados para el destino de almacenamiento y el iniciador iSCSI

En las siguientes tablas se proporciona la lista de valores predeterminados para el iniciador iSCSI y los destinos de almacenamiento cuando se borran las políticas de persistencia.

Tabla 23. Iniciador iSCSI: Valores predeterminados

| Iniciador iSCSI | Valores predeterminados en modo IPv4 | Valores predeterminados en modo IPv6 |
|-----------------------------|--------------------------------------|--------------------------------------|
| IscsilInitiatorIpAddr | 0.0.0.0 | :: |
| IscsilInitiatorIpv4Addr | 0.0.0.0 | 0.0.0.0 |
| IscsilInitiatorIpv6Addr | :: | :: |
| IscsilInitiatorSubnet | 0.0.0.0 | 0.0.0.0 |
| IscsilInitiatorSubnetPrefix | 0 | 0 |
| IscsilInitiatorGateway | 0.0.0.0 | :: |

| Iniciador iSCSI | Valores predeterminados en modo IPv4 | Valores predeterminados en modo IPv6 |
|-------------------------|---|---|
| IscsilniatorIpv4Gateway | 0.0.0.0 | 0.0.0.0 |
| IscsilniatorIpv6Gateway | :: | :: |
| IscsilniatorPrimDns | 0.0.0.0 | :: |
| IscsilniatorIpv4PrimDns | 0.0.0.0 | 0.0.0.0 |
| IscsilniatorIpv6PrimDns | :: | :: |
| IscsilniatorSecDns | 0.0.0.0 | :: |
| IscsilniatorIpv4SecDns | 0.0.0.0 | 0.0.0.0 |
| IscsilniatorIpv6SecDns | :: | :: |
| IscsilniatorName | Valor borrado | Valor borrado |
| IscsilniatorChapId | Valor borrado | Valor borrado |
| IscsilniatorChapPwd | Valor borrado | Valor borrado |
| IPVer | Ipv4 | |

Tabla 24. Atributos de destino de almacenamiento iSCSI: Valores predeterminados

| Atributos de destino de Almacenamiento iSCSI | Valores predeterminados en modo IPv4 | Valores predeterminados en modo IPv6 |
|---|---|---|
| ConnectFirstTgt | Desactivado | Desactivado |
| FirstTgtIpAddress | 0.0.0.0 | :: |
| FirstTgtTcpPort | 3260 | 3260 |
| FirstTgtBootLun | 0 | 0 |
| FirstTgtIscsiName | Valor borrado | Valor borrado |
| FirstTgtChapId | Valor borrado | Valor borrado |
| FirstTgtChapPwd | Valor borrado | Valor borrado |
| FirstTgtIpVer | Ipv4 | |
| ConnectSecondTgt | Desactivado | Desactivado |
| SecondTgtIpAddress | 0.0.0.0 | :: |
| SecondTgtTcpPort | 3260 | 3260 |

| Atributos de destino de Almacenamiento iSCSI | Valores predeterminados en modo IPv4 | Valores predeterminados en modo IPv6 |
|---|---|---|
| SecondTgtBootLun | 0 | 0 |
| SecondTgtIscsiName | Valor borrado | Valor borrado |
| SecondTgtChapId | Valor borrado | Valor borrado |
| SecondTgtChapPwd | Valor borrado | Valor borrado |
| SecondTgtIpVer | Ipv4 | |

Administración de dispositivos de almacenamiento

En la versión 2.00.00.00 de iDRAC, se ha ampliado la administración sin agentes para incluir la configuración directa de las nuevas controladoras PERC9. Se permite configurar de forma remota los componentes de almacenamiento conectados al sistema en el momento de ejecución. Entre estos componentes se incluyen las controladoras RAID y no RAID, los canales, los puertos, los gabinetes y los discos conectados a estos componentes.

Las tareas de descubrimiento, topología, supervisión de la condición y configuración sobre el subsistema de almacenamiento completo se realizan con la estructura de administración incorporada completa (CEM) mediante la interacción en interfaz con las controladoras PERC internas y externas a través de una interfaz de protocolo MCTP sobre I2C. Para realizar la configuración en tiempo real, CEM es compatible con las controladoras PERC9. La versión de firmware para las controladoras PERC9 debe ser 9.1 o posterior.

Con iDRAC, es posible realizar la mayoría de las funciones que se encuentran disponibles en OpenManage Storage Management, lo que incluye los comandos de configuración (sin reinicio) en tiempo real (por ejemplo, la creación de un disco virtual). También se puede configurar completamente RAID antes de instalar el sistema operativo.

Es posible configurar y administrar las funciones de la controladora sin obtener acceso al BIOS. Estas funciones incluyen la configuración de discos virtuales y la aplicación de niveles RAID y repuestos dinámicos para la protección de los datos. Es posible iniciar muchas otras funciones de la controladora, como la recreación y la solución de problemas. Para proteger los datos, se puede configurar la redundancia de datos o asignar repuestos dinámicos.

Los dispositivos de almacenamiento son:

- **Controladoras:** la mayoría de los sistemas operativos no leen ni escriben los datos directamente desde los discos, sino que envían las instrucciones de lectura y escritura a una controladora. La controladora es el hardware de un sistema que interactúa directamente con los discos para escribir y recuperar datos. Cada controladora contiene conectores (canales o puertos) conectados a uno o varios discos físicos o a un gabinete con discos físicos. Las controladoras RAID pueden ampliar los límites de los discos para crear un espacio de almacenamiento extendido (o un disco virtual) donde se use la capacidad de más de un disco. Las controladoras también realizan otras tareas, como el inicio de recreaciones, la inicialización de discos, etc. Para completar sus tareas, las controladoras requieren un software especial, conocido como firmware, y controladores. Para funcionar correctamente, la controladora debe tener instalada la versión mínima requerida para el firmware y los controladores. Las diferentes controladoras presentan distintas características en la manera de leer/escribir datos y ejecutar tareas. Es útil comprender estas características para administrar el almacenamiento de la forma más eficiente posible.
- **Discos físicos o dispositivos físicos:** estos residen dentro de un gabinete o se conectan a la controladora. En una controladora RAID, los discos o los dispositivos físicos se usan para crear discos virtuales.
- **Disco virtual:** es el almacenamiento creado por una controladora RAID a partir de uno o varios discos físicos. Si bien se puede crear un disco virtual a partir de varios discos físicos, el sistema operativo lo

percibirá como un solo disco. Según el nivel RAID usado, el disco virtual puede retener datos redundantes en caso de una falla de disco o tener atributos de rendimiento particulares. Los discos virtuales solo se pueden crear en las controladoras RAID.

- Gabinete: se conecta al sistema de manera externa, mientras que el plano posterior y los discos físicos son internos.
- Plano posterior: es similar a un gabinete. En un plano posterior, el conector de la controladora y los discos físicos se conectan a un gabinete, pero no se pueden usar las funciones de administración (sondas de temperatura, alarmas, etc.) asociadas con los gabinetes externos. Los discos físicos pueden ubicarse en un gabinete o conectarse al plano posterior de un sistema.

Además de administrar los discos físicos en el gabinete, se puede supervisar el estado de los ventiladores, del suministro de energía y de las sondas de temperatura en el gabinete. Es posible realizar un acoplamiento activo de los gabinetes. El acoplamiento activo se define como la adición de un componente a un sistema mientras el sistema operativo aún se encuentra en ejecución.

Los dispositivos físicos conectados a la controladora deben tener el firmware más reciente. Para obtener el firmware compatible más reciente, comuníquese con el proveedor de servicio.

Los sucesos de almacenamiento procedentes de PERC se asignan a capturas SNMP y sucesos WSMAN, según corresponda. Todos los cambios en las configuraciones de almacenamiento se registran en el Registro de Lifecycle.

| Capacidad de PERC | Controladora compatible con configuración CEM (PERC 9.1 o posterior) | Controladora no compatible con configuración CEM (PERC 9.0 y anterior) |
|--------------------------|---|--|
| Real-time (tiempo real) | Si no existen trabajos programados o pendientes para la controladora, se aplica la configuración.
Si existen trabajos programados o pendientes para esa controladora, es necesario borrar los trabajos o esperar que los trabajos se completen antes de aplicar la configuración en el momento de ejecución. La ejecución en el momento o en tiempo real implica que no es necesario reiniciar el sistema. | Se aplicará la configuración. Se mostrará un mensaje de error donde se indicará que la creación de trabajos no se ejecutó correctamente y no se pueden crear trabajos en tiempo real mediante la interfaz web. |
| Organizado en etapas | Si todas las operaciones de configuración se establecen en etapas, la configuración se organiza en etapas y se aplica después de reiniciar el sistema o se aplica en tiempo real. | Se aplicará la configuración después del reinicio. |

Enlaces relacionados

- [Comprensión de los conceptos de RAID](#)
- [Inventario y supervisión de dispositivos de almacenamiento](#)
- [Visualización de la topología de un dispositivo de almacenamiento](#)
- [Administración de controladoras](#)
- [Administración de discos físicos](#)
- [Administración de gabinetes o planos posteriores](#)


[Administración de SSD PCIe](#)
[Administración de discos virtuales](#)
[Forma de hacer parpadear o dejar de hacer parpadear LED de componentes](#)
[Controladoras admitidas](#)
[Gabinetes admitidos](#)
[Resumen de funciones admitidas para Storage Devices \(Dispositivos de almacenamiento\)](#)

Comprensión de los conceptos de RAID

Storage Management utiliza la tecnología de arreglo redundante de discos independientes (RAID) para proporcionar capacidad a Storage Management. Para entender Storage Management es necesario entender los conceptos de RAID, al igual que algunas similitudes sobre cómo las controladoras RAID y el sistema operativo ven el espacio de disco en el sistema.

¿Qué es RAID?

RAID es una tecnología para administrar la manera en la que los datos se almacenan en los discos físicos que residen en el sistema o que están conectados a él. Un aspecto clave de RAID es la capacidad de organizar los discos físicos en forma de tramos, de modo que la capacidad de almacenamiento combinada de varios discos físicos pueda ser tratada como un solo espacio de disco ampliado. Otro aspecto clave de RAID es la capacidad para mantener datos redundantes que pueden ser usados para restaurar datos en caso de una falla del disco. RAID usa técnicas diferentes, como es el seccionamiento, el reflejado y la paridad, para almacenar y reconstruir los datos. Hay distintos niveles RAID que usan métodos diferentes para almacenar y reconstruir datos. Los niveles RAID tienen características diferentes en cuanto a rendimiento de lectura/escritura, protección de datos y capacidad de almacenamiento. No todos los niveles RAID mantienen datos redundantes, lo que significa que, para algunos niveles RAID, los datos perdidos no pueden ser restaurados. La elección de un nivel RAID depende de si la prioridad es el rendimiento, la protección o la capacidad de almacenamiento.

 **NOTA:** El Consejo consultivo de RAID (RAB) define las especificaciones que se utilizan para poner en práctica la tecnología RAID. Aunque el RAB define los niveles RAID, la implementación comercial de los niveles RAID de distintos proveedores puede variar con respecto a las especificaciones de RAID reales. La implementación que utiliza un proveedor en particular puede afectar el rendimiento de lectura y escritura, así como el grado de redundancia de los datos.

RAID por hardware y software

RAID puede implementarse mediante hardware o software. Un sistema que usa RAID por hardware tiene una controladora RAID que implementa los niveles RAID y procesa la lectura y escritura de los datos en los discos físicos. Cuando se usa el software de RAID que proporciona el sistema operativo, el sistema operativo implementa los niveles RAID. Por esta razón, la utilización del RAID de software por sí mismo puede reducir el rendimiento del sistema. Sin embargo, puede usar RAID por software junto con volúmenes RAID por hardware para proporcionar mejor rendimiento y variedad en la configuración de volúmenes RAID. Por ejemplo, puede reflejar un par de volúmenes RAID 5 por hardware entre dos controladoras RAID a fin de proporcionar redundancia de la controladora RAID.

Conceptos de RAID

RAID usa técnicas particulares para escribir datos en los discos. Estas técnicas permiten que RAID proporcione una redundancia de datos o un mejor rendimiento. Estas técnicas incluyen:

- Reflejado: duplicación de datos de un disco físico en otro disco físico. El reflejado proporciona redundancia de datos al mantener dos copias de los mismos datos en discos físicos distintos. Si uno

de los discos en el reflejo falla, el sistema puede continuar funcionando si utiliza el disco que no está afectado. En todo momento, ambos lados del reflejo contienen los mismos datos. Cualquier lado del reflejo puede actuar como el lado operativo. El grupo de discos RAID reflejado es comparable en rendimiento al grupo de discos RAID 5 con respecto a las operaciones de lectura, pero es más rápido en las operaciones de escritura.

- **Seccionamiento:** el seccionamiento de discos escribe datos a lo largo de todos los discos físicos en un disco virtual. Cada sección consiste en direcciones consecutivas de datos en discos virtuales que están asignados en unidades de tamaño fijo a cada disco físico en el disco virtual utilizando un patrón secuencial. Por ejemplo, si el disco virtual incluye cinco discos físicos, la sección escribe datos en los discos físicos uno al cinco sin repetir ninguno de los discos físicos. La cantidad de espacio ocupada por una sección es la misma en todos los discos físicos. La porción de una sección que reside en un disco físico es un elemento de la sección. El seccionamiento por sí mismo no proporciona redundancia de los datos. El seccionamiento en combinación con la paridad realmente proporciona redundancia de los datos.
- **Tamaño de la sección:** espacio total de disco consumido por una sección, sin incluir un disco de paridad. Por ejemplo, considere una sección que contiene 64 KB de espacio en el disco y que tiene 16 KB de datos que residen en cada disco en la sección. En este caso, el tamaño de la sección es de 64 KB y el tamaño del elemento de la sección es de 16 KB.
- **Elemento de la sección:** un elemento de la sección es la porción de una sección que reside en un solo disco físico.
- **Tamaño del elemento de la sección:** cantidad de espacio del disco consumida por un elemento de la sección. Por ejemplo, considere una sección que contiene 64 KB de espacio en el disco y que tiene 16 KB de datos que residen en cada disco en la sección. En este caso, el tamaño del elemento de la sección es de 16 KB y el tamaño de la sección es de 64 KB.
- **Paridad:** la paridad se refiere a los datos redundantes que se mantienen utilizando un algoritmo en combinación con el seccionamiento. Cuando uno de los discos seccionados falla, los datos se pueden reconstruir a partir de la información de paridad que el algoritmo utiliza.
- **Tramo:** un tramo es una técnica de RAID que se utiliza para combinar espacio de almacenamiento de grupos de discos físicos en un disco virtual RAID 10, 50 o 60.

Niveles de RAID

Cada nivel RAID usa alguna combinación de reflejado, seccionamiento y paridad para proporcionar una redundancia de datos o un mejor rendimiento de lectura y escritura. Para obtener información específica sobre cada nivel RAID, consulte [Elección de niveles RAID](#).

Organización del almacenamiento de datos para obtener disponibilidad y rendimiento

RAID proporciona distintos métodos o niveles RAID para organizar el almacenamiento de disco. Algunos niveles RAID mantienen datos redundantes para que usted pueda restaurar los datos después de una falla del disco. Los distintos niveles RAID pueden implicar también un aumento o disminución en el rendimiento de E/S (lectura y escritura) del sistema.

El mantenimiento de datos redundantes requiere el uso de discos físicos adicionales. Entre más discos se vean involucrados, aumenta la probabilidad de una falla de disco. A causa de las diferencias en la redundancia y en el rendimiento de E/S, un nivel RAID puede ser más apropiado que otro, según las aplicaciones que se utilicen en el entorno operativo y la naturaleza de los datos que se almacenen.

Al elegir un nivel RAID, se aplican las siguientes consideraciones de rendimiento y costos:

- **Disponibilidad o tolerancia a fallas:** la disponibilidad o tolerancia a fallas se refiere a la capacidad que el sistema tiene para mantener las operaciones y proporcionar acceso a los datos aun cuando alguno de sus componentes haya fallado. En los volúmenes de RAID, la disponibilidad o tolerancia a fallas se consigue manteniendo datos redundantes. Los datos redundantes incluyen reflejos (datos duplicados) e información de paridad (reconstrucción de los datos mediante un algoritmo).

- Rendimiento: el rendimiento de lectura y escritura puede aumentar o disminuir según el nivel RAID que elija. Algunos niveles RAID pueden ser más apropiados para ciertas aplicaciones.
- Optimización del costo: el mantenimiento de datos redundantes o de información de paridad en relación con volúmenes de RAID requiere de espacio de disco adicional. En situaciones en las que los datos son temporales, de fácil reproducción o no esenciales, es posible que no se justifique el aumento en el costo de la redundancia de datos.
- Tiempo promedio entre fallas (MTBF): el uso de discos adicionales para mantener la redundancia de los datos también aumenta la probabilidad de sufrir fallas de disco en un momento determinado. Aunque esto no se puede evitar en situaciones en las que los datos redundantes son una necesidad, realmente puede repercutir en la carga de trabajo del personal de asistencia de sistemas de la organización.
- Volumen: el volumen se refiere a un solo disco virtual no RAID. Puede crear volúmenes por medio de utilidades externas como la O-ROM <Ctrl+R>. Storage Management no admite la creación de volúmenes. Sin embargo, puede ver volúmenes y usar unidades de estos volúmenes para crear nuevos discos virtuales o para Expansión de capacidad en línea (OCE) de los discos virtuales existentes, siempre que tenga espacio libre disponible. Storage Management permite las operaciones de cambio de nombre y eliminación de estos volúmenes.

Elección de niveles RAID

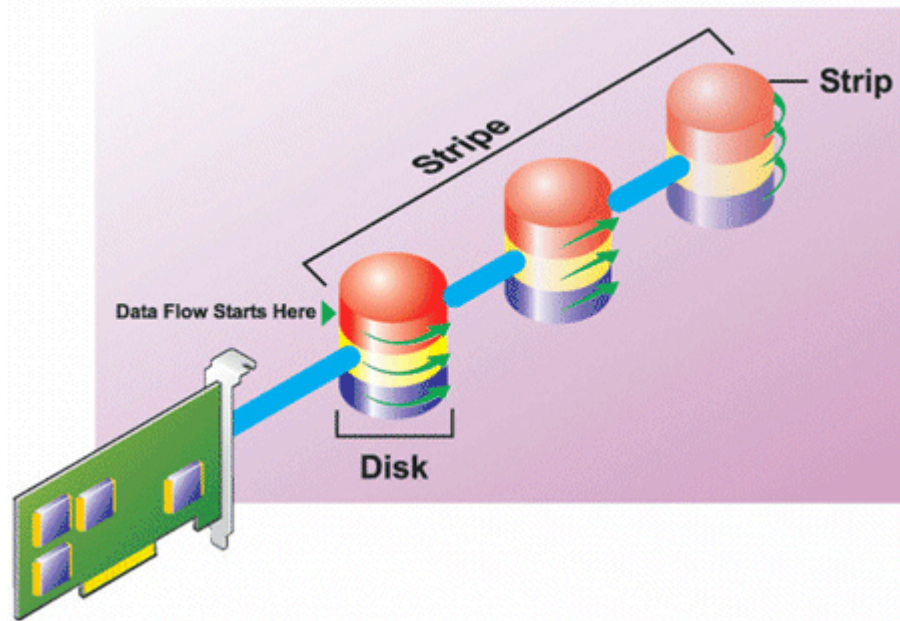
Se puede usar RAID para controlar el almacenamiento de datos en varios discos. Cada nivel RAID o concatenación presenta distintos rendimientos y características para la protección de los datos.

En los temas siguientes se proporciona información específica acerca de la forma en la que cada nivel RAID almacena los datos, así como sus características de protección y rendimiento:

- [Nivel RAID 0 \(seccionamiento\)](#)
- [Nivel RAID 1 \(reflejado\)](#)
- [Nivel RAID 5 \(seccionamiento con paridad distribuida\)](#)
- [Nivel RAID 6 \(seccionamiento con paridad distribuida adicional\)](#)
- [Nivel RAID 50 \(seccionamiento en conjuntos de RAID 5\)](#)
- [Nivel RAID 60 \(seccionamiento en conjuntos de RAID 6\)](#)
- [Nivel RAID 10 \(seccionamiento de conjuntos reflejados\)](#)

Nivel RAID 0 (seccionamiento)

RAID 0 utiliza el seccionamiento de datos, que consisten en escribir los datos en segmentos del mismo tamaño entre los discos físicos. RAID 0 no proporciona redundancia de datos.

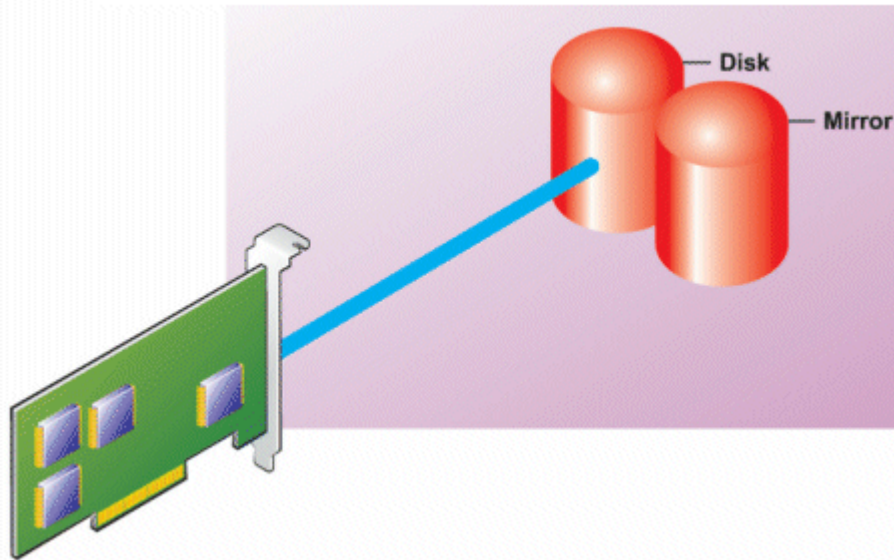


Características de RAID 0:

- Agrupa n discos en un disco virtual grande con una capacidad total de (tamaño de disco más pequeño)* n discos.
- Los datos se guardan en los discos alternadamente.
- No se almacena la redundancia de los datos. Cuando un disco falla, el disco virtual grande fallará sin que haya alguna manera de recrear los datos.
- Mejor rendimiento de lectura y escritura.

Nivel RAID 1 (reflejado)

RAID 1 es la forma más simple de mantener datos redundantes. En RAID 1, los datos se reflejan o duplican en uno o más discos físicos. Si un disco físico falla, los datos pueden recrearse con los mismos datos del otro lado del reflejo.

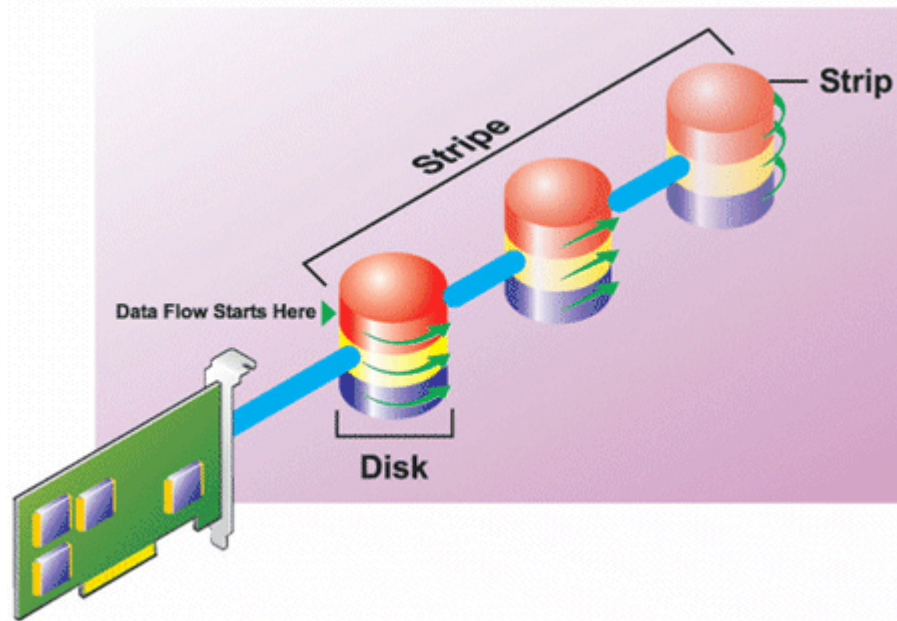


Características de RAID 1:

- Agrupa $n + n$ discos para formar un disco virtual con capacidad de n discos. Las controladoras que actualmente admite Storage Management permiten seleccionar dos discos cuando se crea un RAID 1. Como estos discos se reflejan, la capacidad total de almacenamiento equivale a un disco.
- Los datos se copian en ambos discos.
- Cuando un disco falla, el disco virtual aún funciona. Los datos se leen del reflejo del disco fallido.
- Mejor rendimiento de lectura, pero un rendimiento de escritura ligeramente menor.
- Hay redundancia para la protección de datos.
- RAID 1 es más costoso en términos de espacio de disco, ya que se utiliza el doble de discos de lo que se requiere para almacenar los datos sin redundancia.

Nivel RAID 5 (seccionamiento con paridad distribuida)

RAID 5 proporciona redundancia de los datos al utilizar el seccionamiento de datos en combinación con la información de paridad. Sin embargo, en vez de dedicar un disco físico a la paridad, la información de paridad está seccionada entre todos los discos físicos en el grupo de discos.

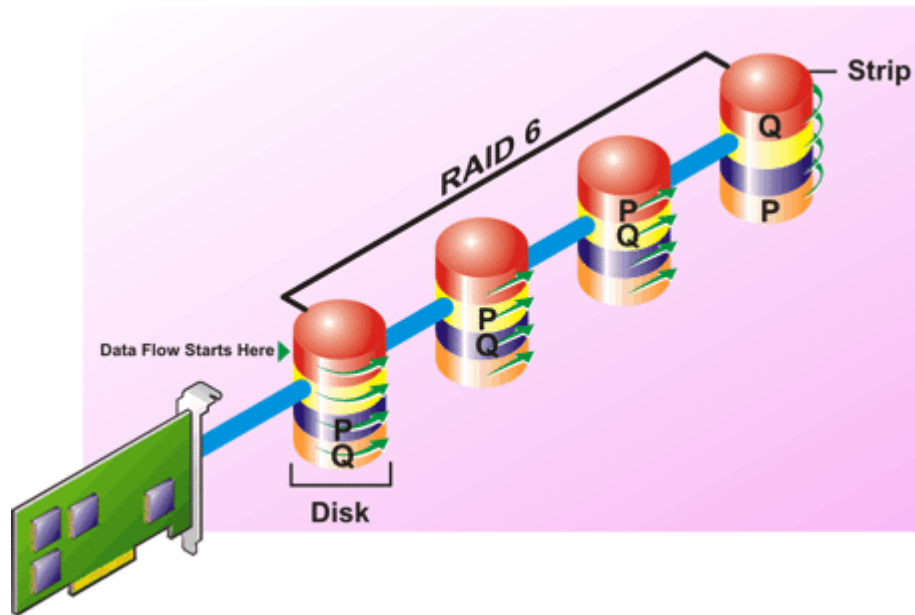


Características de RAID 5:

- Agrupa n discos en un disco virtual grande con capacidad de $(n-1)$ discos.
- La información redundante (paridad) se almacena alternadamente entre todos los discos.
- Cuando un disco falla, el disco virtual seguirá funcionando, pero funcionará en estado degradado. Los datos se reconstruyen a partir de los discos que sobrevivan.
- Mejor rendimiento de lectura, pero un rendimiento de escritura más lento.
- Hay redundancia para la protección de datos.

Nivel RAID 6 (seccionamiento con paridad distribuida adicional)

RAID 6 proporciona redundancia de los datos al utilizar el seccionamiento de datos en combinación con la información de paridad. Al igual que en RAID 5, la paridad se distribuye dentro de cada sección. Sin embargo, RAID 6 utiliza un disco físico adicional para mantener la paridad, de manera que cada sección en el grupo de discos mantiene dos bloques de disco con información de paridad. La paridad adicional proporciona protección de datos en caso de que se presenten dos fallas de disco. En la siguiente imagen, los dos conjuntos de información de paridad se identifican como **P** y **Q**.



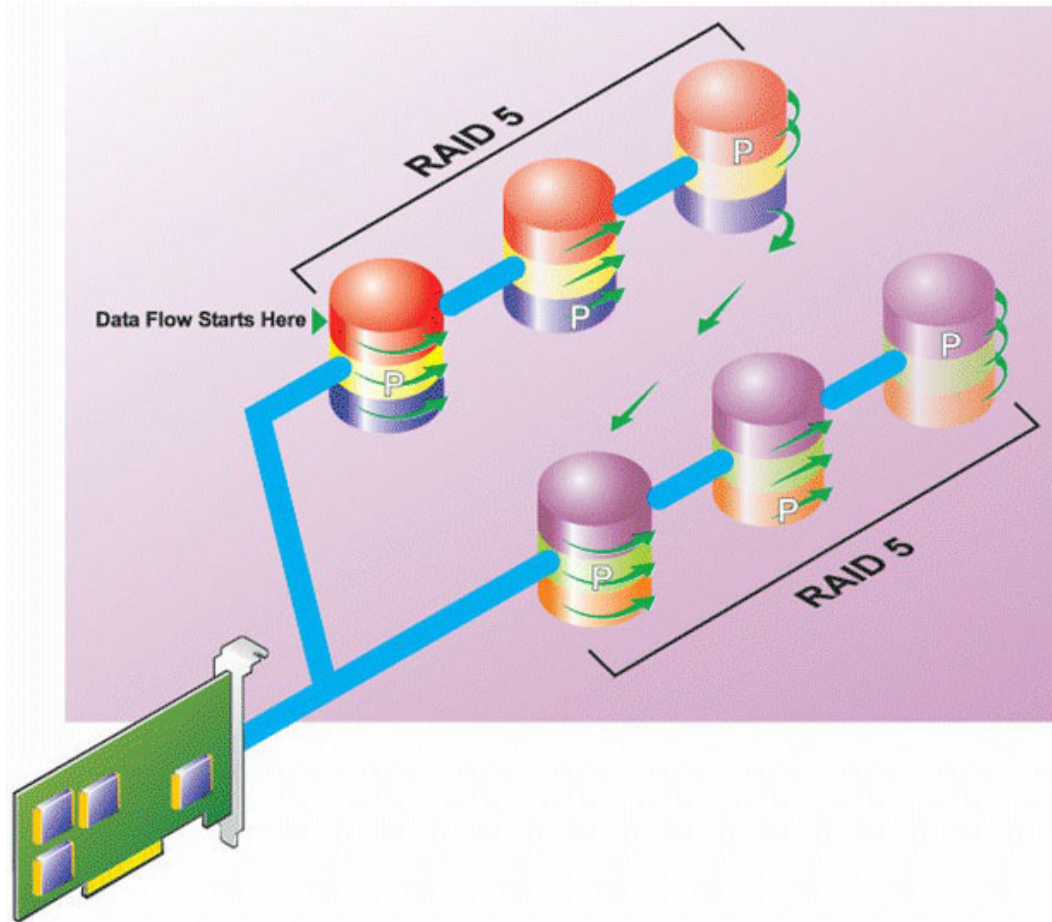
Características de RAID 6:

- Agrupa n discos en un disco virtual grande con capacidad de $(n-2)$ discos.
- La información redundante (paridad) se almacena alternadamente entre todos los discos.
- El disco virtual se mantiene funcionando con hasta dos fallas de disco. Los datos se reconstruyen a partir de los discos que sobrevivan.
- Mejor rendimiento de lectura, pero un rendimiento de escritura más lento.
- Mayor redundancia para la protección de datos.
- Se requieren dos discos por tramo para la paridad. RAID 6 es más costoso en términos de espacio de disco.

Nivel RAID 50 (seccionamiento en conjuntos de RAID 5)

RAID 50 es el seccionamiento en más de un tramo de discos físicos. Por ejemplo, un grupo de discos RAID 5 que esté implementado con tres discos físicos y, luego, continúe con un grupo de tres discos físicos adicionales sería un RAID 50.

Es posible implementar RAID 50 aun si el hardware no lo admita directamente. En este caso, puede establecer varios discos virtuales de RAID 5 y, luego, convertir los discos de RAID 5 en discos dinámicos. A partir de ahí, puede crear un volumen dinámico que se extienda a todos los discos virtuales de RAID 5.

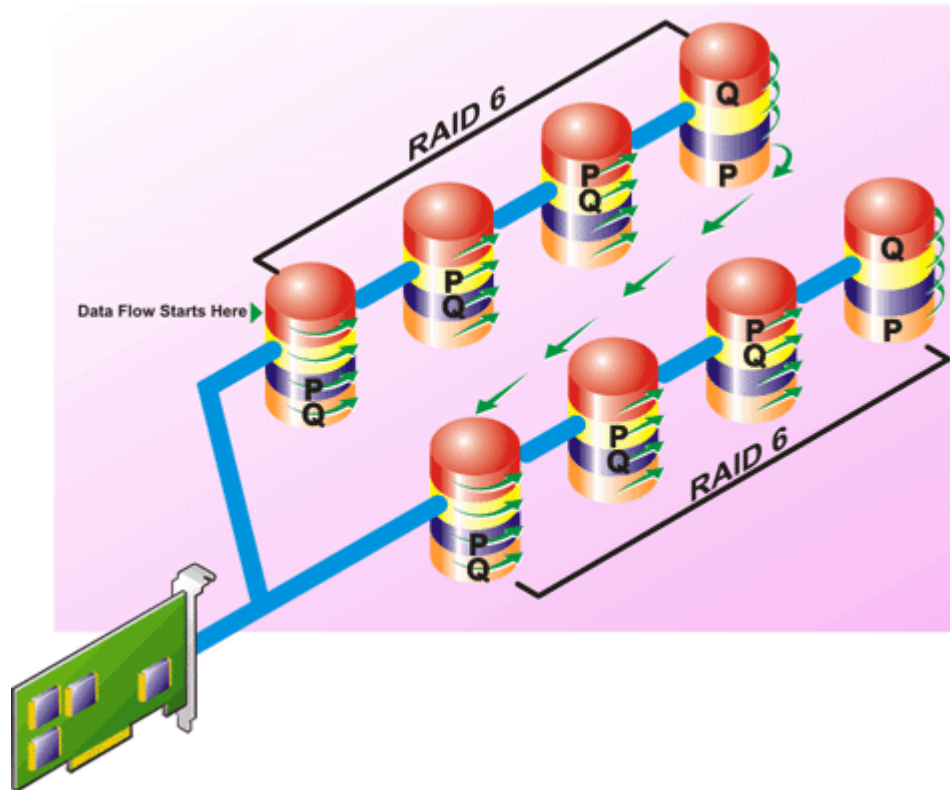


Características de RAID 50:

- Agrupa $n*s$ discos para formar un disco virtual grande con capacidad de $s*(n-1)$ discos, en donde s representa el número de tramos y n es el número de discos dentro de cada tramo.
- La información redundante (paridad) se almacena alternadamente en todos los discos de cada tramo de RAID 5.
- Mejor rendimiento de lectura, pero un rendimiento de escritura más lento.
- Se requiere tanta información de paridad como en RAID 5 convencional.
- Los datos se seccionan a lo largo de todos los tramos. RAID 50 es más costoso en términos de espacio de disco.

Nivel RAID 60 (seccionamiento en conjuntos de RAID 6)

RAID 60 se secciona en más de un tramo de discos físicos configurados como un RAID 6. Por ejemplo, un grupo de discos RAID 6 implementado con cuatro discos físicos que luego continúa con un grupo de discos de cuatro discos físicos más sería un RAID 60.

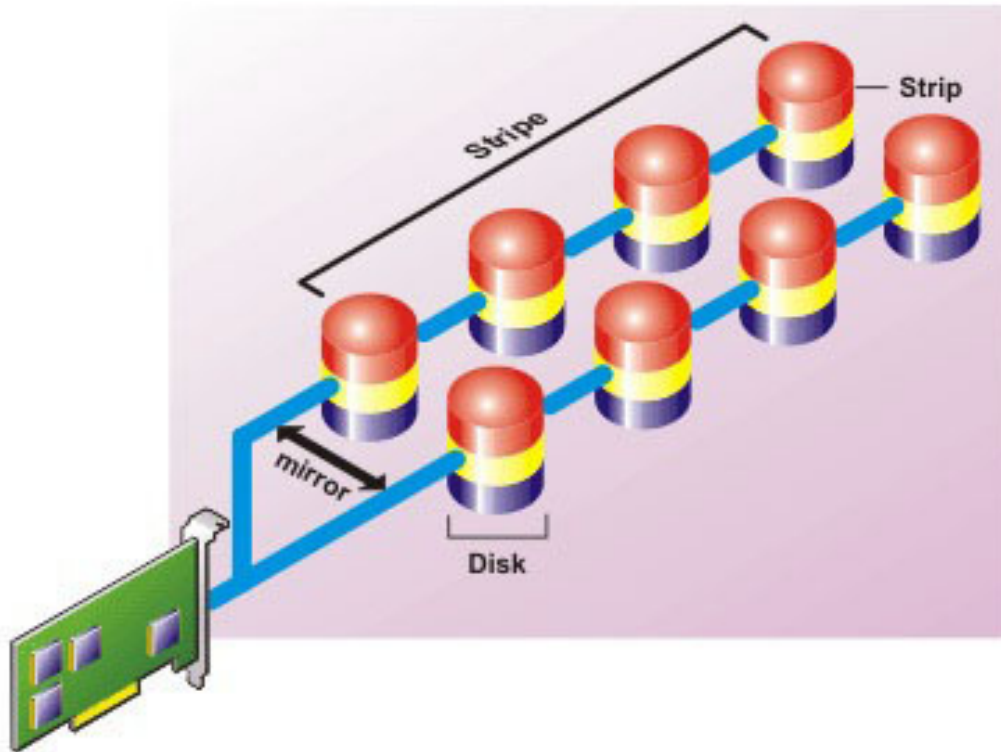


Características de RAID 60:

- Agrupa $n*s$ discos para formar un disco virtual grande con capacidad de $s*(n-2)$ discos, en donde s representa el número de tramos y n es el número de discos dentro de cada tramo.
- La información redundante (paridad) se almacena alternadamente en todos los discos de cada tramo de RAID 6.
- Mejor rendimiento de lectura, pero un rendimiento de escritura más lento.
- La redundancia aumentada proporciona mayor protección de datos que un RAID 50.
- Proporcionalmente, requiere de tanta información de paridad como el RAID 6.
- Se requieren dos discos por tramo para la paridad. RAID 60 es más costoso en términos de espacio de disco.

Nivel RAID 10 (reflejos seccionados)

RAB considera que el nivel RAID 10 es una implementación del nivel RAID 1. RAID 10 combina los discos físicos reflejados (RAID 1) con el seccionamiento de datos (RAID 0). Con RAID 10, los datos se seccionan entre varios discos físicos. Después, el grupo de discos seccionados se refleja en otro conjunto de discos físicos. RAID 10 se puede considerar un *reflejo de secciones*.



Características de RAID 10:

- Agrupa n discos en un disco virtual grande con una capacidad total de $(n/2)$ discos, en donde n es un número entero par.
- Las imágenes de reflejo de los datos son seccionadas entre conjuntos de discos físicos. Este nivel proporciona redundancia por medio del reflejado.
- Cuando un disco falla, el disco virtual aún funciona. Los datos se leen del disco reflejado que sigue funcionando.
- Rendimiento de lectura mejorado y rendimiento de escritura.
- Hay redundancia para la protección de datos.

Comparación de rendimiento de niveles RAID

La tabla siguiente compara las características de rendimiento asociadas con los niveles RAID más comunes. Esta tabla proporciona las pautas generales para elegir un nivel RAID. Evalúe los requisitos específicos de su entorno antes de elegir un nivel RAID.

Tabla 25. Comparación de rendimiento de los niveles RAID

| Nivel de RAID | Disponibilidad de datos | Rendimiento de lectura | Rendimiento de escritura | Rendimiento de recreación | Discos mínimos requeridos | Usos sugeridos |
|---------------|-------------------------|------------------------|--------------------------|---------------------------|---------------------------|--------------------|
| RAID 0 | Ninguno | Muy bueno | Muy bueno | N/A | N | Datos no críticos. |
| RAID 1 | Excelente | Muy bueno | En buen estado | En buen estado | 2N (N = 1) | Pequeñas bases de |

| Nivel de RAID | Disponibilidad de datos | Rendimiento de lectura | Rendimiento de escritura | Rendimiento de recreación | Discos mínimos requeridos | Usos sugeridos |
|---------------|-------------------------|---|--|---------------------------|--|--|
| | | | | | | datos, registros de base de datos, información crítica. |
| RAID 5 | En buen estado | Lecturas secuenciales : Bueno.
Lecturas transaccionales: Muy bueno | Aceptable, a menos que se utilice la escritura no simultánea de la memoria caché | Aceptable | $N + 1$ ($N =$ por lo menos dos discos) | Bases de datos y otros usos transaccionales de lecturas intensivas. |
| RAID 10 | Excelente | Muy bueno | Aceptable | En buen estado | $2N \times X$ | Entornos con intensidad de datos (registros grandes). |
| RAID 50 | En buen estado | Muy bueno | Aceptable | Aceptable | $N + 2$ ($N =$ por lo menos 4) | Usos transaccionales de tamaño medio o usos con intensidad de datos. |
| RAID 6 | Excelente | Lecturas secuenciales : Bueno.
Lecturas transaccionales: Muy bueno | Aceptable, a menos que se utilice la escritura no simultánea de la memoria caché | Pobre | $N + 2$ ($N =$ por lo menos dos discos) | Información crítica. Bases de datos y otros usos transaccionales de lecturas intensivas. |
| RAID 60 | Excelente | Muy bueno | Aceptable | Pobre | $X \times (N + 2)$ ($N =$ por lo menos 2) | Información crítica. Usos transaccionales de tamaño medio o usos con |

| Nivel de RAID | Disponibilidad de datos | Rendimiento de lectura | Rendimiento de escritura | Rendimiento de recreación | Discos mínimos requeridos | Usos sugeridos |
|---|-------------------------|------------------------|--------------------------|---------------------------|---------------------------|----------------------|
| | | | | | | intensidad de datos. |
| <p>N = cantidad de discos físicos</p> <p>X = cantidad de conjuntos RAID</p> | | | | | | |

Controladoras admitidas

Controladoras RAID admitidas

Las interfaces de iDRAC son compatibles con las siguientes controladoras PERC9:


- PERC H830
- PERC H730P
- PERC H730
- PERC H330

Las interfaces de iDRAC son compatibles con las siguientes controladoras PERC8:

- PERC H810
- PERC H710P
- PERC H710
- PERC H310

Controladoras no RAID admitidas

Las interfaces de iDRAC son compatibles con los adaptadores externos HBA SAS de 12 Gbps.

 **NOTA:** iDRAC no es compatible con RAID de software. Para obtener más información sobre el RAID de software, consulte *Lifecycle Controller GUI User's Guide (Guía del usuario de la interfaz gráfica de usuario de Lifecycle Controller)* disponible en dell.com/support/manuals.

Gabinetes admitidos

iDRAC es compatible con gabinetes MD1400 y MD1420.

Resumen de funciones admitidas para Storage Devices (Dispositivos de almacenamiento)

La siguiente tabla proporciona las funciones admitidas por los dispositivos de almacenamiento a través de iDRAC.

| Nombre de la función | Controladoras PERC 9 | | | | Controladoras PERC 8 | | | | SSD PCIe |
|---|-----------------------|-----------------------|-----------------------|-----------------------|-------------------------------|-------------------------------|-------------------------------|----------------------------|--------------|
| | H830 | H730 P | H730 | H330 | H810 | H710P | H710 | H310 | |
| Asignar o desasignar un disco físico como un repuesto dinámico global | Real-time | Real-time | Real-time | Real-time | Organizado en etapas | Organizado en etapas | Organizado en etapas | Organizado en etapas | No aplicable |
| Crear discos virtuales | Real-time | Real-time | Real-time | Real-time | Organizado en etapas | Organizado en etapas | Organizado en etapas | Organizado en etapas | No aplicable |
| Editar las políticas caché de los discos virtuales | Real-time | Real-time | Real-time | Real-time | Organizado en etapas | Organizado en etapas | Organizado en etapas | Organizado en etapas | No aplicable |
| Comprobar coherencia del disco virtual | Real-time | Real-time | Real-time | Real-time | Organizado en etapas | Organizado en etapas | Organizado en etapas | Organizado en etapas | No aplicable |
| Cancelar revisión de congruencia | Real-time | Real-time | Real-time | Real-time | No aplicable | No aplicable | No aplicable | No aplicable | No aplicable |
| Inicialización de discos virtuales | Real-time | Real-time | Real-time | Real-time | Organizado en etapas | Organizado en etapas | Organizado en etapas | Organizado en etapas | No aplicable |
| Cancelar inicialización | Real-time | Real-time | Real-time | Real-time | No aplicable | No aplicable | No aplicable | No aplicable | No aplicable |
| Cifrar discos virtuales | Real-time | Real-time | Real-time | Real-time | Organizado en etapas | Organizado en etapas | Organizado en etapas | Organizado en etapas | No aplicable |
| Asignar o desasignar un repuesto dinámico dedicado | Real-time | Real-time | Real-time | Real-time | Organizado en etapas | Organizado en etapas | Organizado en etapas | Organizado en etapas | No aplicable |
| Eliminar discos virtuales | Real-time | Real-time | Real-time | Real-time | Organizado en etapas | Organizado en etapas | Organizado en etapas | Organizado en etapas | No aplicable |
| Establecer modo de lectura de patrullaje | Real-time | Real-time | Real-time | Real-time | Organizado en etapas | Organizado en etapas | Organizado en etapas | Organizado en etapas | No aplicable |
| Áreas de lectura de patrullaje no configuradas | Real-time (solo en la | Real-time (solo en la | Real-time (solo en la | Real-time (solo en la | Organizado en etapas (solo en | Organizado en etapas (solo en | Organizado en etapas (solo en | Organizado en etapas (solo | No aplicable |

| Nombre de la función | Controladoras PERC 9 | | | | Controladoras PERC 8 | | | | SSD PCIe |
|---|----------------------|------------------|------------------|------------------|----------------------|----------------------|----------------------|------------------------|--------------|
| | H830 | H730 P | H730 | H330 | H810 | H710P | H710 | H310 | |
| | interfaz de web) | interfaz de web) | interfaz de web) | interfaz de web) | la interfaz de web) | la interfaz de web) | la interfaz de web) | en la interfaz de web) | |
| Modo de revisión de congruencia | Real-time | Real-time | Real-time | Real-time | Organizado en etapas | Organizado en etapas | Organizado en etapas | Organizado en etapas | No aplicable |
| Modo de escritura diferida | Real-time | Real-time | Real-time | Real-time | Organizado en etapas | Organizado en etapas | Organizado en etapas | Organizado en etapas | No aplicable |
| Modo de equilibrio de carga | Real-time | Real-time | Real-time | Real-time | Organizado en etapas | Organizado en etapas | Organizado en etapas | Organizado en etapas | No aplicable |
| Porcentaje de revisión de congruencia | Real-time | Real-time | Real-time | Real-time | Organizado en etapas | Organizado en etapas | Organizado en etapas | Organizado en etapas | No aplicable |
| Porcentaje de recreación | Real-time | Real-time | Real-time | Real-time | Organizado en etapas | Organizado en etapas | Organizado en etapas | Organizado en etapas | No aplicable |
| Porcentaje de inicialización de segundo plano | Real-time | Real-time | Real-time | Real-time | Organizado en etapas | Organizado en etapas | Organizado en etapas | Organizado en etapas | No aplicable |
| Porcentaje de reconstrucción | Real-time | Real-time | Real-time | Real-time | Organizado en etapas | Organizado en etapas | Organizado en etapas | Organizado en etapas | No aplicable |
| Importar configuración ajena | Real-time | Real-time | Real-time | Real-time | Organizado en etapas | Organizado en etapas | Organizado en etapas | Organizado en etapas | No aplicable |
| Importar configuración ajena automáticamente | Real-time | Real-time | Real-time | Real-time | Organizado en etapas | Organizado en etapas | Organizado en etapas | Organizado en etapas | No aplicable |
| Borrar configuración ajena | Real-time | Real-time | Real-time | Real-time | Organizado en etapas | Organizado en etapas | Organizado en etapas | Organizado en etapas | No aplicable |
| Restablecer configuración de la controladora | Real-time | Real-time | Real-time | Real-time | Organizado en etapas | Organizado en etapas | Organizado en etapas | Organizado en etapas | No aplicable |

| Nombre de la función | Controladoras PERC 9 | | | | Controladoras PERC 8 | | | | SSD PCIe |
|---|----------------------|--------------|--------------|--------------|----------------------|----------------------|----------------------|----------------------|----------------------|
| | H830 | H730 P | H730 | H330 | H810 | H710P | H710 | H310 | |
| Crear o cambiar claves de seguridad | Real-time | Real-time | Real-time | Real-time | Organizado en etapas | Organizado en etapas | Organizado en etapas | Organizado en etapas | No aplicable |
| Inventario y supervisar de forma remota la condición de los dispositivos SSD PCIe | No aplicable | No aplicable | No aplicable | No aplicable | No aplicable | No aplicable | No aplicable | No aplicable | Real-time |
| Preparar el SSD PCIe se quitó | No aplicable | No aplicable | No aplicable | No aplicable | No aplicable | No aplicable | No aplicable | No aplicable | Real-time |
| Borrar los datos de manera segura | No aplicable | No aplicable | No aplicable | No aplicable | No aplicable | No aplicable | No aplicable | No aplicable | Organizado en etapas |
| Configure el modo de plano posterior | Real-time | Real-time | Real-time | Real-time | No aplicable | No aplicable | No aplicable | No aplicable | No aplicable |
| Hacer parpadear o dejar de hacer parpadear LED de los componentes | Real-time | Real-time | Real-time | Real-time | Real-time | Real-time | Real-time | Real-time | Real-time |

Inventario y supervisión de dispositivos de almacenamiento

Es posible supervisar de manera remota la condición y ver el inventario de los siguientes dispositivos de almacenamiento con capacidad CEM (administración incorporada completa) en el sistema administrador mediante la interfaz web de iDRAC:

- Controladoras RAID, controladoras no RAID y extensores de PCIe
- Gabinetes que incluyen módulos de administración de gabinetes (EMM), suministros de energía, sonda de ventilador y sonda de temperatura
- Discos físicos
- Discos virtuales
- Baterías

No obstante, RACADM y WS-MAN muestran información para la mayoría de los dispositivos de almacenamiento en el sistema.

iDRAC calcula el inventario y supervisa las controladoras RAID de la serie PERC 8 que incluyen H310, H710, H710P y H810. Las controladoras que no admiten CEM son adaptadores de cinta internos (ITA), SAS 6 Gbps HBA y SAS 12 Gbps HBA.

También se muestran los sucesos de almacenamiento recientes y la topología de los dispositivos de almacenamiento.

Para los sucesos de almacenamiento se generan alertas y capturas SNMP y los sucesos se registran en el registro de Lifecycle.

Supervisión de dispositivos de almacenamiento mediante la interfaz web

Para ver la información del dispositivo de almacenamiento mediante la interfaz web:

- Vaya a **Descripción general** → **Almacenamiento** → **Resumen** para ver el resumen de los componentes de almacenamiento y los sucesos registrados recientemente. Esta página se actualiza automáticamente cada 30 segundos.
- Vaya a **Descripción general** → **Almacenamiento** → **Topología** para ver la vista de contención física jerárquica de los componentes de almacenamiento clave.
- Vaya a **Descripción general** → **Almacenamiento** → **Discos físicos** → **Propiedades** para ver la información de un disco físico. Se mostrará la página **Propiedades de discos físicos**.
- Vaya a **Descripción general** → **Almacenamiento** → **Discos virtuales** → **Propiedades** para ver la información de los discos virtuales. Se mostrará la página **Propiedades de discos virtuales**.
- Vaya a **Descripción general** → **Almacenamiento** → **Controladoras** → **Propiedades** para ver la información de la controladora RAID. Se mostrará la página **Propiedades de las controladoras**.
- Vaya a **Descripción general** → **Almacenamiento** → **Gabinetes** → **Propiedades** para ver información sobre el gabinete. Se mostrará la página **Propiedades de gabinete**.

También puede utilizar filtros para ver información de un dispositivo específico.

Para obtener más información acerca de las propiedades mostradas y el uso de las opciones de filtro, consulte la *Ayuda en línea de iDRAC*.

Supervisión de dispositivos de almacenamiento mediante RACADM

Para ver la información de un dispositivo de almacenamiento, utilice el subcomando **raid** o **storage**. Para obtener más información, consulte *iDRAC RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de iDRAC)* disponible en dell.com/support/manuals.

Supervisión de plano posterior mediante la utilidad de configuración de iDRAC

En la utilidad de configuración de iDRAC, vaya a **Resumen del sistema**. Se mostrará la página **Configuración de iDRAC. Resumen del sistema**. En la sección **Inventario de plano posterior** se muestra información sobre el plano posterior. Para obtener información sobre los campos, consulte la *Ayuda en línea de la utilidad de configuración de iDRAC*.

Visualización de la topología de un dispositivo de almacenamiento

Es posible consultar la vista jerárquica de contención física de los componentes de almacenamiento clave, es decir, una lista de las controladoras, los gabinetes conectados a la controladora y un vínculo al disco físico que contiene cada gabinete. También se muestran los discos físicos conectados directamente a la controladora.

Para ver la topología de los dispositivos de almacenamiento, vaya a **Descripción general** → **Almacenamiento** → **Topología**. En la página **Topología** se muestra la representación jerárquica de los componentes de almacenamiento en el sistema.

Haga clic en los vínculos para ver los detalles correspondientes a cada componente.

Administración de discos físicos

Es posible realizar las siguientes tareas para los discos físicos:

- Ver propiedades del disco físico
- Asignar o desasignar un disco físico como repuesto dinámico global
- Convertir a disco con capacidad RAID (solamente se admite en RACADM y es una operación organizada en etapas)
- Convertir a disco no RAID (solamente se admite en RACADM y es una operación organizada en etapas)
- Hacer parpadear o dejar de hacer parpadear LED

Enlaces relacionados

[Inventario y supervisión de dispositivos de almacenamiento](#)

[Asignación o desasignación de un disco físico como repuesto dinámico global](#)

Asignación o desasignación de un disco físico como repuesto dinámico global

El repuesto dinámico global es un disco de reserva no utilizado que forma parte del grupo de discos. Los repuestos dinámicos permanecen en el modo de espera. Cuando un disco físico utilizado en un disco virtual falla, el repuesto dinámico asignado se activará con el fin de reemplazar el disco físico fallido sin interrumpir el sistema ni requerir de intervención. Cuando un repuesto dinámico se activa, recrea los datos de todos los discos virtuales redundantes que usaban el disco físico fallido.

Puede cambiar la asignación del repuesto dinámico al desasignar un disco y elegir otro, según sea necesario. También puede asignar más de un disco físico como repuesto dinámico global.

Los repuestos dinámicos globales se deben asignar y desasignar manualmente. Estos no se asignan a discos virtuales específicos. Si desea asignar un repuesto dinámico a un disco virtual (el repuesto reemplaza cualquier disco físico que falle en el disco virtual), consulte [Asignación o desasignación de repuestos dinámicos dedicados](#).

Al eliminar discos virtuales, todos los repuestos dinámicos globales asignados se pueden desasignar automáticamente en el momento en que se elimina el último disco virtual asociado con la controladora.

Si se restablece la configuración, los discos virtuales se borran y todos los repuestos dinámicos se desasignan.

Es necesario estar familiarizado con los requisitos de tamaño y otras consideraciones relacionadas con los repuestos dinámicos.

Antes de asignar un disco físico como un repuesto dinámico global:

- Asegúrese de que Lifecycle Controller se encuentre activado.

- Si no existen unidades de disco disponibles en estado Listo, inserte unidades de disco adicionales y asegúrese de que las unidades se encuentren en estado Listo.
- Si no existen discos virtuales presentes, es necesario crear al menos un disco virtual.
- Si los discos físicos se encuentran en modo no-RAID, conviértalos al modo RAID mediante el comando racadm o <CTRL+R>.

Si ha asignado un disco físico como repuesto dinámico global en el modo Agregar a operaciones pendientes, se crea la operación pendiente pero no se crea un trabajo. Por lo tanto, si intenta desasignar el mismo disco como repuesto dinámico global, la operación pendiente Asignar repuesto dinámico global se borra.

Si ha desasignado un disco físico como repuesto dinámico global en el modo Agregar a operaciones pendientes, se crea la operación pendiente pero no se crea un trabajo. Por lo tanto, si intenta asignar el mismo disco como repuesto dinámico global, la operación pendiente Desasignar repuesto dinámico global se borra.

Asignación o desasignación de un repuesto dinámico global mediante la interfaz web

Para asignar o desasignar un repuesto dinámico global para una unidad de disco físico:

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Almacenamiento** → **Discos físicos** → . Se mostrará la página **Configuración**.
2. En el menú desplegable **Controladora**, seleccione la controladora para ver los discos físicos asociados.
3. Para asignar un repuesto dinámico global, en los menús desplegables de la columna **Acción: Asignar a todos**, seleccione **Repuesto dinámico global** para uno o varios discos físicos.
4. Para desasignar un repuesto dinámico, en los menús desplegables de la columna **Acción: Asignar a todos**, seleccione **Desasignar repuesto dinámico** para uno o varios discos físicos.
5. En el menú desplegable **Aplicar modo de operación**, seleccione el momento en que desea aplicar la configuración.
6. Haga clic en **Apply (Aplicar)**.
Según el modo de operación seleccionado, se aplicará la configuración.

Enlaces relacionados

[Elección del modo de operación mediante la interfaz web](#)

Asignación o desasignación de un repuesto dinámico global mediante RACADM

Utilice el subcomando **storage** y especifique el tipo como repuesto dinámico global. Para obtener más información, consulte *iDRAC RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de iDRAC)* disponible en dell.com/esmanuals.

Enlaces relacionados

[Elección del modo de operación mediante RACADM](#)

Convertir a disco RAID

Esta tarea activa un disco para todas las operaciones RAID:

Si la unidad de disco físico se encuentra en el modo no RAID, es necesario realizar lo siguiente para convertirla a modo RAID:

1. Presione <Ctrl+R> mientras se reinicia el servidor y, a continuación, seleccione la controladora requerida.

2. Presione <F2> y seleccione la opción **Convertir a compatible con RAID**. A continuación, complete la operación.


 **NOTA:**

- Esta tarea no se admite en las controladoras de hardware PERC que se ejecutan en modo **HBA**.
- Esta tarea solo se admite como una operación organizada en etapas.

Convertir a disco no RAID

Esta tarea convierte un disco en un disco no RAID. Después de convertir un disco en no RAID, el disco está expuesto al sistema operativo no como discos no configurados y en buen estado, lo que permite utilizar el disco en modo de paso directo.

Esta tarea se admite en las controladoras H310 y H330.

 **NOTA:** Esta tarea no se admite en las controladoras de hardware PERC que se ejecutan en modo **HBA**.

Administración de discos virtuales

Es posible realizar las siguientes operaciones para los discos virtuales:

- Crear
- Eliminar
- Editar políticas
- Inicializar
- Revisión de congruencia
- Cancelar revisión de congruencia
- Cifrar discos virtuales
- Asignar o desasignar repuestos dinámicos dedicados
- Hacer parpadear y dejar de hacer parpadear discos virtuales

Enlaces relacionados

[Creación de discos virtuales](#)

[Edición de políticas de caché de discos virtuales](#)

[Eliminación de discos virtuales](#)

[Revisión de congruencia en el disco virtual](#)

[Inicialización de discos virtuales](#)

[Cifrado de discos virtuales](#)

[Asignación o desasignación de repuestos dinámicos dedicados](#)

[Administración de discos virtuales mediante la interfaz web](#)

[Administración de discos virtuales mediante RACADM](#)

Creación de discos virtuales


Para implementar las funciones de RAID, se debe crear un disco virtual. El disco virtual hace referencia al almacenamiento creado por una controladora RAID a partir de uno o varios discos físicos. Si bien se puede crear un disco virtual a partir de varios discos físicos, el sistema operativo lo percibirá como un solo disco.

Antes de crear un disco virtual, debe estar familiarizado con la información de Consideraciones antes de crear discos virtuales.

Es posible crear un disco virtual mediante el uso de los discos físicos conectados a la controladora PERC. Para crear un disco virtual, es necesario tener el privilegio de usuario Control del servidor. Es posible crear un máximo de 64 discos virtuales y un máximo de 16 unidades virtuales en el mismo grupo de unidades.

No se puede crear un disco virtual si:

- Las unidades de disco físico no están disponibles para la creación del disco virtual. Instale unidades de disco físico adicionales.
- Se ha alcanzado el número máximo de discos virtuales que se pueden crear en la controladora. Debe eliminar al menos un disco virtual y, a continuación, crear un nuevo disco virtual.
- Se ha creado el número máximo de discos virtuales admitidos por un grupo de unidades. Se debe eliminar un disco virtual del grupo seleccionado y, a continuación, crear un nuevo disco virtual.
- Hay un trabajo en ejecución o programado en la controladora seleccionada. Debe esperar que finalice este trabajo o puede eliminarlo antes de intentar una operación nueva. Puede ver y administrar el estado del trabajo programado en la página Cola de trabajo en espera .
- El disco físico se encuentra en modo no RAID. Es necesario convertirlo al modo RAID mediante el comando racadm o <CTRL+R>.

 **NOTA:** Si se crea un disco virtual en el modo Agregar a operaciones pendientes, pero no se crea un trabajo, cuando se elimina el disco virtual, se borra la operación pendiente Crear para el disco virtual.

Consideraciones antes de crear discos virtuales

Antes de crear discos virtuales, tenga en cuenta lo siguiente:

- Los nombres de los discos virtuales no se almacenan en la controladora: los nombres de los discos virtuales que se crean no se almacenan en la controladora. Esto significa que si se reinicia mediante un sistema operativo distinto, es posible que el nuevo sistema operativo cambie el nombre del disco virtual aplicando sus propias convenciones de nombres.
- La agrupación de discos es una agrupación lógica de discos conectados a una controladora RAID donde se crean uno o varios discos virtuales de manera tal que todos los discos virtuales en el grupo de discos usen todos los discos físicos en el grupo. La implementación actual admite la formación de bloques con grupos de discos mixtos durante la creación de dispositivos lógicos.
- Los discos físicos se unen a grupos de discos. Por lo tanto, los niveles RAID no se mezclan en un grupo de discos.
- Existen limitaciones con respecto a la cantidad de discos físicos que se pueden incluir en el disco virtual. Estas limitaciones dependen de la controladora. Cuando se crea un disco virtual, las controladoras admiten un cierto número de secciones y tramos (métodos para combinar el almacenamiento en los discos físicos). Como el número total de secciones y tramos es limitado, el número de discos físicos que se pueden utilizar también es limitado. Las limitaciones de secciones y tramos afectan los niveles RAID como se indica a continuación:
 - Número máximo de tramos afecta a los niveles RAID 10, RAID 50 y RAID 60.
 - Número máximo de secciones afecta a los niveles RAID 0, RAID 5, RAID 50, RAID 6 y RAID 60.
 - Número de discos físicos en un reflejo es siempre 2. Esto afecta a RAID 1 y RAID 10.
- No se pueden crear discos virtuales en SSD PCIe.

Creación de discos virtuales mediante la interfaz web

Para crear un disco virtual:


1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Almacenamiento** → **Discos virtuales** → **Crear**.
Se mostrará la página **Crear un disco virtual**.
2. En la sección **Configuración**, haga lo siguiente:
 - a. Introduzca el nombre para el disco virtual.
 - b. En el menú desplegable **Controladora**, seleccione la controladora para la que desea crear el disco virtual.
 - c. En el menú desplegable **Diseño**, seleccione el nivel RAID para el disco virtual.
Solo los niveles RAID compatibles con la controladora se muestran en el menú desplegable y esto se basa en los niveles RAID disponibles según el número total de discos físicos disponibles.
 - d. Seleccione **Tipo de medios**, **Tamaño de la sección**, **Política de lectura**, **Política de escritura**, **Política de caché de disco** y **Capacidad PI T10**.
Solo los valores compatibles con la controladora se muestran en los menús desplegables para estas propiedades.
 - e. En el campo **Capacidad**, especifique el tamaño del disco virtual.
El tamaño máximo se muestra y se actualiza a medida que se seleccionan discos.
 - f. El campo **Recuento de tramos** se muestra en función de los discos físicos seleccionados (paso 3). No se puede establecer este valor. Se calcula automáticamente después de seleccionar discos para un nivel multi-RAID. Si se selecciona RAID 10 y la controladora admite RAID 10 desigual, no se muestra el valor de recuento de tramos. La controladora establece automáticamente el valor apropiado.
3. En la sección **Seleccionar discos físicos**, seleccione la cantidad de discos físicos.
Para obtener más información acerca de los campos, consulte *iDRAC Online Help* (Ayuda en línea de iDRAC).
4. En el menú desplegable **Aplicar modo de operación**, seleccione el momento en que desea aplicar la configuración.
5. Haga clic en **Crear disco virtual**.
Según en la opción de **Aplicar modo de operación** seleccionada, se aplicará la configuración.

Creación de discos virtuales mediante RACADM

Utilice el comando `racadm storage createvd`. Para obtener más información, consulte *iDRAC RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de iDRAC) disponible en dell.com/esmanuals.

Edición de políticas de caché de discos virtuales

Es posible cambiar la política de lectura, de escritura o de caché de disco de un disco virtual.

 **NOTA:** Algunas controladoras no admiten todas las políticas de lectura o escritura. Por lo tanto, cuando se aplique una política, se mostrará un mensaje de error.

Las políticas de lectura indican si la controladora debe leer los sectores secuenciales del disco virtual al buscar datos:

- **Lectura anticipada adaptativa:** la controladora inicia la lectura anticipada solo si las dos últimas solicitudes de lectura obtuvieron acceso a sectores secuenciales del disco. Si las solicitudes de lectura

subsiguientes obtienen acceso a sectores aleatorios del disco, la controladora vuelve a la política sin lectura anticipada. La controladora continuará evaluando si las solicitudes de lectura obtienen acceso a sectores secuenciales del disco y, si es necesario, iniciará una lectura anticipada.

- **Lectura anticipada:** la controladora lee los sectores secuenciales del disco virtual cuando busca datos. La política de lectura anticipada puede mejorar el rendimiento del sistema si los datos se escriben en sectores secuenciales del disco virtual.
- **Sin lectura anticipada:** si se selecciona la política sin lectura anticipada, la controladora no debe usar la política de lectura anticipada.

Las políticas de escritura especifican si la controladora enviará una señal de término de la solicitud de escritura en cuanto los datos estén en la caché o después de que se hayan escrito en el disco.

- **Escritura simultánea:** la controladora envía una señal de finalización de la solicitud de escritura solo cuando los datos ya están escritos en el disco. La escritura simultánea de la memoria caché proporciona una mayor seguridad para los datos que la escritura no simultánea de la memoria caché, puesto que el sistema asume que los datos están disponibles solo después de que se han escrito de forma segura en el disco.
- **Escritura no simultánea:** la controladora envía un señal de finalización de la solicitud de escritura tan pronto como los datos están en la caché de la controladora pero aún no se han escrito en el disco. La escritura no simultánea de la memoria caché puede mejorar el rendimiento, ya que las solicitudes de lectura subsecuentes pueden recuperar datos de la caché más rápidamente que del disco. Sin embargo, la pérdida de datos se puede producir en caso de una falla del sistema que impide que los datos se escriban en un disco. Otras aplicaciones también podrían experimentar problemas cuando realizan acciones que asumen que los datos están disponibles en el disco.
- **Forzar escritura no simultánea:** la caché de escritura se activa sin importar si la controladora tiene una batería. Si la controladora no tiene una batería y se usa la escritura no simultánea de la memoria caché, podrían perderse datos ante una falla de alimentación.

La política de caché de disco se aplica a las lecturas en un disco virtual específico. Estos valores no afectan a la política de lectura anticipada.

NOTA:

- Las opciones de caché no volátil de la controladora y de respaldo de batería para la caché de la controladora afectan la política de lectura o la política de escritura que una controladora puede admitir. No todas las controladoras PERC contienen batería y caché.
- La lectura anticipada y la escritura no simultánea requieren una caché. Por lo tanto, si la controladora no dispone de una caché, no se permite la configuración de valores de políticas.

De manera similar, si PERC dispone de una caché, pero no de una batería, y se ha establecido una política por la que se requiere acceso a la memoria caché, se puede producir una pérdida de datos en caso de apagado. Por eso, muy pocas PERC no permiten esa política.

Por lo tanto, se establece el valor de política en función de la controladora PERC.

Eliminación de discos virtuales

La eliminación de un disco virtual destruye toda la información, incluidos los sistemas de archivos y los volúmenes que residen en el disco virtual, y quita el disco virtual de la configuración de la controladora. Al eliminar discos virtuales, todos los repuestos dinámicos globales asignados se pueden desasignar automáticamente en el momento en que se elimina el último disco virtual asociado con la controladora. Cuando se elimina el último disco virtual de un grupo de discos, todos los repuestos dinámicos dedicados asignados se convierten automáticamente en repuestos dinámicos globales.

Es necesario tener el privilegio de inicio de sesión y control del servidor para eliminar discos virtuales.

Cuando se permite esta operación, es posible eliminar un disco virtual de inicio. Esto se realiza desde la banda lateral y de forma independiente al sistema operativo. Por lo tanto, es posible que se muestre un mensaje de advertencia antes de eliminar la unidad virtual.

Si se elimina un disco virtual e inmediatamente se crea un nuevo disco virtual con las mismas características que el disco eliminado, la controladora reconoce los datos como si el primer disco virtual nunca se hubiera eliminado. En esta situación, si no desea conservar los datos antiguos después de recrear un nuevo disco virtual, vuelva a inicializar el disco virtual.

Revisión de congruencia en el disco virtual


Esta operación comprueba la exactitud de la información redundante (de paridad). Esta tarea solo se aplica a los discos virtuales redundantes. Cuando es necesario, la tarea Revisar congruencia recrea los datos redundantes. Si el disco virtual se encuentra en estado Degradado, es posible que la ejecución de una revisión de congruencia haga que el disco virtual regrese a un estado Listo. También es posible cancelar la operación Revisión de congruencia.

La opción Cancelar revisión de congruencia es una operación en tiempo real.


Es necesario tener el privilegio de inicio de sesión y control del servidor para realizar una revisión de congruencia en los discos virtuales.

Inicialización de discos virtuales

La inicialización de discos virtuales borra todos los datos en el disco, pero no cambia la configuración del disco virtual. Es necesario inicializar un disco virtual ya configurado antes de usarlo.

 **NOTA:** No inicialice discos virtuales si intenta recrear una configuración existente.

Es posible realizar una inicialización rápida o una inicialización completa o bien, cancelar la operación de inicialización.

 **NOTA:** Cancelar la inicialización es una operación en tiempo real. Se puede cancelar la inicialización utilizando solamente la interfaz web de iDRAC y no por medio de RACADM.

Inicialización rápida

La operación Inicialización rápida inicializa todos los discos físicos incluidos en el disco virtual. Esta tarea actualiza los metadatos en los discos físicos, de modo que todo el espacio en disco quede disponible para operaciones de escritura futuras. La tarea de inicialización se puede completar rápidamente, ya que la información existente en los discos físicos no se borra, a pesar de que las operaciones de escritura futuras sobrescribirán toda la información que permanezca en los discos físicos.

La inicialización rápida solo elimina la información en las secciones y en el sector de inicio. Realice una inicialización rápida solo si existen limitaciones de tiempo o las unidades de disco duro son nuevas o se encuentran en desuso. La inicialización rápida se completa en menos tiempo (generalmente entre 30 y 60 segundos).

 **PRECAUCIÓN:** Después de ejecutar una inicialización rápida, no se puede obtener acceso a los datos existentes.

La tarea Inicialización rápida no escribe ceros en los bloques de discos de los discos físicos. Debido a que la tarea Inicialización rápida no realiza una operación de escritura, se produce menos degradación en el disco.

Si se realiza una inicialización rápida en un disco virtual, se sobrescriben los primeros y los últimos 8 MB del disco virtual, con lo que se eliminan los registros de inicio o la información sobre particiones. Esta operación tarda solo 2 o 3 segundos en completarse; se recomienda realizarla al recrear discos virtuales.

La inicialización de segundo plano se inicia cinco minutos después de que se haya finalizado la inicialización rápida.


Inicialización completa o lenta

La inicialización completa (también denominada inicialización lenta) inicializa todos los discos físicos incluidos en el disco virtual. Esta tarea actualiza los metadatos en los discos físicos y borra todos los datos y los sistemas de archivos existentes. Es posible realizar una inicialización completa después de crear el disco virtual. En comparación con la operación de inicialización rápida, es recomendable utilizar la inicialización completa si existe algún problema con un disco físico o se sospecha que el disco contiene bloques de disco dañados. La operación de inicialización completa reasigna los bloques dañados y escribe ceros en todos los bloques de disco.

Si se lleva a cabo la inicialización completa de un disco virtual, no se necesita una inicialización de segundo plano. Durante la inicialización completa, el host no puede obtener acceso al disco virtual. Si el sistema se reinicia durante una inicialización completa, la operación se anula y se inicia el proceso de inicialización de segundo plano en el disco virtual.


Siempre se recomienda ejecutar una inicialización completa en las unidades donde se hayan almacenado datos anteriormente. La inicialización completa puede tardar entre 1 y 2 minutos por GB. La velocidad de inicialización varía según el modelo de la controladora, la velocidad de las unidades de disco duro y la versión de firmware.

La tarea de inicialización completa inicializa un disco físico a la vez.

 **NOTA:** La inicialización completa solo se admite en tiempo real. Unas pocas controladoras admiten la inicialización completa.

Cifrado de discos virtuales

Cuando se desactiva el cifrado en una controladora (es decir, se elimina la clave de seguridad), es necesario activar manualmente el cifrado para los discos virtuales creados con unidades SED. Si el disco virtual se crea después de haber activado el cifrado en una controladora, el disco virtual se cifra automáticamente. Sin embargo, se configurará automáticamente como un disco virtual cifrado, a menos que se desactive la opción de cifrado activada durante la creación del disco virtual.

 **NOTA:** Esta tarea solo se puede organizar en etapas y no admite el tiempo real.

Es necesario tener el privilegio de inicio de sesión y control del servidor para administrar las claves de cifrado.

Asignación o desasignación de repuestos dinámicos dedicados

El repuesto dinámico dedicado es un disco de reserva sin usar que se asigna a un disco virtual. Cuando un disco físico en el disco virtual falla, el repuesto dinámico se activa a fin de reemplazar el disco físico fallido sin interrumpir el sistema ni requerir de intervención.

Es necesario tener el privilegio de inicio de sesión y control del servidor para ejecutar esta operación.

Solo los discos físicos compatibles con T10 PI (DIF) pueden asignarse como repuestos dinámicos a discos virtuales activados con T10 PI (DIF). Las unidades sin T10 PI (DIF) que se asignan como repuestos dinámicos dedicados no pueden ser repuestos dinámicos si T10 PI (DIF) se activa en un disco virtual más adelante.

Es posible asignar solamente unidades de 4000 como repuesto dinámico a discos virtuales de 4000.

Si ha asignado un disco virtual como repuesto dinámico dedicado en el modo Agregar a operaciones pendientes, se crea la operación pendiente, pero no se crea un trabajo. Por lo tanto, si intenta desasignar el repuesto dinámico dedicado, la operación pendiente Asignar repuesto dinámico dedicado se borra.

Si ha desasignado un disco virtual como repuesto dinámico dedicado en el modo Agregar a operaciones pendientes, se crea la operación pendiente, pero no se crea un trabajo. Por lo tanto, si intenta asignar el repuesto dinámico dedicado, la operación pendiente Desasignar repuesto dinámico dedicado se borra.

Administración de discos virtuales mediante la interfaz web

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Almacenamiento** → **Discos virtuales** → **Administrar**.

Se mostrará la página **Administrar discos virtuales**.

2. En el menú desplegable **Controladora**, seleccione la controladora para la que desea administrar los discos virtuales.
3. Para uno o varios discos virtuales, en cada menú desplegable **Acción**, seleccione una acción.

Es posible especificar más de una acción para una unidad virtual. Cuando se selecciona una acción, se muestra un menú desplegable **Acción** adicional. Seleccione otra acción desde este menú desplegable. La acción que ya se ha seleccionado no aparece en los menús desplegables **Acción** adicionales. Además, se muestra el vínculo **Quitar** al lado de la acción seleccionada. Haga clic en este vínculo para eliminar la acción seleccionada.

- **Eliminar**
- **Editar política: caché de lectura:** cambie la política de caché de lectura a una de las siguientes opciones:
 - **Lectura anticipada adaptativa**
 - **Sin lectura anticipada**
 - **Lectura anticipada**
- **Editar política: caché de escritura:** cambie la política de caché de escritura a una de las siguientes opciones:
 - **Escritura simultánea**
 - **Escritura no simultánea**
 - **Forzar escritura no simultánea**

- **Editar política: caché de disco:** cambie la política de caché de disco a una de las siguientes opciones:
 - **Default (Predeterminado)**
 - **Activado**
 - **Desactivado**
- **Inicialización: rápida:** actualiza los metadatos en los discos físicos, de modo que todo el espacio en disco quede disponible para operaciones de escritura futuras. La inicialización se puede completar rápidamente, ya que la información existente en los discos físicos no se borra, a pesar de que las operaciones de escritura futuras sobrescribirán toda la información que permanezca en los discos físicos.
- **Inicialización: total:** Se borran todos los datos y los sistemas de archivos existentes.
- **Revisión de congruencia**
- **Cifrar disco virtual:** cifra la unidad de disco virtual. Si la controladora no admite el cifrado, es posible crear, cambiar o eliminar las claves de seguridad.
- **Administrar repuestos dinámicos dedicados:** asigne o desasigne un disco físico como un repuesto dinámico dedicado. Solo se muestran los repuestos dinámicos dedicados válidos. Si no hay repuestos dinámicos dedicados válidos, esta sección no aparece en el menú desplegable.

Para obtener más información sobre estas opciones, consulte la *Ayuda en línea de iDRAC*.

4. En el menú desplegable **Aplicar modo de operación**, seleccione el momento en que desea aplicar la configuración.
5. Haga clic en **Apply (Aplicar)**.
Según el modo de operación seleccionado, se aplicará la configuración.

Administración de discos virtuales mediante RACADM

Utilice los siguientes comandos RACADM para administrar discos virtuales:

- Para eliminar un disco virtual: `racadm storage deletevd:<VD FQDD>`
- Para inicializar un disco virtual: `racadm storage init:<VD FQDD> -speed {fast|full}`
- Para comprobar la congruencia de discos virtuales: `racadm storage ccheck:<vdisk fqdd>`
- Para cifrar discos virtuales: `racadm storage encryptvd:<VD FQDD>`
- Para asignar o desasignar repuestos dinámicos dedicados: `racadm storage hotspare:<Physical Disk FQDD> -assign yes -type dhs -vdkey: <FQDD of VD>`
- Para cancelar la revisión de congruencia: `racadm storage cancelcheck: <vdisks fqdd>`

Administración de controladoras

Es posible realizar las siguientes tareas para las controladoras:

- Configurar propiedades de la controladora
- Importar o importar automáticamente configuración ajena
- Borrar configuración ajena
- Restablecer configuración de la controladora
- Crear, modificar o eliminar claves de seguridad

Enlaces relacionados

- [Configuración de las propiedades de la controladora](#)
- [Importación o importación automática de la configuración ajena](#)
- [Borrar configuración ajena](#)

[Restablecimiento de la configuración de la controladora](#)
[Controladoras admitidas](#)
[Resumen de funciones admitidas para Storage Devices \(Dispositivos de almacenamiento\)](#)
[Convertir a disco RAID](#)
[Convertir a disco no RAID](#)

Configuración de las propiedades de la controladora

Es posible configurar las siguientes propiedades de la controladora:

- Modo de lectura de patrullaje (automático o manual)
- Iniciar o detener la lectura de patrullaje si el modo de lectura de patrullaje es manual
- Áreas de lectura de patrullaje no configuradas
- Modo de revisión de congruencia
- Modo de escritura diferida
- Modo de equilibrio de carga
- Porcentaje de revisión de congruencia
- Porcentaje de recreación
- Porcentaje de inicialización de segundo plano
- Porcentaje de reconstrucción
- Importación automática de configuración ajena mejorada
- Crear o cambiar claves de seguridad



NOTA: Es posible configurar la propiedad Áreas de lectura de patrullaje no configuradas por medio de la interfaz web de iDRAC y no por medio de RACADM.

Es necesario tener el privilegio de inicio de sesión y control del servidor para configurar las propiedades de la controladora.


Consideraciones sobre el modo de lectura de patrullaje

La lectura de patrullaje identifica los errores en el disco para evitar fallas de disco y pérdida o daño de datos.

La lectura de patrullaje no se ejecuta en un disco físico en las siguientes circunstancias:

- El disco físico no está incluido en un disco virtual o no está asignado como un repuesto dinámico.
- El disco físico está incluido en un disco virtual que actualmente está experimentando alguna de las siguientes acciones:
 - Una recreación
 - Una reconfiguración o reconstrucción
 - Una inicialización de segundo plano
 - Una revisión de congruencia

Además, la lectura de patrullaje se suspende durante actividad de E/S intensa y se reanuda una vez completada la actividad de E/S.

 **NOTA:** Para obtener más información acerca de la frecuencia con la que se ejecuta la lectura de patrullaje en modo automático, consulte la documentación de la controladora correspondiente.

Load Balance

La propiedad Equilibrio de carga ofrece la capacidad de utilizar automáticamente los dos puertos o conectores de la controladora conectados al mismo gabinete para dirigir solicitudes de E/S. Esta propiedad solo se encuentra disponible en las controladoras SAS.

Porcentaje de inicialización de segundo plano

En las controladoras PERC, la inicialización de segundo plano de un disco virtual redundante comienza automáticamente de 0 a 5 minutos después de la creación del disco virtual. La inicialización de segundo plano de un disco virtual redundante prepara el disco virtual para mantener datos redundantes y mejora el rendimiento de escritura. Por ejemplo, una vez completada la inicialización de segundo plano de un disco virtual RAID 5, se inicializa la información de paridad. Una vez completada la inicialización de segundo plano de un disco virtual RAID 1, se reflejan los discos físicos.

El proceso de inicialización de segundo plano ayuda a la controladora a identificar y corregir problemas que se podrían producir en otro momento con los datos redundantes. Con respecto a esto, el proceso de inicialización de segundo plano es similar al de la revisión de congruencia. Se debe permitir que la inicialización de segundo plano se ejecute hasta su finalización. Si se cancela, la inicialización de segundo plano se reinicia automáticamente entre 0 y 5 minutos después. Algunos procesos, como las operaciones de lectura y escritura, son posibles mientras se ejecuta la inicialización de segundo plano. Otros procesos, como la creación de un disco virtual, no pueden ejecutarse de forma simultánea con la inicialización de segundo plano. Estos procesos provocan la cancelación de la inicialización de segundo plano.

El porcentaje de inicialización de segundo plano, que se puede configurar entre 0 % y 100 %, representa el porcentaje de recursos del sistema dedicado a ejecutar la tarea de inicialización de segundo plano. En 0 %, la inicialización de segundo plano queda última en la lista de prioridades de la controladora, demora el mayor tiempo posible en completarse y es la configuración con el menor impacto sobre el rendimiento del sistema. Un porcentaje de inicialización de segundo plano de 0 % no significa que el proceso quede detenido o en pausa. En 100 %, la inicialización de segundo plano queda primera en la lista de prioridades de la controladora, el tiempo de inicialización de segundo plano es mínimo y esta configuración ejerce el mayor impacto sobre el rendimiento del sistema.

Revisión de congruencia

La tarea Revisar congruencia comprueba la exactitud de la información redundante (de paridad). Esta tarea solo aplica a los discos virtuales redundantes. Cuando es necesario, la tarea Revisar congruencia recrea los datos redundantes. Si el disco virtual está en estado de redundancia fallida, es posible que la ejecución de una revisión de congruencia haga que el disco virtual regrese a un estado Listo.

El porcentaje de revisión de congruencia, que se puede configurar entre 0 % y 100 %, representa el porcentaje de recursos del sistema dedicado a ejecutar la tarea de revisión de congruencia. En 0 %, la revisión de congruencia queda última en la lista de prioridades de la controladora, demora el mayor tiempo posible en completarse y es la configuración con el menor impacto sobre el rendimiento del sistema. Un porcentaje de revisión de congruencia de 0 % no significa que el proceso quede detenido o en pausa. En 100 %, la revisión de congruencia queda primera en la lista de prioridades de la

controladora, el tiempo de revisión de congruencia es mínimo y esta configuración ejerce el mayor impacto sobre el rendimiento del sistema.

Crear o cambiar claves de seguridad

Al configurar las propiedades de la controladora, es posible crear o cambiar las claves de seguridad. La controladora usa la clave de cifrado para bloquear o desbloquear el acceso a los discos de cifrado automático (SED). Se puede crear una sola clave de cifrado para cada controladora con funciones de cifrado. La clave de seguridad se administra mediante el uso de la función Administración de claves locales (LKM). LKM se utiliza para generar la identificación de la clave y la clave o contraseña requerida para proteger el disco virtual. Si se usa LKM, se debe proporcionar el identificador de clave de seguridad y la frase de contraseña para crear la clave de cifrado.

Esta tarea no se admite en las controladoras de hardware PERC que se ejecutan en modo HBA.

Si se crea la clave de seguridad en el modo Agregar a operaciones pendientes, pero no se crea un trabajo, cuando se elimina la clave de seguridad, se borra la operación pendiente Crear clave de seguridad.

Configuración de las propiedades de la controladora mediante la interfaz web

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Almacenamiento** → **Controladoras** → **Configuración**.
Se mostrará la página **Configuración de controladoras**.
2. En la sección **Configurar propiedades de la controladora**, en el menú desplegable **Controladora**, seleccione la controladora que desea configurar.
3. Especifique la información necesaria para las distintas propiedades.
En la columna **Valor actual** se muestran los valores existentes para cada propiedad. Para modificar este valor, seleccione la opción en el menú desplegable **Acción** de cada propiedad.
Para obtener información acerca de los campos, consulte la *Ayuda en línea de iDRAC*.
4. En el menú desplegable **Aplicar modo de operación**, seleccione el momento en que desea aplicar la configuración.
5. Haga clic en **Apply (Aplicar)**.
Según el modo de operación seleccionado, se aplicará la configuración.

Configuración de las propiedades de la controladora mediante RACADM

- Para establecer el modo de lectura de patrullaje:

```
racadm set storage.controller.<index>.PatrolReadMode {Automatic | Manual | Disabled}
```
- Si el modo de lectura de patrullaje se ha configurado en Manual, utilice los comandos siguientes para iniciar y detener el modo de lectura de patrullaje:

```
racadm storage patrolread:<Controller FQDD> -state {start|stop}
```
- Para especificar el modo de revisión de congruencia, utilice el objeto **Storage.Controller.CheckConsistencyMode**.
- Para activar o desactivar el modo de escritura diferida, utilice el objeto **Storage.Controller.CopybackMode**.
- Para activar o desactivar el modo de equilibrio de carga, utilice el objeto **Storage.Controller.PossibleloadBalancedMode**.

- Para especificar el porcentaje de recursos del sistema dedicados a realizar la revisión de congruencia en un disco virtual redundante, utilice el objeto **Storage.Controller.CheckConsistencyRate**.
- Para especificar el porcentaje de recursos de la controladora dedicados a recrear un disco fallido, utilice el objeto **Storage.Controller.RebuildRate**.
- Para especificar el porcentaje de recursos de la controladora dedicados a realizar la inicialización de segundo plano (BGI) de un disco virtual tras su creación, utilice el objeto **Storage.Controller.BackgroundInitializationRate**.
- Para especificar el porcentaje de recursos de la controladora dedicados a reconstruir un grupo de discos después de agregar un disco físico o cambiar el nivel RAID de un disco virtual que reside en el grupo de discos, utilice el objeto **Storage.Controller.ReconstructRate**.
- Para activar o desactivar la importación automática mejorada de la configuración ajena para la controladora, utilice el objeto **Storage.Controller.EnhancedAutoImportForeignConfig**.
- Para crear, modificar o eliminar la clave de seguridad para cifrar las unidades virtuales:

```
racadm storage createsecuritykey:<Controller FQDD> -key <Key id> -passwd <passphrase>
```

```
racadm storage modifysecuritykey:<Controller FQDD> -key <key id> -oldpasswd <old passphrase> -newpasswd <new passphrase>
```

```
racadm storage deletesecuritykey:<Controller FQDD>
```

Importación o importación automática de la configuración ajena

Una configuración ajena consiste en datos residentes en discos físicos que han sido trasladados de una controladora a otra. Se considera que los discos virtuales que residen en discos físicos que fueron cambiados constituyen una configuración ajena.

Es posible importar configuraciones ajenas, de forma que los discos virtuales no se pierdan después de cambiar los discos físicos. Una configuración ajena se puede importar únicamente si contiene un disco virtual en estado Listo o Degradado o bien, un repuesto dinámico dedicado a un disco virtual que se puede importar o ya se encuentra presente.


Todos los datos de los discos virtuales deben estar presentes, pero si los discos virtuales usan un nivel RAID redundante, no se requieren los datos redundantes adicionales.

Por ejemplo, si la configuración ajena contiene solo un lado de un reflejo en un disco virtual RAID 1, el disco virtual se encuentra en estado Degradado y se puede importar. Si la configuración ajena contiene solo un disco físico que se configuró originalmente como RAID 5 usando tres discos físicos, el disco virtual RAID 5 se encuentra en estado Fallido y no se puede importar.

Además de tener discos virtuales, una configuración ajena puede constar de un disco físico que haya sido asignado como repuesto dinámico en una controladora y que después haya sido cambiado a otra controladora. La tarea Importar configuración ajena importa el nuevo disco físico como repuesto dinámico. Si el disco físico era un repuesto dinámico dedicado en la controladora anterior, pero el disco virtual al que el repuesto dinámico fue asignado ya no está presente en la configuración ajena, el disco físico se importa como repuesto dinámico global.

Si se detecta alguna configuración ajena bloqueada donde se usa el administrador de claves locales (LKM), no se puede ejecutar la operación Importar configuración ajena en iDRAC en esta versión. Es necesario desbloquear las unidades mediante CTRL-R y continuar con la importación de la configuración ajena desde iDRAC.


La tarea Importar configuración ajena sólo se muestra cuando la controladora ha detectado una configuración ajena. También puede identificar si un disco físico contiene una configuración ajena (disco virtual o repuesto dinámico), revisando el estado del disco físico. Si el estado del disco físico es Ajeno, entonces el disco físico contiene la totalidad o una parte de un disco virtual, o bien tiene una asignación de repuesto dinámico.

 **NOTA:** La tarea de importación de configuración ajena importa todos los discos virtuales que residen en los discos físicos que se han agregado a la controladora. Si hay más de un disco virtual ajeno presente, no es posible elegir cuál importar. Se importan todas las configuraciones ajenas.

La controladora PERC9 admite la importación automática de configuraciones ajenas sin la interacción de los usuarios. La importación automática puede estar activada o desactivada. Si esta opción se encuentra activada, la controladora PERC puede importar automáticamente cualquier configuración ajena detectada sin intervención manual. Si la opción se encuentra desactivada, la controladora PERC no importa automáticamente ninguna configuración ajena.

Es necesario tener el privilegio de inicio de sesión y control del servidor para importar configuraciones ajenas.

Esta tarea no se admite en las controladoras de hardware PERC que se ejecutan en modo HBA.

 **NOTA:** No se recomienda quitar el cable de un gabinete externo cuando el sistema operativo se está ejecutando en el sistema. Quitar el cable puede provocar una configuración ajena cuando la conexión se vuelva a establecer.

Es posible administrar configuraciones ajenas en los siguientes casos:

- Se quitan y se vuelven a insertar todos los discos físicos de una configuración.
- Se quitan y se vuelven a insertar algunos de los discos físicos de una configuración.
- Se quitan todos los discos físicos de un disco virtual, pero en momentos diferentes; a continuación, se vuelven a insertar.
- Se quitan los discos físicos de un disco virtual sin redundancia.

Las siguientes limitaciones se aplican para los discos físicos que se considera importar:

- El estado de unidad de un disco físico puede cambiar desde el momento en que se analiza la configuración ajena hasta el momento en que se ejecuta la importación real. La importación de configuraciones ajenas solo se realiza en discos que se encuentran en el estado No configurado y en buen estado.
- Las unidades que se encuentran en el estado Fallido o Fuera de línea no pueden importarse.
- El firmware no permite importar más de ocho configuraciones ajenas.


Importación de la configuración ajena mediante la interfaz web

Para importar la configuración ajena:

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Almacenamiento** → **Controladoras** → **Configuración**.
Se mostrará la página **Configuración de controladoras**.
2. En la sección **Configuración ajena**, en el menú desplegable **Controladora**, seleccione la controladora que desea configurar.

3. En el menú desplegable **Aplicar modo de operación**, seleccione el momento en que desea realizar la importación.
4. Haga clic en **Importar configuración ajena**.
Según el modo de operación seleccionado, se importará la configuración.

Para importar configuraciones ajenas automáticamente, en la sección **Configurar propiedades de la controladora**, active la opción **Importación automática de configuración ajena mejorada**, seleccione **Aplicar modo de operación** y haga clic en **Aplicar**.

 **NOTA:** Después de activar la opción **Importación automática de configuración ajena mejorada**, es necesario reiniciar el sistema para importar la configuración ajena.

Importación de la configuración ajena mediante RACADM

Para importar la configuración ajena, utilice el siguiente comando:

```
racadm storage importconfig:<Controller FQDD>
```

Para obtener más información, consulte *iDRAC RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de iDRAC)* disponible en dell.com/esmanuals.

Borrar configuración ajena

Después de mover un disco físico de una controladora a otra, es posible descubrir que dicho disco físico contiene la totalidad o una porción de un disco virtual (configuración ajena). Para identificar si un disco físico previamente usado contiene o no una configuración ajena (disco virtual), se puede revisar el estado del disco físico. Si el estado del disco físico es Ajeno, el disco contiene la totalidad o una porción de un disco virtual. Es posible borrar o eliminar la información del disco virtual de los discos físicos recientemente conectados.

La operación Borrar configuración ajena borra permanentemente todos los datos de los discos físicos que se agregaron a la controladora. Si existe más de un disco virtual ajeno presente, se borrarán todas las configuraciones. Se puede preferir importar el disco virtual en lugar de destruir los datos. Se debe llevar a cabo una inicialización para eliminar los datos ajenos. Si se cuenta con una configuración ajena incompleta que no puede importarse, es posible usar la opción Borrado de la configuración ajena para borrar los datos ajenos de los discos físicos.

Borrado de la configuración ajena mediante la interfaz web

Para borrar la configuración ajena:

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Almacenamiento** → **Controladoras** → **Configuración**.
Se mostrará la página **Configuración de controladoras**.
2. En la sección **Configuración ajena**, en el menú desplegable **Controladora**, seleccione la controladora en la que desea borrar la configuración ajena.
3. En el menú desplegable **Aplicar modo de operación**, seleccione el momento en que desea borrar los datos.
4. Haga clic en **Borrar**.
Según el modo de operación seleccionado, se borrarán los discos virtuales que residen en el disco físico.

Borrado de la configuración ajena mediante RACADM


Para borrar la configuración ajena, utilice el siguiente comando:

```
racadm storage clearconfig:<Controller FQDD>
```

Para obtener más información, consulte *iDRAC RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de iDRAC)* disponible en dell.com/esmanuals.

Restablecimiento de la configuración de la controladora

Es posible restablecer la configuración de una controladora. Esta operación elimina las unidades de disco virtual y desasigna los repuestos dinámicos en la controladora. Esto no borra los datos que no se incluyen en la eliminación de los discos de la configuración. El restablecimiento de la configuración tampoco elimina configuraciones ajenas. El soporte en tiempo real de esta función solo se encuentra disponible en el firmware PERC 9.1. El restablecimiento de la configuración no borra ningún dato. Es posible recrear exactamente la misma configuración sin una operación de inicialización, lo que puede dar lugar a que se recuperen los datos. Es necesario tener el privilegio de control del servidor.

 **NOTA:** El restablecimiento de la configuración de la controladora no elimina una configuración ajena. Para eliminar una configuración ajena, ejecute una operación Borrar configuración.

Restablecimiento de la configuración de la controladora mediante la interfaz web

Para restablecer la configuración de la controladora:

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Almacenamiento** → **Controladoras** → **Solución de problemas**.
Se mostrará la página **Solución de problemas de controladoras**.
2. En el menú desplegable **Acciones**, seleccione la opción **Restablecer configuración** para una o varias controladoras.
3. Para cada controladora, en el menú desplegable **Aplicar modo de operación**, seleccione el momento en que desea aplicar la configuración.
4. Haga clic en **Apply (Aplicar)**.
Según el modo de operación seleccionado, se aplicará la configuración.

Restablecimiento de la configuración de la controladora mediante RACADM

Para restablecer la configuración de la controladora, utilice el siguiente comando:

```
racadm storage resetconfig:<Controller FQDD>
```

Para obtener más información, consulte *iDRAC RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de iDRAC)* disponible en dell.com/esmanuals.

Operaciones con adaptadores HBA SAS de 12 Gbps

Las controladoras no RAID son HBA que no disponen de algunas capacidades de RAID. Estas controladoras no admiten discos virtuales.

La interfaz de iDRAC solo admite la controladora HBA SAS de 12 Gbps en esta versión.

Es posible realizar las siguientes tareas para controladoras no RAID:

- Ver las propiedades de la controladora, los discos físicos y el gabinete que se apliquen a la controladora no RAID. También, ver las propiedades de EMM, el ventilador, la unidad de suministro de energía y la sonda de temperatura asociadas con el gabinete. Las propiedades se muestran en función del tipo de controladora.
- Ver información sobre el inventario de software y hardware.
- Actualizar el firmware para gabinetes detrás de la controladora HBA SAS de 12 Gbps (organizados en etapas).
- Supervisar el sondeo o la frecuencia de sondeo para el estado de intervalo SMART en el disco físico cuando se detecta un cambio de estado.
- Supervisar el estado de acoplamiento activo o extracción directa en los discos físicos.
- Hacer parpadear o dejar de hacer parpadear los LED.

NOTA:

- Es necesario realizar la operación Recopilar inventario del sistema en el reinicio (CSIOR) antes de hacer un inventario o supervisar las controladoras no RAID.
- Reinicie el sistema después de realizar una actualización del firmware.
- La supervisión en tiempo real para unidades con capacidad SMART y sensores de un gabinete SES solo se realiza en las controladoras HBA SAS de 12 Gbps.

Enlaces relacionados

- [Inventario y supervisión de dispositivos de almacenamiento](#)
- [Visualización del inventario del sistema](#)
- [Actualización del firmware de dispositivos](#)
- [Supervisión de análisis de falla predictiva en unidades](#)
- [Forma de hacer parpadear o dejar de hacer parpadear LED de componentes](#)

Supervisión de análisis de falla predictiva en unidades

Storage Management es compatible con la tecnología de supervisión automática, análisis y generación de informes (SMART) en discos físicos habilitados para SMART.

SMART realiza un análisis de falla predictiva en cada disco y envía alertas si se predice una falla en el disco. Las controladoras revisan los discos físicos en busca de predicciones de fallas y, si encuentran alguna, pasan esta información a iDRAC. iDRAC inmediatamente registra una alerta.

Operaciones de la controladora en modo no RAID (HBA)


Si la controladora se encuentra en el modo no-RAID (modo HBA):

- Los discos virtuales o los repuestos dinámicos no se encuentran disponibles.
- El estado de seguridad de la controladora se encuentra desactivado.
- Todos los discos físicos se encuentran en el modo no RAID.

Es posible realizar las siguientes operaciones si la controladora se encuentra en modo no RAID:

- Hacer parpadear y dejar de hacer parpadear el disco físico.
- Configurar las siguientes propiedades:
 - Modo de equilibrio de carga
 - Modo de revisión de congruencia

- Modo de lectura de patrullaje
 - Modo de escritura diferida
 - Modo de inicio de la controladora
 - Importación automática de configuración ajena mejorada
 - Porcentaje de recreación
 - Porcentaje de revisión de congruencia
 - Porcentaje de reconstrucción
 - Porcentaje de inicialización de segundo plano
 - Modo de gabinete o de plano posterior
- Ver todas las propiedades que se aplican a una controladora RAID esperadas para discos virtuales.
 - Borrar configuración ajena

 **NOTA:** Si una operación no se admite en el modo no RAID, se mostrará un mensaje de error.

Cuando la controladora se encuentra en el modo no RAID, no es posible supervisar las sondas de temperatura de gabinete, los ventiladores ni los suministros de energía.

Ejecución de trabajos de configuración de RAID en varias controladoras de almacenamiento

Al realizar operaciones en más de dos controladoras de almacenamiento desde cualquier interfaz de iDRAC compatible, asegúrese de realizar lo siguiente:

- Ejecute los trabajos en cada controladora de manera individual. Espere a que cada trabajo se complete antes de comenzar con la configuración y la creación de trabajos en la siguiente controladora.
- Programe varios trabajos de manera que se ejecuten más tarde utilizando las opciones de programación.

Administración de SSD PCIe

La unidad de estado sólido (SSD) de interconexión rápida de componentes periféricos (PCIe) es un dispositivo de almacenamiento de alto rendimiento diseñado para soluciones en la que se requiere latencia baja, alta capacidad de operaciones de entrada y salida por segundo (IOPS) y confiabilidad en almacenamiento y servicio de clase empresarial. El diseño de SSD PCIe se basa en la tecnología flash NAND con celda de nivel individual (SLC) y celda de múltiples niveles (MLC) con una interfaz de alta velocidad compatible con PCIe 2.0 y PCIe 3.0.

Si se usan interfaces de iDRAC, es posible visualizar y configurar las unidades SSD PCIe de NVMe.

A continuación se enumeran las funciones clave de PCIe SSD:

- Capacidad de acoplamiento activo
- Dispositivo de alto rendimiento

El subsistema SSD PCIe consta de un plano posterior, una tarjeta de extensión PCIe que se conecta al plano posterior del sistema y proporciona conectividad de PCIe para un máximo de cuatro a ocho SSD PCIe en la parte frontal del chasis y los SSD PCIe.

Es posible realizar las siguientes operaciones para SSD PCIe:

- Crear inventario y supervisar de manera remota la condición de los dispositivos SSD PCIe en el servidor
- Preparar para quitar SSD PCIe
- Borrar los datos de manera segura
- Hacer parpadear o dejar de hacer parpadear LED de dispositivos

Enlaces relacionados

[Inventario y supervisión de SSD PCIe](#)

[Preparar para quitar una unidad SSD PCIe](#)

[Borrado de datos de un dispositivo SSD PCIe](#)

Inventario y supervisión de SSD PCIe

Ya sea organizada en etapas o en tiempo real, la siguiente información de inventario y supervisión se encuentra disponible para los dispositivos SSD PCIe:

- Información de hardware:
 - Tarjeta de extensión de SSD PCIe
 - Plano posterior de SSD PCIe
- El inventario de software incluye solamente la versión de firmware para SSD PCIe.

Inventario y supervisión de SSD PCIe mediante la interfaz web

Para crear un inventario y supervisar los dispositivos SSD PCIe, en la interfaz web de iDRAC, vaya a **Descripción general** → **Almacenamiento** → **Discos físicos**. Se mostrará la página **Propiedades**. Para SSD PCIe, la columna **Nombre** muestra **PCIe SSD**. Expanda para ver las propiedades.

Inventario y supervisión de SSD PCIe mediante RACADM

Use el comando `racadm storage get controllers:<PcieSSD controller FQDD>` para realizar un inventario y supervisar los dispositivos SSD PCIe.

Para ver todas las unidades SSD PCIe:


```
racadm storage get pdisks
```

Para ver las tarjetas de extensión PCIe:

```
racadm storage get controllers
```

Para ver la información sobre el plano posterior de SSD PCIe:

```
racadm storage get enclosures
```

 **NOTA:** Para todos los comandos mencionados, también se muestran los dispositivos PERC.

Para obtener más información, consulte *iDRAC RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de iDRAC)* disponible en dell.com/esmanuals.

Preparar para quitar una unidad SSD PCIe

Las unidades SSD PCIe admiten el intercambio directo ordenado. Esto permite agregar o quitar dispositivos sin interrumpir ni reiniciar el sistema en el que se encuentran instalados los dispositivos. Para evitar la pérdida de datos, es obligatorio utilizar la operación Preparar para quitar antes de retirar físicamente un dispositivo.

 **NOTA:**

- El intercambio directo ordenado solo se admite cuando las unidades SSD PCIe se encuentran instaladas en un sistema compatible donde se ejecuta un sistema operativo admitido. Para asegurarse de tener la configuración correcta para SSD PCIe, consulte el Manual del propietario específico de su sistema.
- La tarea Preparar para quitar no se admite para SSD PCIe en los sistemas VMware vSphere (ESXi).
- La tarea Preparar para quitar solo se puede organizar en etapas y no admite el tiempo real.

La operación Preparar para quitar detiene toda actividad en segundo plano y toda actividad de E/S en proceso para que el dispositivo pueda extraerse de forma segura. Esta tarea hace que los LED de estado parpadeen en el dispositivo. El dispositivo se puede extraer del sistema de forma segura en las siguientes condiciones después de iniciar la operación Preparar para quitar:

- La SSD PCIe está haciendo parpadear el modelo LED seguro para quitar.
- El sistema ya no puede acceder al SSD PCIe.


Antes de preparar el dispositivo PCIe SSD para su extracción, asegúrese de lo siguiente:

- El módulo de servicio de iDRAC se encuentra instalado.
- Lifecycle Controller está activado.
- Cuenta con privilegios de inicio de sesión y control del servidor.

Forma de preparar para quitar una unidad SSD PCIe mediante la interfaz web

Para preparar el dispositivo SSD PCIe para su extracción:

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Almacenamiento** → **Discos físicos** → **Configuración**.
Se mostrará la página **Configuración de discos físicos**.
2. En el menú desplegable **Controladora**, seleccione la tarjeta de extensión para ver las unidades SSD PCIe asociadas.
3. En los menús desplegables, seleccione **Preparar para quitar** para una o varias unidades SSD PCIe.
Si ha seleccionado **Preparar para quitar** y desea ver las otras opciones en el menú desplegable, seleccione **Acción** y, a continuación, haga clic en el menú desplegable para ver las otras opciones.
4. En el menú desplegable **Aplicar modo de operación**, seleccione **Aplicar ahora** para aplicar las acciones de inmediato.
Si existen trabajos que se deben completar, esta opción se mostrará en gris.

 **NOTA:** Para los dispositivos SSD PCIe, solo la opción **Aplicar ahora** se encuentra disponible. Esta operación no se admite en el modo organizado en etapas.

5. Haga clic en **Apply (Aplicar)**.
Si la tarea no se ha creado, aparecerá un mensaje indicando que el trabajo no se creó. El mensaje también muestra la identificación de mensaje y las acciones de respuesta recomendadas.
Si la tarea se ha creado correctamente, se mostrará un mensaje indicando que se ha creado el valor de ID de trabajo para la controladora seleccionada. Haga clic en **Cola de trabajos** para ver el progreso de ese trabajo en la página **Cola de trabajos**.

Si no se ha creado la operación pendiente, se mostrará un mensaje de error. Si la operación pendiente es exitosa y la creación de un trabajo no se ejecuta correctamente, se mostrará un mensaje de error.

Forma de preparar para quitar una unidad SSD PCIe mediante RACADM

Para preparar la unidad SSD PCIe para su extracción, ejecute el siguiente comando:

```
racadm storage preparetoremove:<PCIeSSD FQDD>
```

Para crear el trabajo de destino después de ejecutar el comando **preparetoremove**, ejecute el siguiente comando:

```
racadm jobqueue create <PCIe SSD FQDD> -s TIME_NOW --realtime
```

Para consultar el valor de ID de trabajo devuelto, ejecute el siguiente comando:

```
racadm jobqueue view -i <job ID>
```

Para obtener más información, consulte *iDRAC RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de iDRAC)* disponible en dell.com/esmanuals.

Borrado de datos de un dispositivo SSD PCIe

El borrado seguro borra de forma permanente todos los datos presentes en el disco. La realización de un borrado criptográfico en una unidad SSD PCIe sobrescribe todos los bloques y provoca la pérdida permanente de todos los datos en SSD PCIe. Durante el borrado criptográfico, el host no puede acceder a SSD PCIe. Los cambios se aplican después de reiniciar el sistema.

Si el sistema se reinicia o sufre una pérdida de alimentación durante el borrado criptográfico, se cancela la operación. Es necesario reiniciar el sistema y el proceso.

Antes de borrar datos en un dispositivo SSD PCIe, asegúrese de lo siguiente:

- Lifecycle Controller está activado.
- Cuenta con privilegios de inicio de sesión y control del servidor.

NOTA:


- Cuando se borra la unidad, se muestra en el sistema operativo como en línea pero no se inicializa. Es necesario volver a inicializar y a formatear la unidad para poder usarla nuevamente.
- Después de realizar el acoplamiento activo de una unidad SSD PCIe, es posible que la unidad demore varios segundos para mostrarse en la interfaz web.

Borrado de datos de un dispositivo SSD PCIe mediante la interfaz web

Para borrar los datos en el dispositivo SSD PCIe:

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Almacenamiento** → **Discos físicos** → **Configuración**.
Se mostrará la página **Configuración de discos físicos**.
2. En el menú desplegable **Controladora**, seleccione la controladora para ver las unidades SSD PCIe asociadas.
3. En los menús desplegables, seleccione **Borrado seguro** para una o varias unidades SSD PCIe.
Si ha seleccionado **Borrado seguro** y desea ver las otras opciones en el menú desplegable, seleccione **Acción** y, a continuación, haga clic en el menú desplegable para ver las otras opciones.
4. En el menú desplegable **Aplicar modo de operación**, seleccione una de las siguientes opciones:
 - **Al siguiente reinicio**: seleccione esta opción para aplicar las acciones durante el siguiente reinicio del sistema. Esta es la opción predeterminada para las controladoras PERC 8.

- **A la hora programada:** seleccione esta opción para aplicar la acciones en un día y hora programados:
 - **Hora de inicio y Hora de finalización:** haga clic en los iconos de calendario y seleccione los días. Desde los menús desplegables, seleccione la hora. La acción se aplica entre la hora de inicio y la hora de finalización.
 - En el menú desplegable, seleccione el tipo de reinicio:
 - * Sin reinicio (se reinicia el sistema manualmente)
 - * Apagado ordenado
 - * Forzar apagado
 - * Realizar ciclo de encendido del sistema (reinicio mediante suministro de energía)

 **NOTA:** Para PERC 8 o controladoras anteriores, la opción **Apagado ordenado** es la opción predeterminada. Para controladoras PERC 9, **Sin reinicio (se reinicia el sistema manualmente)** es la opción predeterminada.

5. Haga clic en **Apply (Aplicar)**.

Si la tarea no se ha creado, aparecerá un mensaje indicando que el trabajo no se creó. El mensaje también muestra la identificación de mensaje y las acciones de respuesta recomendadas.

Si la tarea se ha creado correctamente, se mostrará un mensaje indicando que se ha creado el valor de ID de trabajo para la controladora seleccionada. Haga clic en **Cola de trabajos** para ver el progreso de ese trabajo en la página Cola de trabajos.

Si no se ha creado la operación pendiente, se mostrará un mensaje de error. Si la operación pendiente es exitosa y la creación de un trabajo no se ejecuta correctamente, se mostrará un mensaje de error.

Borrado de datos de un dispositivo SSD PCIe mediante RACADM

Para realizar un borrado seguro en un dispositivo SSD PCIe, ejecute el siguiente comando:

```
racadm storage secureerase:<PCIeSSD FQDD>
```

Para crear el trabajo de destino después de ejecutar el comando **secureerase**, ejecute el siguiente comando:

```
racadm jobqueue create <PCIe SSD FQDD> -s TIME_NOW --realtime
```

Para consultar el valor de ID de trabajo devuelto, ejecute el siguiente comando:

```
racadm jobqueue view -i <job ID>
```

Para obtener más información, consulte *iDRAC RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de iDRAC)* disponible en dell.com/esmanuals.

Administración de gabinetes o planos posteriores

Es posible realizar las siguientes tareas para los gabinetes o los planos posteriores:

- Ver propiedades
- Configurar el modo universal o el modo dividido
- Ver información de ranura (universal o compartida)
- Establecer el modo de SGPIO

Enlaces relacionados

[Resumen de funciones admitidas para Storage Devices \(Dispositivos de almacenamiento\)](#)

[Gabinetes admitidos](#)
[Configuración del modo de plano posterior](#)
[Visualización de ranuras universales](#)
[Configuración de modo de SGPIO](#)

Configuración del modo de plano posterior

Los servidores Dell PowerEdge de 13.ª generación admiten una nueva topología de almacenamiento interno, donde se pueden conectar dos controladoras de almacenamiento (PERC) a un conjunto de unidades internas a través de un único dispositivo expansor. Esta configuración se utiliza para el modo de alto rendimiento sin una funcionalidad de protección contra fallas o alta disponibilidad (HA). El expansor divide el arreglo de discos internos entre las dos controladoras de almacenamiento. En este modo, la creación de un disco virtual solo muestra las unidades conectadas a una controladora determinada. No existen requisitos de licencia para esta función. Esta función se admite únicamente en unos pocos sistemas.

El plano posterior admite dos modos:

- Modo unificado: la controladora PERC primaria obtiene acceso a todas las unidades conectadas al plano posterior, incluso si existe una segunda controladora PERC instalada.
- Modo dividido: una controladora obtiene acceso a las primeras 12 unidades y la segunda controladora obtiene acceso a las últimas 12 unidades. Esta separación no se puede configurar. Las unidades conectadas a la primera controladora se enumeran de 0 a 11, mientras que las unidades conectadas a la segunda controladora se enumeran de 12 a 23.

El valor predeterminado es el modo unificado.

iDRAC permite el valor de modo dividido si el expansor admite la configuración. Se recomienda activar este modo antes de instalar la segunda controladora. iDRAC realiza una comprobación de capacidad sobre el extensor antes de permitir que se configure este modo y no verifica la presencia de la segunda controladora PERC.

Para modificar la configuración, es necesario tener el privilegio de control del servidor.

Si alguna otra operación de RAID se muestra como pendiente o se programa un trabajo de RAID, no se puede cambiar el modo de plano posterior. De forma similar, si este valor se muestra pendiente, no es posible programar otros trabajos de RAID.

NOTA:

- Cuando se intenta modificar la configuración, se muestran mensajes de advertencia debido a la posibilidad de pérdida de datos.
- Una operación de eliminación de LC o restablecimiento de iDRAC no cambia la configuración de expansor para este modo.
- Esta operación solo se admite en tiempo real y no en etapas.

Todo cambio sobre esta configuración solamente se aplica después de un restablecimiento de la alimentación en el sistema. Al pasar de modo dividido a unificado, se mostrará un mensaje de error en el próximo inicio, ya que la segunda controladora no verá ninguna de las unidades. Además, la primera controladora verá una configuración ajena. Si se ignora el error, se perderán los discos virtuales existentes.

Configuración del modo de plano posterior mediante la interfaz web

Para configurar el modo de plano posterior mediante la interfaz web de iDRAC:

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Almacenamiento** → **Gabinetes** → **Configuración**.
Se mostrará la página **Configuración de gabinetes**.
2. En el menú desplegable **Controladora**, seleccione la controladora para configurar sus gabinetes asociados.
3. En la columna **Valor**, seleccione el modo requerido para el plano posterior o gabinete requerido:
 - Unificado
 - Dividido
4. En el menú desplegable **Aplicar modo de operación**, seleccione **Aplicar ahora** para aplicar las acciones inmediatamente y, a continuación, haga clic en **Aplicar**.
Se creará una identificación de trabajo.
5. Vaya a la página **Cola de trabajos** y compruebe que se muestre el estado Completado para el trabajo.
6. Realice un ciclo de encendido del sistema para que se aplique la configuración.

Configuración de un gabinete mediante RACADM

Para configurar el gabinete o el plano posterior, utilice el objeto `BackplaneMode` con el subcomando `set`.

Por ejemplo, para establecer el atributo `BackplaneMode` en el modo dividido:

1. En el símbolo del sistema RACADM, ejecute el siguiente comando para ver el modo de plano posterior actual:

```
get storage.enclosure.1.backplanecurrentmode
```

El resultado es:

```
BackplaneCurrentMode=UnifiedMode
```

2. Ejecute el siguiente comando para ver el modo solicitado:

```
get storage.enclosure.1.backplanerequestedmode
```

El resultado es:

```
BackplaneRequestedMode=None
```

3. Ejecute el siguiente comando para establecer el modo de plano posterior solicitado en el modo dividido:

```
set storage.enclosure.1.backplanerequestedmode "splitmode"
```

Se mostrará el mensaje de operación satisfactoria.

4. Ejecute el siguiente comando para verificar si el atributo `backplanerequestedmode` se ha establecido en el modo dividido:

```
get storage.enclosure.1.backplanerequestedmode
```

El resultado es:

```
BackplaneRequestedMode=None (Pending=SplitMode)
```

5. Ejecute el comando `storage get controllers` y anote el valor de ID de la instancia de la controladora.

6. Ejecute el siguiente comando para crear un trabajo:


```
jobqueue create <controller instance ID> -s TIME_NOW --realtime
```

Se devolverá una identificación de trabajo.
7. Ejecute el siguiente comando para consultar el estado del trabajo:


```
jobqueue view -i JID_XXXXXXXX
```

donde JID_XXXXXXXX es la identificación de trabajo del paso 6.

Se indicará el estado Pendiente.

Continúe consultando el valor de ID de trabajo hasta ver el estado Completado (este proceso puede tardar hasta tres minutos).
8. Ejecute el siguiente comando para ver el valor del atributo `backplanerequestedmode`:


```
get storage.enclosure.1.backplanerequestedmode
```

El resultado es:

```
BackplaneRequestedMode=SplitMode
```
9. Ejecute el siguiente comando para reiniciar mediante suministro de energía el servidor:


```
serveraction powercycle
```
10. Una vez que el sistema complete el proceso POST y CSIOR, escriba el siguiente comando para verificar el valor de `backplanerequestedmode`:


```
get storage.enclosure.1.backplanerequestedmode
```

El resultado es:

```
BackplaneRequestedMode=None
```
11. Ejecute el siguiente comando para verificar que el modo de plano posterior se haya establecido en el modo dividido:


```
get storage.enclosure.1.backplanecurrentmode
```

El resultado es:

```
BackplaneCurrentMode=SplitMode
```
12. Ejecute el siguiente comando y verifique que solo se muestren las unidades 0-11:


```
storage get pdisks
```

Para obtener más información sobre el comando `racadm`, consulte *iDRAC8 RACADM Command Line Interface Reference Guide (Guía de referencia de la interfaz de línea de comandos RACADM de iDRAC8)* disponible en dell.com/support/manuals.


Visualización de ranuras universales

Algunos de los planos posteriores de servidores PowerEdge de 13.^a generación admiten unidades SAS/SATA y unidades SSD PCIe en la misma ranura. Estas ranuras se conectan por cable a la controladora de almacenamiento primaria (PERC) y a una tarjeta de extensión PCIe. Estas ranuras se llaman "universales". El firmware del plano posterior proporciona información sobre las ranuras que admiten esta función. El plano posterior admite discos SAS/SATA o SSD PCIe. Por lo general, las cuatro ranuras con el número más alto son universales. Por ejemplo, si un plano posterior universal admite 24 ranuras, las ranuras de la 0 a la 19 solo admiten discos SAS/SATA mientras que las ranuras de la 20 a la 23 admiten SAS/SATA o SSD PCIe.

El estado de condición de recopilación para el gabinete proporciona el estado de condición combinado de todas las unidades en el gabinete. El vínculo para el gabinete en la página **Topología** muestra toda la información del gabinete, independientemente de la controladora a la que se encuentre asociado. Como es posible conectar dos controladoras de almacenamiento (PERC y extensión PCIe) al mismo plano posterior, solamente el plano posterior asociado con la controladora PERC aparece en la página **Inventario del sistema**.

En la página **Almacenamiento** → **Gabinetes** → **Propiedades**, la sección **Descripción general de los discos físicos** muestra lo siguiente:

- Si una ranura se encuentra vacía, se muestra **Ranura vacía** para la ranura.
- Si no existe ninguna ranura con capacidad PCIe, no se muestra la columna **Admite PCIe**.
- Si se trata de un plano posterior universal con SSD PCIe en una de las ranuras, la columna **Protocolo de bus** muestra el valor **PCIe**.
- La columna **Repuesto dinámico** no se aplica a SSD PCIe.

 **NOTA:** El intercambio directo es compatible con las ranuras universales. Si desea eliminar una unidad SSD PCIe y cambiarla por una unidad SAS/SATA, asegúrese de completar primero la tarea PrepareToRemove para la unidad SSD PCIe. Si no lleva a cabo esta tarea, el sistema operativo host puede presentar problemas como una pantalla azul, un aviso importante de núcleo, etc.

Configuración de modo de SGPIO


La controladora de almacenamiento se puede conectar al plano posterior en el modo I2C (valor predeterminado para planos posteriores Dell) o el modo de entrada/salida en serie de uso general (SGPIO). Esta conexión es necesaria para el parpadeo de LED en las unidades. Tanto las controladoras PERC como el plano posterior de Dell admiten estos modos. Para admitir ciertos adaptadores de canal, el modo de plano posterior debe ser cambiado al modo de SGPIO.

El modo de SGPIO solamente es compatible con los planos posteriores pasivos. No se admite en planos posteriores basados en expansor o planos posteriores pasivos en modo descendente. El firmware del plano posterior proporciona información acerca de la capacidad, del estado actual y del estado solicitado.

Después de una operación de eliminación de LC o un restablecimiento de iDRAC a los valores predeterminados, el modo de SGPIO se restablece a un estado desactivado. Se compara la configuración de iDRAC con la configuración del plano posterior. Si el plano posterior se ha establecido en el modo de SGPIO, iDRAC cambia su configuración para que coincida con la configuración del plano posterior.

Se requiere un ciclo de encendido del servidor para que se implementen los cambios en la configuración.

Es necesario tener el privilegio de control del servidor para modificar este valor.

 **NOTA:** No se puede establecer el modo de SGPIO mediante la interfaz web de iDRAC.

Configuración del modo de SGPIO mediante RACADM

Para configurar el modo de SGPIO, utilice el objeto **SGPIOMode** con el subcomando **set**. Si el objeto se establece en desactivado, se usa el modo I2C. Si se establece en activado, se usa el modo de SGPIO. Para obtener más información, consulte *iDRAC RACADM Command Line Interface Reference Guide (Guía de referencia de la interfaz de línea de comandos RACADM de iDRAC)* disponible en dell.com/support/manuals.


Elección de modo de operación para aplicar configuración

Durante la creación y la administración de discos virtuales, la configuración de discos físicos, controladoras y gabinetes o el restablecimiento de controladoras, antes de aplicar los distintos valores, se debe seleccionar el modo de operación. Es decir, se debe especificar el momento en que se desea aplicar la configuración:

- Inmediatamente
- Durante el siguiente reinicio del sistema
- En un tiempo programado
- Como una operación pendiente que se aplique como un lote como parte de un único trabajo

Elección del modo de operación mediante la interfaz web

Para seleccionar el modo de operación para aplicar la configuración:

1. Se puede seleccionar el modo de operación al estar en alguna de las páginas siguientes:
 - **Descripción general** → **Almacenamiento** → **Discos físicos** → **Configuración**.
 - **Descripción general** → **Almacenamiento** → **Discos virtuales** → **Crear**
 - **Descripción general** → **Almacenamiento** → **Discos virtuales** → **Administrar**
 - **Descripción general** → **Almacenamiento** → **Controladoras** → **Configuración**
 - **Descripción general** → **Almacenamiento** → **Controladoras** → **Solución de problemas**
 - **Descripción general** → **Almacenamiento** → **Gabinetes** → **Configuración**
 - **Descripción general** → **Almacenamiento** → **Operaciones pendientes**
 2. Seleccione una de las siguientes opciones en el menú desplegable **Aplicar modo de operación**:
 - **Aplicar ahora**: seleccione esta opción para aplicar la configuración de manera inmediata. Esta opción está disponible para las controladoras PERC 9 solamente. Si existen trabajos que se deben llevar a cabo, esta opción se muestra en gris. Esta tarea demorará al menos 2 minutos en completarse.
 - **Al siguiente reinicio**: seleccione esta opción para aplicar la configuración durante el siguiente reinicio del sistema. Esta es la opción predeterminada para las controladoras PERC 8.
 - **A la hora programada**: seleccione esta opción para aplicar la configuración en un día y una hora programados:
 - **Hora de inicio y Hora de finalización**: haga clic en los iconos de calendario y seleccione los días. En los menús desplegables, seleccione la hora. La configuración se aplicará entre la hora de inicio y la hora de finalización.
 - En el menú desplegable, seleccione el tipo de reinicio:
 - * Sin reinicio (se reinicia el sistema manualmente)
 - * Apagado ordenado
 - * Forzar apagado
 - * Realizar ciclo de encendido del sistema (reinicio mediante suministro de energía)
-  **NOTA:** Para PERC 8 o controladoras anteriores, la opción **Apagado ordenado** es la opción predeterminada. Para controladoras PERC 9, **Sin reinicio (se reinicia el sistema manualmente)** es la opción predeterminada.

- **Agregar a operaciones pendientes:** seleccione esta opción para crear una operación pendiente para aplicar la configuración. Todas las operaciones pendientes de una controladora se pueden ver en la página **Descripción general** → **Almacenamiento** → **Operaciones pendientes**.

 **NOTA:**

- La opción **Agregar a operaciones pendientes** no es aplicable para la página **Operaciones pendientes** ni para los dispositivos SSD PCIe en la página **Discos físicos** → **Configuración**.
- Solo la opción **Aplicar ahora** se encuentra disponible en la página **Configuración de gabinete**.

3. Haga clic en **Apply (Aplicar)**.

Según el modo de operación seleccionado, se aplicará la configuración.

Elección del modo de operación mediante RACADM

Utile el subcomando `jobjqueue` para seleccionar el modo de operación. Para obtener más información, consulte *iDRAC RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de iDRAC)* disponible en dell.com/esmanuals.

Visualización y aplicación de operaciones pendientes

Es posible ver y confirmar todas las operaciones pendientes de la controladora de almacenamiento. Todos los valores se aplicarán a la vez, durante el siguiente reinicio o a una hora programada en función de las opciones seleccionadas. Es posible eliminar todas las operaciones pendientes para una controladora. No se pueden eliminar operaciones pendientes individuales.

Las operaciones pendientes se crean en los componentes seleccionados (controladoras, gabinetes, discos físicos y discos virtuales).

Los trabajos de configuración se crean únicamente en la controladora. En el caso de SSD PCIe, el trabajo se crea en el disco SSD PCIe y no en la extensión PCIe.

Visualización, aplicación o eliminación de operaciones pendientes mediante la interfaz web

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Almacenamiento** → **Operaciones pendientes**.
Se mostrará la página **Operaciones pendientes**.
2. En el menú desplegable **Componente**, seleccione la controladora en la que desea ver, asignar o eliminar operaciones pendientes.
Se mostrará la lista de operaciones pendientes para la controladora seleccionada.

 **NOTA:**

- Se crean operaciones pendientes para importar la configuración ajena, borrar la configuración ajena, operaciones de clave de seguridad y cifrar discos virtuales. Sin embargo, no se muestran en la página **Operaciones pendientes** ni en el mensaje emergente **Operaciones pendientes**.
 - Los trabajos para SSD PCIe no se pueden crear desde la página **Operaciones pendientes**.
3. Para eliminar las operaciones pendientes en la controladora seleccionada, haga clic en **Eliminar todas las operaciones pendientes**.
 4. En el menú desplegable, seleccione una de las opciones siguientes y haga clic en **Aplicar** para confirmar la pendiente operaciones:

- **Aplicar ahora:** seleccione esta opción para confirmar todas las operaciones inmediatamente. Esta opción está disponible para las controladoras PERC 9 con las últimas versiones de firmware.
- **En el siguiente reinicio:** seleccione esta opción para confirmar todas las operaciones durante el siguiente reinicio del sistema. Esta es la opción predeterminada para las controladoras PERC 8. Esta opción se aplica a PERC 8 y las versiones posteriores.
- **A la hora programada:** seleccione esta opción para confirmar las operaciones en un día y una hora programados. Esta opción se aplica a PERC 8 y las versiones posteriores.
 - **Hora de inicio y Hora de finalización:** haga clic en los iconos de calendario y seleccione los días. Desde los menús desplegables, seleccione la hora. La acción se aplica entre la hora de inicio y la hora de finalización.
 - En el menú desplegable, seleccione el tipo de reinicio:
 - * Sin reinicio (se reinicia el sistema manualmente)
 - * Apagado ordenado
 - * Forzar apagado
 - * Realizar ciclo de encendido del sistema (reinicio mediante suministro de energía)



NOTA: Para PERC 8 o controladoras anteriores, la opción **Apagado ordenado** es la opción predeterminada. Para controladoras PERC 9, **Sin reinicio (se reinicia el sistema manualmente)** es la opción predeterminada.

5. Si el trabajo de confirmación no se ha creado, aparecerá un mensaje indicando que la creación de trabajos no se completó correctamente. El mensaje también muestra la identificación de mensaje y las acciones de respuesta recomendadas.
6. Si el trabajo de confirmación no se ha creado, se mostrará un mensaje indicando que no se creó la identificación de trabajo para la controladora seleccionada. Haga clic en **Cola de trabajos** para ver el progreso del trabajo en la página **Cola de trabajos**.
Si las operaciones para borrar la configuración ajena, importar la configuración ajena, usar la clave de seguridad o cifrar el disco virtual se encuentran en estado pendiente, y si estas son las únicas operaciones pendientes, no se podrá crear un trabajo desde la página **Operaciones pendientes**. Es necesario realizar otra operación de configuración de almacenamiento o usar el comando RACADM o WSMAN para crear el trabajo de configuración requerido en la controladora requerida.
No se pueden ver ni borrar operaciones pendientes para SSD PCIe en la página **Operaciones pendientes**. Utilice el comando racadm para borrar todas las operaciones pendientes en SSD PCIe.

Visualización y aplicación de operaciones pendientes mediante RACADM

Utilice el subcomando **jobqueue** para aplicar las operaciones pendientes. Para obtener más información, consulte *iDRAC RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de iDRAC)* disponible en dell.com/esmanuals.

Situaciones de almacenamiento: situaciones de aplicación de la operación

Caso 1: se seleccionó una operación de aplicación (Aplicar ahora, En el siguiente reinicio, o A la hora programada) y no hay operaciones pendientes existentes

Si seleccionó la opción **Aplicar ahora**, **En el siguiente reinicio** o **A la hora programada** y, a continuación, hizo clic en **Aplicar**, primero se crea la operación pendiente para la operación de configuración del almacenamiento seleccionada.

- Si la operación pendiente se realiza correctamente y no existen operaciones pendientes anteriores, se crea el trabajo. Si el trabajo se creó correctamente, aparece un mensaje que indica que se ha creado la Id. de trabajo para el dispositivo seleccionado. Haga clic en **Cola de trabajo en espera** para ver el progreso del trabajo en la página **Cola de trabajo en espera**. Si el trabajo no se creó, aparecerá un mensaje indicando que el trabajo no pudo crearse. También se muestra la identificación del mensaje y la acción de respuesta recomendada.
- Si la operación pendiente no se crea correctamente y no hay operaciones pendientes anteriores, aparecerá un mensaje de error con la Id. y la acción de respuesta recomendada.

Caso 2: se seleccionó una operación de aplicación (Aplicar ahora, En el siguiente reinicio o A la hora programada) y existen operaciones pendientes

Si seleccionó la opción **Aplicar ahora, En el siguiente reinicio o A la hora programada** y, a continuación, hizo clic en **Aplicar**, primero se crea la operación pendiente para la operación de configuración del almacenamiento seleccionada.

- Si la operación pendiente se creó correctamente y hay operaciones pendientes, aparecerá un mensaje.
 - Haga clic en el vínculo **Ver operaciones pendientes** para ver las operaciones pendientes para el dispositivo.
 - Haga clic en **Crear trabajo** para crear el trabajo para el dispositivo seleccionado. Si el trabajo se creó correctamente, aparece un mensaje que indica que se ha creado la Id. de trabajo para el dispositivo seleccionado. Haga clic en **Cola de trabajo en espera** para ver el progreso del trabajo en la página **Cola de trabajo en espera**. Si el trabajo no se creó, aparecerá un mensaje indicando que el trabajo no pudo crearse. También se mostrará la Id. del mensaje y la acción de respuesta recomendada.
 - Haga clic en **Cancelar** para no crear el trabajo y permanecer en la página para realizar más operaciones de configuración del almacenamiento.
- Si la operación pendiente no se crea correctamente y hay operaciones pendientes, aparecerá un mensaje de error.
 - Haga clic en **Operaciones pendientes** para ver las operaciones pendientes para el dispositivo.
 - Haga clic en **Crear trabajo para operaciones correctas** para crear el trabajo para las operaciones pendientes existentes. Si el trabajo se creó correctamente, aparece un mensaje que indica que se ha creado la Id. de trabajo para el dispositivo seleccionado. Haga clic en **Cola de trabajo en espera** para ver el progreso del trabajo en la página **Cola de trabajo en espera**. Si el trabajo no se creó, aparecerá un mensaje indicando que el trabajo no se creó. También se mostrará la Id. del mensaje y la acción de respuesta recomendada.
 - Haga clic en **Cancelar** para no crear el trabajo y permanecer en la página para realizar más operaciones de configuración del almacenamiento.

Caso 3: se seleccionó Agregar a operaciones pendientes y no existen operaciones pendientes

Si seleccionó **Agregar a operaciones pendientes** y, a continuación, hizo clic en **Aplicar**, primero se crea la operación pendiente para la operación de configuración del almacenamiento seleccionada.

- Si la operación pendiente se creó correctamente y no existen operaciones pendientes, aparecerá un mensaje informativo:
 - Haga clic en **Aceptar** para permanecer en la página para realizar más operaciones de configuración del almacenamiento.
 - Haga clic en **Operaciones pendientes** para ver las operaciones pendientes para el dispositivo. Estas operaciones pendientes no se aplican hasta que se crea el trabajo en la controladora seleccionada.

- Si la operación pendiente no se crea correctamente y no existen operaciones pendientes, aparecerá un mensaje de error.

Caso 4: se seleccionó Agregar a operaciones pendientes y no existen operaciones pendientes anteriores

Si seleccionó **Agregar a operaciones pendientes** y, a continuación, hizo clic en **Aplicar**, primero se crea la operación pendiente para la operación de configuración del almacenamiento seleccionada.

- Si la operación pendiente se crea correctamente y si existen operaciones pendientes, aparecerá un mensaje informativo:
 - Haga clic en **Aceptar** para permanecer en la página para realizar más operaciones de configuración del almacenamiento.
 - Haga clic en **Operaciones pendientes** para ver las operaciones pendientes para el dispositivo.
- Si la operación pendiente no se crea correctamente y hay operaciones pendientes, aparecerá un mensaje de error.
 - Haga clic en **Aceptar** para permanecer en la página para realizar más operaciones de configuración del almacenamiento.
 - Haga clic en **Operaciones pendientes** para ver las operaciones pendientes para el dispositivo.

NOTA:


- En cualquier momento, si no aparece la opción para crear un trabajo en las páginas de configuración del almacenamiento, vaya a la página **Descripción general del almacenamiento** → **Operaciones pendientes** para ver las operaciones pendientes existentes y para crear el trabajo en la controladora correspondiente.
- Solo los casos 1 y 2 se aplican a SSD PCIe. No se pueden ver las operaciones pendientes para SSD PCIe; por consiguiente, la opción **Agregar a operaciones pendientes** no se encuentra disponible. Utilice el comando racadm para borrar todas las operaciones pendientes para SSD PCIe.

Forma de hacer parpadear o dejar de hacer parpadear LED de componentes

Es posible localizar un disco físico, una unidad de disco virtual y PCIe SSD dentro de un gabinete cuando se hace parpadear uno de los diodos emisores de luz (LED) en el disco.

Es necesario tener privilegios de inicio de sesión para hacer parpadear o dejar de hacer parpadear un LED.

La controladora debe ser compatible con la configuración en tiempo real. El soporte en tiempo real de esta función solo se encuentra disponible en el firmware PERC 9.1 y las versiones posteriores.

 **NOTA:** La opción para hacer parpadear o dejar de hacer parpadear no es compatible con los servidores sin plano posterior.

Forma de hacer parpadear o dejar de hacer parpadear LED de componentes mediante la interfaz web

Para hacer parpadear o dejar de hacer parpadear un LED de componente:

1. En la interfaz web de iDRAC, vaya a cualquiera de las siguientes páginas según su requisito:

- **Descripción general** → **Almacenamiento** → **Identificar**: se muestra la página **Identificar LED de componentes**, donde se puede hacer parpadear o dejar de hacer parpadear los discos físicos, los discos virtuales y los SSD PCIe.
 - **Descripción general** → **Almacenamiento** → **Discos físicos** → **Identificar**: se muestra la página **Identificar discos físicos**, donde se puede hacer parpadear o dejar de hacer parpadear los discos físicos y los SSD PCIe.
 - **Descripción general** → **Almacenamiento** → **Discos virtuales** → **Identificar**: se muestra la página **Identificar discos virtuales**, donde se pueden hacer parpadear o dejar de hacer parpadear los discos virtuales.
2. Si está en la página **Identificar LED de componente** :
 - Seleccione o anule la selección de LED de los componentes: seleccione la opción **Seleccionar/Deseleccionar todo** y haga clic en **Hacer parpadear** para iniciar el parpadeo de los LED del componente. De forma similar, haga clic en **Dejar de hacer parpadear** para detener el parpadeo de los LED de los componentes.
 - Seleccione o anule la selección de los LED de los componente individuales: seleccione uno o más componentes y haga clic en **Hacer parpadear** para iniciar el parpadeo del LED del componente seleccionado. De forma similar, haga clic en **Dejar de hacer parpadear** para detener el parpadeo de los LED del componente.
 3. Si se encuentra en la página **Identificar discos físicos**:
 - Seleccione o anule la selección de todas las unidades de disco físico o SSD PCIe: seleccione la opción **Seleccionar/Deseleccionar todo** y haga clic en **Hacer parpadear** para iniciar el parpadeo de todas las unidades de disco físico y los SSD PCIe. De forma similar, haga clic en **Dejar de hacer parpadear** para detener el parpadeo de los LED.
 - Seleccione o anule la selección de unidades de disco físico o SSD PCIe: seleccione una o más unidades de disco físico y haga clic en **Hacer parpadear** para iniciar el parpadeo de los LED para las unidades de disco físicas o los SSD PCIe. De forma similar, haga clic en **Dejar de hacer parpadear** para detener el parpadeo de los LED.
 4. Si se encuentra en la página **Identificar discos virtuales**:
 - Seleccione o anule la selección de todos los discos virtuales: seleccione la opción **Seleccionar/Deseleccionar todo** y haga clic en **Hacer parpadear** para iniciar el parpadeo de los LED para todos los discos virtuales. De forma similar, haga clic en **Dejar de hacer parpadear** para detener el parpadeo de los LED .
 - Seleccione o anule la selección de discos virtuales individuales: seleccione uno o más discos virtuales y haga clic en **Hacer parpadear** para iniciar el parpadeo de los LED de los discos virtuales. De forma similar, haga clic en **Dejar de hacer parpadear** para detener el parpadeo de los LED.

Si la operación de hacer parpadear o dejar de parpadear no es satisfactoria, se mostrarán mensajes de error.

Blinking or Unblinking Component LEDs Using RACADM

To blink or unblink component LEDs, use the following commands:

```
racadm storage blink:<PD FQDD, VD FQDD, or PCIe SSD FQDD>
```

```
racadm storage unblink:<PD FQDD, VD FQDD, or PCIe SSD FQDD>
```

For more information, see the *iDRAC RACADM Command Line Reference Guide* available at dell.com/esmmanuals.

Configuración y uso de la consola virtual

Puede utilizar la consola virtual para administrar un sistema remoto mediante el teclado, el video y el mouse de la estación de trabajo para controlar los dispositivos correspondientes en un servidor administrado. Esta función requiere licencia para los servidores tipo bastidor y torre y está disponible de manera predeterminada para los servidores Blade.

Las características claves son las siguientes:

- Se admite un máximo de seis sesiones de consola virtual simultáneas. Todas las sesiones visualizan la misma consola de servidor administrado a la vez.
- Puede iniciar la consola virtual en un explorador web compatible mediante un complemento Java o ActiveX. Debe utilizar el visor de Java si la estación de administración se ejecuta en un sistema operativo distinto de Windows.
- Al abrir una sesión de consola virtual, el servidor administrado no indica que la consola ha sido redirigida.
- Puede abrir varias sesiones de consola virtual desde una sola estación de administración a uno o más sistemas administrados de manera simultánea.
- No puede abrir dos sesiones de consola virtual desde la estación de administración al servidor administrado mediante el mismo complemento.
- Si otro usuario solicita una sesión de consola virtual, el primer usuario recibe una notificación y tendrá la opción de denegar el acceso, permitir un acceso de solo lectura o permitir un acceso de uso compartido completo. El segundo usuario recibe notificación de que el primer usuario tiene el control. El primer usuario debe responder dentro de un plazo de 30 segundos o el acceso se otorga al segundo usuario según la configuración predeterminada. Cuando haya dos sesiones activas simultáneamente, el primer usuario verá un mensaje en la esquina superior izquierda de la pantalla que el segundo usuario tiene una sesión activa. Si ni el primer usuario ni el segundo dispone de privilegios de administrador, la terminación de la sesión del primer usuario terminará automáticamente la sesión del segundo usuario.

Enlaces relacionados

[Configuración de exploradores web para usar la consola virtual](#)

[Configuración de la consola virtual](#)

[Inicio de la consola virtual](#)


Resoluciones de pantalla y velocidades de actualización admitidas

En la tabla siguiente se indican las resoluciones de pantalla admitidas y las velocidades de actualización para una sesión de consola virtual que se ejecuta en el servidor administrado.

Tabla 26. Resoluciones de pantalla y velocidades de actualización admitidas

| Resolución de pantalla | Velocidad de actualización (Hz) |
|------------------------|---------------------------------|
| 720x400 | 70 |
| 640x480 | 60, 72, 75, 85 |
| 800x600 | 60, 70, 72, 75, 85 |
| 1024x768 | 60, 70, 72, 75, 85 |
| 1280x1024 | 60 |


Se recomienda configurar la resolución del monitor en 1280x1024 píxeles o más.

 **NOTA:** Si hay una sesión de consola virtual activa y se conecta un monitor de menor resolución a la consola virtual, la resolución de la consola de servidor podría restablecerse si el servidor se selecciona en la consola local. Si el sistema ejecuta el sistema operativo Linux, es posible que una consola X11 no pueda visualizarse en el monitor local. Presione <Ctrl><Alt><F1> en la consola virtual de iDRAC para cambiar Linux a una consola de texto.

Configuración de exploradores web para usar la consola virtual

Para utilizar la consola virtual en la estación de administración:

1. Asegúrese de tener instalada una versión de explorador compatible [Internet Explorer (Windows) o Mozilla Firefox (Windows o Linux), Google Chrome, Safari].
Para obtener más información sobre las versiones de exploradores compatibles, consulte el archivo *Léame* disponible en dell.com/support/manuals.
2. Para utilizar Internet Explorer, establezca IE en **Ejecutar como administrador**.
3. Configure el explorador web para que utilice el complemento ActiveX o Java.
El visor de ActiveX solo se admite con Internet Explorer. Un visor de Java se admite en cualquier explorador.
4. Importe los certificados raíz en el sistema administrado para evitar las ventanas emergentes que solicita la verificación de los certificados.
5. Instale el paquete **compat-libstdc++-33-3.2.3-61**.

 **NOTA:** En Windows, el paquete relacionado "compat-libstdc++-33-3.2.3-61" puede incluirse en el paquete de .NET Framework o el paquete de sistema operativo.

6. Si utiliza un sistema operativo MAC, seleccione la opción **Activar acceso para dispositivos de asistencia** en la ventana **Acceso universal**.

Para obtener más información, consulte la documentación del sistema operativo MAC.

Enlaces relacionados


[Configuración de exploradores web para usar el complemento Java](#)

[Configuración de IE para usar el complemento ActiveX](#)

[Importación de certificados de CA a Management Station](#)

Configuración de exploradores web para usar el complemento Java

Instale Java Runtime Environment (JRE) si utiliza Firefox o IE y desea utilizar el visor de Java.

 **NOTA:** Instale una versión de 32 bits o de 64 bits de JRE en un sistema operativo de 64 bits o una versión de 32 bits de JRE en un sistema operativo de 32 bits.

Para configurar IE para utilizar el complemento Java:

- Desactive la solicitud automática de descargas de archivo en Internet Explorer.
- Desactive la opción *Modo de seguridad mejorado* en Internet Explorer.

Enlaces relacionados

[Configuración de la consola virtual](#)

Configuración de IE para usar el complemento ActiveX


Es necesario configurar los valores para el explorador IE antes de iniciar y ejecutar la consola virtual basada en ActiveX y las aplicaciones de medios virtuales. Las aplicaciones de ActiveX se proporcionan como archivos CAB firmados desde el servidor de iDRAC. Si el tipo de complemento se establece en ActiveX nativo en la consola virtual, cuando se intente iniciar la consola virtual, se descargará el archivo CAB en el sistema cliente y se iniciará la consola virtual basada en ActiveX. Internet Explorer requiere algunas configuraciones para descargar, instalar y ejecutar estas aplicaciones basadas en ActiveX.

Internet Explorer se encuentra disponible en exploradores con versiones de 32 bits y de 64 bits. Se puede utilizar cualquier versión, pero si se instala el complemento en el explorador web de 64 bits y, a continuación, se intenta ejecutar el visor en un explorador de 32 bits, será necesario volver a instalar el complemento.

 **NOTA:** El complemento ActiveX solo se puede utilizar con Internet Explorer.

Para aplicaciones de ActiveX en Windows 2003, Windows XP, Windows Vista, Windows 7 y Windows 2008, configure los siguientes valores de IE para utilizar el complemento ActiveX:

1. Borre la memoria caché del explorador.
2. Agregue la dirección IP o el nombre de host de iDRAC IP a la lista **Sitios de confianza**.
3. Restablezca la configuración personaliza en **Medio-bajo** o cambie los valores para permitir la instalación de complementos ActiveX firmados.
4. Active el explorador para descargar contenido cifrado y activar las extensiones de explorador de terceros. Para ello, vaya a **Herramientas** → **Opciones de Internet** → **Opciones avanzadas**, desactive la opción **No guardar las páginas cifradas en el disco** y active la opción **Habilitar extensiones de explorador de terceros**.

 **NOTA:** Reinicie Internet Explorer para que la opción Habilitar las extensiones de explorador de terceros surta efecto.

5. Vaya a **Herramientas** → **Opciones de Internet** → **Seguridad** y seleccione la zona en la que desee ejecutar la aplicación.
6. Haga clic en **Nivel personalizado**. En la ventana **Configuración de seguridad**, realice lo siguiente:
 - Seleccione **Activar** para **Preguntar automáticamente si se debe usar un control ActiveX**.
 - Seleccione **Preguntar** para **Descargar los controles ActiveX firmados**.
 - Seleccione **Habilitar** o **Preguntar** para **Ejecutar controles y complementos de ActiveX**.

- Seleccione **Habilitar** o **Preguntar** para **Generar scripts de los controles ActiveX marcados como seguros para scripts**.
7. Haga clic en **Aceptar** para cerrar la ventana **Configuración de seguridad**.
 8. Haga clic en **Aceptar** para cerrar la ventana **Opciones de Internet**.

 **NOTA:**

- Las diferentes versiones de Internet Explorer comparten el mismo componente **Opciones de Internet**. Por lo tanto, después de agregar el servidor a la lista de *sitios de confianza* para un explorador, el otro explorador utilizará la misma configuración.
- Antes de instalar el control ActiveX, Internet Explorer puede mostrar una advertencia de seguridad. Para completar el procedimiento de instalación de control ActiveX, acepte este último cuando Internet Explorer muestre una advertencia de seguridad.

Enlaces relacionados

[Borrado de la caché del explorador](#)

[Valores adicionales para los sistemas operativos de Microsoft Windows Vista o más recientes](#)

Valores adicionales para los sistemas operativos de Microsoft Windows Vista o más recientes

Los exploradores Internet Explorer en los sistemas operativos Windows Vista o más recientes tienen una función de seguridad adicional denominada *Modo protegido*.

Para iniciar y ejecutar aplicaciones ActiveX en los exploradores Internet Explorer con la función *Modo protegido*:

1. Ejecute IE como administrador.
2. Vaya a **Herramientas** → **Opciones de Internet** → **Seguridad** → **Sitios de confianza**.
3. Asegúrese de que la opción **Habilitar modo protegido** está desactivada para la zona Sitios de confianza. También puede agregar la dirección de iDRAC a los sitios de la zona Intranet. De manera predeterminada, el modo protegido está desactivado para los sitios de la zona Intranet y los sitios de la zona Sitios de confianza.
4. Haga clic en **Sitios**.
5. En el campo **Agregar este sitio web a la zona**, agregue la dirección de iDRAC y haga clic en **Agregar**.
6. Haga clic en **Cerrar** y, a continuación, en **Aceptar**.
7. Cierre y reinicie el explorador para que la configuración tenga efecto.

Borrado de la caché del explorador

Si tiene problemas para usar la consola virtual (errores de fuera de rango, problemas de sincronización, etc.) borre la caché del explorador para quitar o eliminar las versiones anteriores del visor que pudieran estar almacenadas en el sistema e inténtelo nuevamente.

 **NOTA:** Debe tener privilegios de administrador para borrar la caché del explorador.

Borrado de versiones anteriores de ActiveX en IE7

Para borrar versiones anteriores del visor de Active-X para IE7, realice lo siguiente:

1. Cierre Video Viewer y el explorador de Internet Explorer.
2. Vuelva a abrir Internet Explorer y vaya a **Internet Explorer** → **Herramientas** → **Administrar complementos** y haga clic en **Activar o desactivar complementos**. Se mostrará la ventana **Administrar complementos**.
3. Seleccione **Complementos utilizados por Internet Explorer** en el menú desplegable **Mostrar**.
4. Elimine el complemento *Video Viewer*.

Borrado de versiones anteriores de ActiveX en IE8

Para limpiar las versiones anteriores del visor Active-X para IE8, realice lo siguiente:

1. Cierre Video Viewer y el explorador de Internet Explorer.
2. Vuelva a abrir Internet Explorer y vaya a **Internet Explorer** → **Herramientas** → **Administrar complementos** y haga clic en **Activar o desactivar complementos**. Se mostrará la ventana **Administrar complementos**.
3. Seleccione **Todos los complementos** en el menú desplegable **Mostrar**.
4. Seleccione el complemento *Video Viewer* y haga clic en el vínculo **Más información**.
5. Seleccione **Quitar** de la ventana **Más información**.
6. Cierre las ventanas **Más información** y **Administrar complementos**.

Borrado de versiones anteriores de Java

Para borrar las versiones anteriores del visor de Java en Windows o Linux, haga lo siguiente:

1. En el indicador de comandos, ejecute `javaws-viewer` o `javaws-uninstall`.
Aparece el **Visor de la caché de Java**.
2. Elimine los elementos con el título *Cliente de consola virtual de iDRAC*.

Importación de certificados de CA a Management Station

Al iniciar la consola virtual o los medios virtuales, aparecen peticiones para verificar los certificados. Si hay certificados de servidor web personalizados, puede evitar estas peticiones importando los certificados de CA al almacén de certificados de confianza de Java o ActiveX.

Enlaces relacionados

[Importación de certificados de CA al almacén de certificados de confianza de Java](#)

[Importación de certificados de CA al almacén de certificados de confianza de ActiveX](#)

Importación de certificados de CA al almacén de certificados de confianza de Java

Para importar el certificado de CA al almacén de certificados de confianza de Java:

1. Inicie el **Panel de control de Java**.
2. Seleccione la ficha **Seguridad** y haga clic en **Certificados**.
Se muestra el cuadro de diálogo **Certificados**.
3. En el menú desplegable Tipo de certificado, seleccione **Certificados de confianza**.
4. Haga clic en **Importar**, seleccione el certificado de CA (en formato de codificación Base64) y haga clic en **Abrir**.
El certificado seleccionado se importa al almacén de certificados de confianza de inicio web.
5. Haga clic en **Cerrar** y, a continuación, en **Aceptar**. Se cerrará la ventana **Panel de control de Java**.

Importación de certificados de CA al almacén de certificados de confianza de ActiveX

Debe utilizar la herramienta de línea de comandos OpenSSL para crear el hash del certificado mediante el algoritmo Hash seguro (SHA). Es recomendable utilizar la herramienta OpenSSL 1.0.x o una versión posterior, ya que esta utiliza SHA de manera predeterminada. El certificado de CA debe estar codificado en formato PEM Base64. Este es un proceso único que se debe realizar para importar cada certificado CA.

Para importar el certificado de CA al almacén de certificados de confianza de ActiveX:

1. Abra el símbolo del sistema de OpenSSL.
2. Ejecute un Hash de 8 bytes en el certificado de CA que se esté utilizando en la estación de administración mediante el comando: `openssl x509 -in (name of CA cert) -noout -hash`
Se generará un archivo de salida. Por ejemplo, si el nombre de archivo del certificado de CA es **cacert.pem**, es comando será:

```
openssl x509 -in cacert.pem -noout -hash
```


Se genera una salida similar a "431db322".
3. Cambie el nombre del archivo de CA al nombre de archivo de salida e incluya una extensión ".0". Por ejemplo, 431db322.0.
4. Copie el certificado de CA con el nombre nuevo en el directorio de inicio. Por ejemplo, el directorio **C:\Documents and Settings\<usuario>**.

Configuración de la consola virtual

Antes de configurar la consola virtual, asegúrese de que esté configurada la estación de administración.

Es posible configurar la consola virtual mediante la interfaz web de iDRAC o la interfaz de línea de comandos RACADM.

Enlaces relacionados

[Configuración de exploradores web para usar la consola virtual](#)

[Inicio de la consola virtual](#)

Configuración de la consola virtual mediante la interfaz web

Para configurar la consola virtual mediante la interfaz web de iDRAC:

1. Vaya a **Descripción general** → **Servidor** → **Consola virtual**. Aparece la página **Consola virtual**.
2. Active la consola virtual y especifique los valores necesarios. Para obtener más información acerca de estas opciones, consulte la *Ayuda en línea de iDRAC*.
3. Haga clic en **Aplicar**. Se configura la consola virtual.

Configuración de la consola virtual mediante RACADM


Para configurar la consola virtual, utilice una de las siguientes opciones:

- Utilice los objetos del grupo **iDRAC.VirtualConsole** con el comando **set**.
- Utilice los objetos siguientes con el comando **config**:
 - `cfgRACTuneConRedirEnable`
 - `cfgRACTuneConRedirPort`
 - `cfgRACTuneConRedirEncryptEnable`
 - `cfgRacTunePluginType`
 - `cfgRacTuneVirtualConsoleAuthorizeMultipleSessions`

Para obtener más información sobre estos objetos, consulte *iDRAC8 RACADM Command Line Interface Reference Guide (Guía de referencia de la interfaz de línea de comandos RACADM de iDRAC8)* disponible en dell.com/support/manuals.


Vista previa de la consola virtual

Antes de iniciar la consola virtual, puede obtener una vista previa del estado de la misma en la página **Sistema** → **Propiedades** → **Resumen del sistema**. En la sección **Vista previa de la consola virtual** se muestra una imagen que indica el estado de la consola. La imagen se actualiza cada 30 segundos. Esta función requiere una licencia.

 **NOTA:** La imagen de la consola virtual está disponible únicamente si se ha activado la consola virtual.


Inicio de la consola virtual

Es posible iniciar la consola virtual mediante la interfaz web de iDRAC o un URL:

 **NOTA:** No inicie la sesión de consola virtual desde un explorador web del sistema administrado.

Antes de iniciar la consola virtual, asegúrese de lo siguiente:

- Dispone de privilegios de administrador.
- El explorador web está configurado para utilizar los complementos Java o ActiveX.
- Hay un ancho de banda de red mínimo de 1 MB/seg.

 **NOTA:** Si la controladora de vídeo integrada se desactiva en el BIOS e inicia la consola virtual, el visor de la consola virtual aparece en blanco.

Cuando se inicia la consola virtual mediante exploradores de IE de 32 o 64 bits, el complemento necesario (Java o ActiveX) está disponible en el explorador correspondiente. Las opciones de Internet son comunes a ambos exploradores.

Cuando se inicia la consola virtual mediante el complemento Java, es posible que de vez en cuando se produzca un error de compilación Java. Para resolver este problema, vaya a **Panel de control de Java** → **General** → **Configuración de la red** y seleccione **Conexión directa**.

Si la consola virtual está configurada para utilizar el complemento ActiveX, es posible que la primera vez no se inicie. Esto se debe a una conexión de red lenta y a un tiempo de espera de las credenciales temporales (que la consola virtual utiliza para conectarse) es de dos minutos. El tiempo de descarga del complemento del cliente ActiveX puede superar este tiempo. Una vez que el complemento se haya descargado correctamente, podrá iniciar la consola virtual con normalidad.

Cuando inicia la consola virtual por primera vez mediante IE8 con el complemento ActiveX, es posible que aparezca el mensaje "Certificate Error: Navigation Blocked". Haga clic en **Seguir a este sitio web** y, a continuación, en **Instalar** para instalar los controles ActiveX en la ventana **Advertencia de seguridad**. Se iniciará la sesión de consola virtual.

Enlaces relacionados

[Inicio de la consola virtual mediante URL](#)

[Configuración de exploradores web para usar el complemento Java](#)

[Configuración de IE para usar el complemento ActiveX](#)

[Inicio de la consola virtual mediante la interfaz web](#)

[Desactivación de mensajes de advertencia mientras se inicia la consola virtual o los medios virtuales mediante el complemento de Java o ActiveX](#)
[Sincronización de los punteros del mouse](#)

Inicio de la consola virtual mediante la interfaz web

Puede iniciar la consola virtual de las maneras siguientes:

- Vaya a **Descripción general** → **Servidor** → **Consola virtual**. Aparece la página **Consola virtual**. Haga clic en **Iniciar consola virtual**. Se inicia el **Visor de la consola virtual**.
- Vaya a **Descripción general** → **Servidor** → **Propiedades**. Aparece la página **Resumen del sistema**. En **Vista previa de la consola virtual**, haga clic en **Iniciar**. Se inicia el **Visor de la consola virtual**.

En el **Visor de la consola virtual** se muestra el escritorio del sistema remoto. Utilice este visor para controlar las funciones del mouse y el teclado del sistema remoto desde la estación de administración.

Es posible que aparezcan varios cuadros de mensajes después de iniciar la aplicación. Para evitar un acceso no autorizado a la aplicación, desplácese por estos cuadros de mensaje dentro de un plazo de tres minutos. De lo contrario, se le solicitará que reinicie la aplicación.

Si aparecen una o más ventanas de alerta de seguridad mientras se inicia el visor, haga clic en Sí para continuar.

Es posible que aparezcan dos apuntadores del mouse en la ventana del visor: uno para el servidor administrado y otro para la estación de administración. Para sincronizar los cursores, consulte [Sincronización de los apuntadores del mouse](#).

Si se inicia la consola virtual desde una estación de administración con Windows Vista, es posible que aparezcan mensajes de reinicio de la consola virtual. Para evitar esta, establezca valores de tiempo de espera adecuados en las ubicaciones siguientes:

- **Panel de control** → **Opciones de energía** → **Ahorro de energía** → **Configuración avanzada** → **Disco duro** → **Apagar el disco duro después de <tiempo de espera>**
- **Panel de control** → **Opciones de energía** → **Alto rendimiento** → **Configuración avanzada** → **Disco duro** → **Apagar el disco duro después de <tiempo de espera>**


Inicio de la consola virtual mediante URL

Para iniciar la consola virtual mediante el URL:

1. Abra un explorador web compatible y, en el cuadro de dirección, escriba la siguiente URL en minúsculas: **https://iDRAC_ip/console**
2. Según la configuración de inicio de sesión, aparecerá la página **Inicio de sesión** correspondiente:
 - Si está desactivado el inicio de sesión único y está activado el inicio de sesión local, de Active Directory, de LDAP o mediante tarjeta inteligente, aparecerá la página **Inicio de sesión** correspondiente.
 - Si está activado el inicio de sesión único, se iniciará el **Visor de la consola virtual** y la página **Consola virtual** se muestra en segundo plano.





NOTA: Internet Explorer admite el inicio de sesión local, de Active Directory, de LDAP y mediante tarjeta inteligente (SC), así como el inicio de sesión único. Firefox admite el inicio de sesión local, de AD y SSO en sistemas operativos basados en Windows y el inicio de sesión local, de Active Directory y de LDAP en sistemas operativos basados en Linux.

 **NOTA:** Si no dispone de privilegios de acceso a la consola virtual, pero sí a los medios virtuales, al utilizar el URL se iniciarán los medios virtuales en lugar de la consola virtual.


Desactivación de mensajes de advertencia mientras se inicia la consola virtual o los medios virtuales mediante el complemento de Java o ActiveX

Puede desactivar los mensajes de advertencia mientras inicia la consola virtual o los medios virtuales mediante el complemento de Java.

1. Inicialmente, al iniciar la consola virtual o los medios virtuales mediante el complemento de Java, aparece el indicador para verificar el publicador. Haga clic en **Yes (Si)**.
Aparece un mensaje de advertencia de certificado que indica que no se ha encontrado un certificado de confianza.
 **NOTA:** Si el certificado se encuentra en el almacén de certificados del sistema operativo o en una ubicación especificada anteriormente por el usuario, este mensaje de advertencia no se muestra.
2. Haga clic en **Continue (Continuar)**.
Se inicia el visor de la consola virtual o el visor de medios virtuales.
 **NOTA:** El visor de medios virtuales se inicia si la consola virtual está desactivada.
3. En el menú **Herramientas**, haga clic en **Opciones de sesión** y, a continuación, en la ficha **Certificado**.
4. Haga clic en **Examinar ruta de acceso**, especifique la ubicación para almacenar el certificado del usuario, haga clic en **Aplicar**, haga clic en **Aceptar** y salga del visor.
5. Inicie la consola virtual de nuevo.
6. En el mensaje de advertencia del certificado, seleccione la opción **Confiar siempre en este certificado** y, a continuación, haga clic en **Continuar**.
7. Salga del visor.
8. Cuando vuelva a iniciar la consola virtual, el mensaje de advertencia no aparecerá.

Uso del visor de la consola virtual

El visor de la consola virtual proporciona diversos controles como sincronización de mouse, ajuste de escala de la consola virtual, opciones de chat, macros para el teclado, acciones relacionadas con la alimentación, dispositivos para el siguiente inicio y acceso a medios virtuales. Para obtener información sobre cómo usar estas funciones, consulte *iDRAC Online Help* (Ayuda en línea de iDRAC).

 **NOTA:** Si el servidor remoto está apagado, se mostrará el mensaje "Sin señal".

En la barra de título del visor de la consola virtual se muestra el nombre DNS y la dirección IP de un iDRAC al que el usuario se encuentra conectado desde Management Station. Si iDRAC no tiene un nombre DNS, se mostrará la dirección IP. El formato es el siguiente:

- Servidores tipo bastidor y torre:
<DNS name / IPv6 address / IPv4 address>, <Model>, User: <username>, <fps>
- Servidores Blade:
<DNS name / IPv6 address / IPv4 address>, <Model>, <Slot number>, User:
<username>, <fps>

A veces, el visor de la consola virtual puede mostrar video de baja calidad. Esto se debe a una conexión de red lenta que provoca la pérdida de uno o dos fotogramas al iniciar la sesión de consola virtual. Para transmitir todos los fotogramas y mejorar la calidad de video, realice cualquiera de las acciones siguientes:

- En la página **Resumen del sistema**, en la sección **Vista previa de la consola virtual**, haga clic en **Actualizar**.
- En el **Visor de la consola virtual**, en la ficha **Rendimiento**, establezca el control deslizante en **Calidad de video máxima**.

Sincronización de los punteros del mouse


Cuando se conecta a un sistema administrado a través de la consola virtual, es posible que la velocidad de aceleración del mouse del sistema administrado no se sincronice con el puntero del mouse de la estación de administración y que se muestren dos punteros del mouse en la ventana del visor.

Si utiliza Red Hat Enterprise Linux o Novell SUSE Linux, configure el modo de mouse para Linux antes de iniciar el visor de la consola virtual. La configuración predeterminada del sistema operativo se utiliza para controlar la flecha del mouse en el visor de la consola virtual.

Cuando se ven dos cursores de mouse en el visor de la consola virtual cliente, esto indica que el sistema operativo del servidor admite el posicionamiento relativo. Esto es típico para sistemas operativos Linux o Lifecycle Controller y genera dos cursores del mouse si los valores de aceleración del mouse del servidor son diferentes de los valores de aceleración del mouse en la consola virtual cliente. Para resolver esto, cambie a un cursor único o haga coincidir la aceleración del mouse en el sistema administrado y en la estación de administración:

- Para cambiar a un cursor único, en el menú **Herramientas**, seleccione **Cursor único**.
- Para establecer la aceleración del mouse, vaya a **Herramientas** → **Opciones de sesión** → **Mouse**. En la ficha **Aceleración del mouse**, seleccione **Windows** o **Linux** en función del sistema operativo.

Para salir del modo de cursor único, presione <Esc> o la tecla de terminación configurada.

 **NOTA:** Esto no se aplica a los sistemas administrados que ejecutan Windows, ya que estos admiten el posicionamiento absoluto.

Si se utiliza la consola virtual para conectarse a un sistema administrado con un sistema operativo de distribución Linux recientemente instalado, es posible que se produzcan problemas de sincronización con el mouse. Esto puede deberse a la función Aceleración previsible de puntero del escritorio GNOME. Para lograr una sincronización adecuada con el mouse en la consola virtual de iDRAC, se debe desactivar esta función. Para ello, en la sección de mouse en el archivo `/etc/X11/xorg.conf`, agregue lo siguiente:

```
Option "AccelerationScheme" "lightweight".
```

Si se siguen produciendo problemas de sincronización, realice el siguiente cambio adicional en el archivo `<inicio de usuario>/gconf/desktop/gnome/peripherals/mouse/%gconf.xml`:

Cambie los valores de `motion_threshold` y `motion_acceleration` a `-1`.

Si desactiva la aceleración del mouse en el escritorio GNOME, en el visor de la consola virtual, vaya a **Herramientas** → **Opciones de sesión** → **Mouse**. En la ficha **Aceleración del mouse**, seleccione **Ninguno**.

Para obtener un acceso exclusivo a la consola del servidor administrado, deberá desactivar la consola local y volver a configurar la opción **Sesiones máximas** en 1 en la **página Consola virtual**.

Pulsación de teclas a través de la consola virtual

Puede activar la opción **Pasar todas las pulsaciones de tecla al servidor** y enviar todas las pulsaciones de tecla y combinaciones de teclas desde la estación de administración al sistema administrado a través del visor de la consola virtual. Si está desactivada, dirige todas las combinaciones de teclas a la estación de administración en donde se ejecuta la sesión de la consola virtual. Para pasar todas las pulsaciones de tecla al servidor, en el visor de la consola virtual, vaya a la ficha **Herramientas** → **Opciones de sesión** → **General** y seleccione la opción **Pasar todas las pulsaciones de tecla al servidor** para pasar las pulsaciones de tecla de la estación de administración al sistema administrado.

El comportamiento de la función Pasar todas las pulsaciones de tecla al servidor depende de lo siguiente:

- Tipo de complemento (Java o ActiveX) según la sesión de consola virtual que se inicia.
En el cliente Java, se debe cargar la biblioteca nativa para que funcionen tanto la opción "Pasar todas las pulsaciones de tecla al servidor" como el modo de cursor único. Si no se cargan las bibliotecas nativas, se anula la selección de las opciones **Pasar todas las pulsaciones de tecla al servidor** y **Cursor único**. Si intenta seleccionar una de estas opciones, se mostrará un mensaje de error que indica que no se admiten las opciones seleccionadas.

En el cliente ActiveX, se debe cargar la biblioteca nativa para que funcione la opción "Pasar todas las pulsaciones de tecla al servidor". Si no se cargan las bibliotecas nativas, se anula la selección de la opción **Pasar todas las pulsaciones de tecla al servidor**. Si intenta seleccionar esta opción, se mostrará un mensaje de error que indica que no se admite la opción seleccionada.

En los sistemas operativos MAC, active la opción **Activar acceso de dispositivos de asistencia en Acceso universal** para que funcione la opción "Pasar todas las pulsaciones de tecla al servidor".

- El sistema operativo que se ejecuta en la estación de administración y el sistema administrado. Las combinaciones de teclas que son significativas para el sistema operativo de la estación de administración no se pasan al sistema administrado.
- El modo del visor de la consola virtual (ventana o pantalla completa).
En el modo de pantalla completa, la opción **Pasar todas las pulsaciones de tecla al servidor** está activada de manera predeterminada.

En el modo de ventana, las pulsaciones de teclas solo se pasan cuando el visor de la consola virtual es visible y está activo.

Cuando cambia del modo de pantalla completa al modo de ventana, se reanuda el estado anterior de la opción para pasar todas las pulsaciones de teclas.

Enlaces relacionados

[Sesión de consola virtual basada en Java que se ejecuta en el sistema operativo Windows](#)

[Sesión de consola virtual basada en Java que se ejecuta en el sistema operativo Linux](#)

[Sesión de consola virtual basada en ActiveX que se ejecuta en el sistema operativo Windows](#)

Sesión de consola virtual basada en Java que se ejecuta en el sistema operativo Windows

- La combinación de teclas Ctrl+Alt+Supr no se envía al sistema administrado pero siempre es interpretada por la estación de administración.
- Cuando está activada la opción Pasar todas las pulsaciones de teclas al servidor, las pulsaciones de teclas siguientes no se envían al sistema administrado:

- Tecla Atrás del explorador
- Tecla Adelante del explorador
- Tecla Actualizar del explorador
- Tecla Detener del explorador
- Tecla Buscar del explorador
- Tecla Favoritos del explorador
- Tecla Inicio y Página inicial del explorador
- Tecla de silencio de volumen
- Tecla de reducción de volumen
- Tecla de aumento de volumen
- Tecla de pista siguiente
- Tecla de pista anterior
- Tecla Detener medios
- Tecla Reproducir/pausar medios
- Tecla Iniciar correo
- Tecla Seleccionar medios
- Tecla Iniciar aplicación 1
- Tecla Iniciar aplicación 2
- Todas las teclas individuales (no una combinación de diferentes teclas, sino una pulsación única de tecla) siempre se envían al sistema administrado. Esto incluye todas las teclas de función, las teclas Mayús, Alt y Ctrl, y las teclas de menú. Algunas de estas teclas afectan tanto a la estación de administración como al sistema administrado.
 Por ejemplo, si la estación de administración y el sistema administrado ejecutan el sistema operativo Windows y la opción Pasar todas las pulsaciones de teclas está desactivada, al presionar la tecla Windows para abrir el menú **Inicio**, el menú **Inicio** se abrirá tanto en la estación de administración como en el sistema administrado. Sin embargo, si la opción Pasar todas las pulsaciones de teclas está activada, el menú **Inicio** se abrirá solamente en el sistema administrado y no en la estación de administración.
- Cuando la opción Pasar todas las pulsaciones de teclas está desactivada, el comportamiento depende en las combinaciones de teclas pulsadas y las combinaciones especiales que interprete el sistema operativo en la estación de administración.

Sesión de consola virtual basada en Java que se ejecuta en el sistema operativo Linux

El comportamiento mencionado para el sistema operativo Windows también se aplica al sistema operativo Linux con las excepciones siguientes:

- Cuando la opción Pasar todas las pulsaciones de teclas al servidor está activada, <Ctrl+Alt+Del> se pasa al sistema operativo en el sistema administrado.
- Las teclas mágicas SysRq con combinaciones de teclas que interpreta el núcleo de Linux y son de utilidad si el sistema operativo de la estación de administración o el servidor administrado se bloquea y es necesario recuperar el sistema. Puede activar las teclas mágicas SysRq en Linux mediante uno de los métodos siguientes:
 - Agregue una entrada a **/etc/sysctl.conf**
 - `echo "1" > /proc/sys/kernel/sysrq`
- Cuando la opción Pasar todas las pulsaciones de teclas al servidor está activada, las teclas mágicas SysRq se pasan al sistema operativo del sistema administrado. El comportamiento de la secuencia de teclas para restablecer el sistema operativo, es decir, reiniciar sin desmontar ni sincronizar, depende de si las teclas mágicas SysRq están activadas o desactivadas en la estación de administración:

- Si SysRq está activado en la estación de administración, <Ctrl+Alt+SysRq+b> o <Alt+SysRq+b> restablece la estación de administración, independientemente del estado del sistema.
- Si SysRq está activado en la estación de administración, <Ctrl+Alt+SysRq+b> o <Alt+SysRq+b> restablece el sistema operativo del sistema administrado.
- Otras combinación de teclas SysRq (por ejemplo, <Alt+SysRq+k>, <Ctrl+Alt+SysRq+m>, etc.) se pasan al sistema administrado, independientemente de si las teclas SysRq están activadas o no en la estación de administración.

Uso de teclas mágicas de SysRq a través de la consola remota

Puede activar las teclas mágicas de SysRq a través de la consola remota mediante cualquiera de los métodos siguientes:

- Herramienta IPMI de código abierto
- Uso de SSH/Telnet o conector serie externo

Uso de la herramienta IPMI de código abierto

Asegúrese de que la configuración del BIOS/iDRAC admite la redirección de consola mediante SOL.

1. En el indicador de comandos, ejecute el comando active SOL:

```
Ipmitool -I lanplus -H <ipaddr> -U <username> -P <password> sol activate
```

Se activa la sesión de SOL.

2. Después de que el servidor se inicie en el sistema operativo, aparecerá la petición de inicio de sesión `localhost.localdomain`. Inicie sesión con el nombre de usuario y la contraseña del sistema operativo.
3. Si SysRq no está activado, actívelo mediante `echo 1 >/proc/sys/kernel/sysrq`.
4. Ejecute la secuencia de interrupción ~ B.
5. Use la tecla mágica SysRq para habilitar la función SysRq. Por ejemplo, el siguiente comando muestra la información de memoria en la consola:

```
echo m >/proc/sysrq-trigger displays
```

Uso de SSH/Telnet o conector serie externo (conexión directa a través de un cable serie)

1. Para las sesiones Telnet/SSH, después de iniciar sesión mediante el nombre de usuario y la contraseña del iDRAC, en la solicitud `/admin >`, ejecute el comando `console com2`. Aparecerá la solicitud `localhost.localdomain`.
2. Para la redirección de consola mediante el conector serie externo conectado directamente al sistema mediante un cable de serie, la solicitud de inicio de sesión `localhost.localdomain` aparece después de que el servidor se inicia en el sistema operativo.
3. Inicie sesión mediante el nombre de usuario y la contraseña del sistema operativo.
4. Si SysRq no está activado, actívelo mediante `echo 1 >/kernel/sysrq /proc/sys`.
5. Use la tecla mágica para activar la función SysRq. Por ejemplo, el siguiente comando reinicia el servidor:

```
echo b >/proc/sysrq-trigger
```



NOTA: No es necesario ejecutar la secuencia de interrupción antes de usar las teclas mágicas de SysRq.

Sesión de consola virtual basada en ActiveX que se ejecuta en el sistema operativo Windows

El comportamiento de la opción de pasar todas las pulsaciones de teclas al servidor en una sesión de consola virtual basada en ActiveX que se ejecuta en un sistema operativo de Windows es similar al

comportamiento explicado para una sesión de consola virtual basada en Java que se ejecuta en la estación de administración de Windows con las excepciones siguientes:

- Cuando la opción Pasar todas las pulsaciones de teclas está desactivada, si presiona F1 se iniciará la ayuda de la aplicación tanto en la estación de administración como en el sistema administrado. También se mostrará el mensaje siguiente:

`Click Help on the Virtual Console page to view the online Help`

- Es posible que las teclas multimedia no se bloqueen explícitamente.
- Las combinaciones <Alt + Espacio>, <Ctrl + Alt + +>, <Ctrl + Alt + -> no se envían al sistema administrado y son interpretadas por el sistema operativo en la estación de administración.

Administración de medios virtuales

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.

Mediante la función de medios virtuales se puede realizar lo siguiente:

- Acceder de manera remota a los medios conectados a un sistema remoto a través de la red
- Instalar aplicaciones
- Actualizar controladores
- Instalar un sistema operativo en el sistema administrado

Esta función requiere licencia para los servidores tipo bastidor y torre y está disponible de manera predeterminada para los servidores Blade.

Las características claves son las siguientes:

- Los medios virtuales admiten unidades ópticas virtuales (CD/DVD), unidades de discos flexibles (incluidas las unidades USB) y unidades Flash USB.
- Puede conectar a un sistema administrado una sola unidad de disco flexible, unidad Flash USB, imagen o clave y una unidad óptica en la estación de administración. Entre las unidades de disco flexible compatibles se incluyen una imagen de disco flexible o una unidad de disco flexible disponible. Entre las unidades ópticas compatibles se incluye un máximo de una unidad óptica disponible o un archivo de imagen ISO.

En la figura siguiente se muestra una configuración típica de medios virtuales.

- No puede accederse a los medios de disco flexible virtuales de iDRAC desde máquinas virtuales.
- Todo medio virtual emula un dispositivo físico del sistema administrado.
- En sistemas administrados basados en Windows, las unidades de medios virtuales se montan automáticamente si están conectados y configurados con una letra de unidad.
- Con algunas configuraciones en los sistemas administrados basados en Linux, las unidades de medios virtuales no se montan automáticamente. Para montarlas manualmente, utilice el comando mount.
- Todas las solicitudes de acceso a la unidad virtual desde el sistema administrado se dirigen a la estación de administración a través de la red.
- Los dispositivos virtuales aparecen como dos unidades en el sistema administrado sin los medios que se están instalando en las unidades.
- Entre dos sistemas administrados se puede compartir la unidad CD/DVD (solo lectura) de la estación de administración, pero no un medio USB.
- Los medios virtuales requieren un ancho de banda de red mínimo disponible de 128 Kbps.
- Si se produce una conmutación por error LOM o NIC, es posible que se desconecte la sesión de medios virtuales.

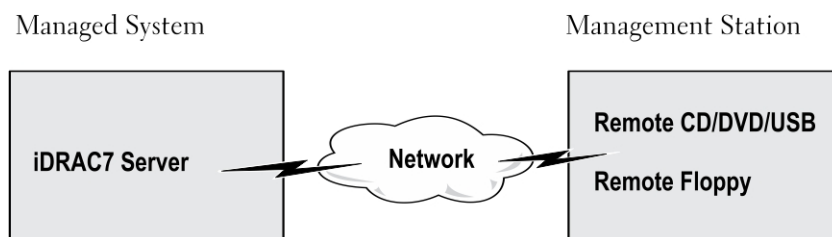


Ilustración 4. Configuración de medios virtuales

Unidades y dispositivos compatibles

En la tabla siguiente se enumeran las unidades compatibles a través de los medios virtuales.

Tabla 27. Unidades y dispositivos compatibles

| Unidad | Medios de almacenamiento compatibles |
|--------------------------------------|--|
| Unidades ópticas virtuales | <ul style="list-style-type: none"> Unidad de disco flexible heredada de 1,44 con disco flexible de 1,44 CD-ROM DVD CD-RW Unidad combinada con medios CD-ROM |
| Unidades de disco flexible virtuales | <ul style="list-style-type: none"> Archivo de imagen de CD-ROM/DVD en el formato ISO9660 Archivo de imagen de disco flexible en el formato ISO9660 |
| Unidades Flash USB | <ul style="list-style-type: none"> Unidad de CD-ROM USB con medios CD-ROM Imagen de llave USB en el formato ISO9660 |

Configuración de medios virtuales

Antes de configurar los valores de los medios virtuales, asegúrese de haber configurado el explorador web para utilizar el complemento Java o ActiveX.

Enlaces relacionados

[Configuración de exploradores web para usar la consola virtual](#)

Configuración de medios virtuales mediante la interfaz web de iDRAC

Para configurar los valores de medios virtuales:

- ⚠ PRECAUCIÓN:** No restablezca iDRAC mientras ejecuta una sesión de medios virtuales. De lo contrario, es posible que se produzcan resultados no deseados, incluida la pérdida de datos.
1. En la interfaz web de iDRAC, vaya a **Información general** → **Servidor** → **Medios conectados**.
 2. Especifique los valores necesarios. Para obtener más información, consulte la *Ayuda en línea de iDRAC*.

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

Configuración de medios virtuales mediante RACADM

Para configurar medios virtuales:

- Utilice los objetos del grupo **iDRAC.VirtualMedia** con el comando **set**.
- Utilice los objetos del grupo **cfgRacVirtual** con el comando **config**.

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

Configuración de medios virtuales mediante la utilidad de configuración de iDRAC

Puede conectar, desconectar o conectar automáticamente medios virtuales mediante la utilidad de configuración de iDRAC. Para ello, realice lo siguiente:

1. En la utilidad de configuración de iDRAC, vaya a **Configuración de medios y puertos USB**.
Se mostrará la página **Configuración de iDRAC.Configuración de medios y puertos USB**.
2. En la sección **Medios virtuales**, seleccione **Desconectar**, **Conectar** o **Conectar automáticamente** en función de las necesidades. Para obtener más información acerca de las opciones, consulte la *Ayuda en línea de la utilidad de configuración de iDRAC*.
3. Haga clic en **Atrás**, en **Terminar** y, a continuación, en **Sí**.
Se configuran los valores de los medios virtuales.

Estado de medios conectados y respuesta del sistema

En la tabla siguiente se describe la respuesta del sistema en función de la configuración de medios conectados.

Tabla 28. Estado de medios conectados y respuesta del sistema

| Estado de los medios conectados | Respuesta del sistema |
|---------------------------------|--|
| Desconectar | No se puede asignar una imagen al sistema. |
| Conectar | Los medios se asignan, incluso cuando se cierre la Vista de cliente . |
| Conexión automática | Los medios se asignan cuando se abre la Vista de cliente y su asignación se anula cuando se cierra la Vista de cliente . |

Configuración del servidor para ver los dispositivos virtuales en los medios virtuales

Es necesario configurar los valores siguientes en Management Station para permitir la visibilidad de las unidades vacías. Para ello, en Windows Explorer, desde el menú **Organizar**, haga clic en **Opciones de carpeta y de búsqueda**. En la ficha **Ver**, anule la selección de la opción **Ocultar unidades vacías en la carpeta Equipo** y haga clic en **Aceptar**.

Acceso a medios virtuales

Puede acceder a los medios virtuales con o sin la consola virtual. Antes de acceder a ellos, asegúrese de haber configurado los exploradores web.

Los medios virtuales y RFS son mutuamente exclusivos. Si la conexión del RFS se activa e intenta iniciar el cliente de medios virtuales, se muestra el siguiente mensaje de error: *Los medios virtuales no están disponibles actualmente. Hay una sesión de medios virtuales o recurso compartido de archivos remoto en uso.*

Si la conexión del RFS no está activa e intenta iniciar el cliente de medios virtuales, el cliente se inicia satisfactoriamente. Luego puede usar el cliente de medios virtuales para asignar dispositivos y archivos a las unidades virtuales de medios virtuales.

Enlaces relacionados

[Configuración de exploradores web para usar la consola virtual](#)

[Configuración de medios virtuales](#)


Inicio de medios virtuales mediante la consola virtual

Antes de iniciar medios virtuales a través de la consola virtual, asegúrese de lo siguiente:

- La consola virtual está activada.
- El sistema está configurado para no ocultar unidades vacías: En el Explorador de Windows, vaya a **Opciones de carpeta**, borre la opción **Ocultar unidades vacías en la carpeta Equipo** y haga clic en **Aceptar**.

Para acceder a los medios virtuales mediante la consola virtual:

1. En la interfaz web de iDRAC, vaya a **Información general** → **Servidor** → **Consola virtual**.
Se muestra la ventana **Consola virtual**.
2. Haga clic en **Iniciar Consola virtual**.
Se muestra el **Visor de consola virtual**.

 **NOTA:** En Linux, Java es el tipo de complemento predeterminado para acceder a la consola virtual. En Windows, abra el archivo `.jnlp` para iniciar la consola virtual mediante Java.

3. Haga clic en **Medios virtuales** → **Conectar medios virtuales**.
La sesión de medios virtuales se establece y el menú **Medios virtuales** muestra la lista de dispositivos disponibles para la asignación.

 **NOTA:** La aplicación de la ventana **Visor de consola virtual** debe permanecer activa mientras accede a los medios virtuales.

Enlaces relacionados

[Configuración de exploradores web para usar la consola virtual](#)

[Configuración de medios virtuales](#)

[Desactivación de mensajes de advertencia mientras se inicia la consola virtual o los medios virtuales mediante el complemento de Java o ActiveX](#)

Inicio de medios virtuales sin usar la consola virtual

Antes de iniciar medios virtuales cuando la **Consola virtual** está desactivada, asegúrese de lo siguiente:

- Los medios virtuales se encuentran en el estado *Conectar*.
- El sistema está configurado para mostrar las unidades vacías. Para ello, en Explorador de Windows, vaya a **Opciones de carpeta**, desactive la opción **Ocultar las unidades vacías en la carpeta Mi PC** y haga clic en **Aceptar**.

Para iniciar los medios virtuales cuando la consola virtual está desactivada:

1. En la interfaz web de iDRAC, vaya a **Información general** → **Servidor** → **Consola virtual**.

Se muestra la ventana **Consola virtual**.

2. Haga clic en **Iniciar Consola virtual**.

Aparece el mensaje siguiente:

Virtual Console has been disabled. Do you want to continue using Virtual Media redirection?

3. Haga clic en **Aceptar**.

Aparece la ventana **Medios virtuales**.

4. Desde el menú **Medios virtuales**, haga clic en **Asignar CD/DVD** o **Asignar disco extraíble**.

Para obtener más información, consulte [Asignación de unidad virtual](#).



NOTA: Las letras de unidad de los dispositivos virtuales en el sistema administrado no coinciden con las letras de unidades físicas en la estación de administración.



NOTA: Es posible que los medios virtuales no funcionen correctamente en clientes Windows configurados con la seguridad mejorada de Internet Explorer. Para resolver este problema, consulte la documentación del sistema operativo de Microsoft o póngase en contacto con el administrador del sistema.

Enlaces relacionados

[Configuración de medios virtuales](#)

[Desactivación de mensajes de advertencia mientras se inicia la consola virtual o los medios virtuales mediante el complemento de Java o ActiveX](#)

Adición de imágenes de medios virtuales

Puede crear una imagen de medios de la carpeta remota y montarla como un dispositivo USB conectado al sistema operativo del servidor. Para agregar las imágenes de medios virtuales:

1. Haga clic en **Medios virtuales** → **Crear imagen...**
2. En el campo **Carpeta de origen**, haga clic en **Examinar** y vaya a la carpeta o al directorio que se utilizará como origen para el archivo de imagen. El archivo de imagen se encuentra en la estación de administración o en la unidad C: del sistema administrado.
3. En el campo **Nombre de archivo de imagen** aparecerá la ruta de acceso predeterminada para almacenar los archivos de imagen creados (por lo general, el directorio del escritorio). Para cambiar esta ubicación, haga clic en **Examinar** y especifique una ubicación.
4. Haga clic en **Crear imagen**.

Se inicia el proceso de creación de la imagen. Si la ubicación del archivo de imagen está dentro de la carpeta de origen, aparecerá un mensaje de advertencia para indicar que la creación de la imagen no puede continuar porque la ubicación del archivo de imagen dentro de la carpeta de origen

provocará un lazo infinito. Si la ubicación del archivo de imagen no está dentro de la carpeta de origen, la creación de la imagen continúa.

Cuando se cree la imagen, aparecerá un mensaje para indicarlo.

5. Haga clic en **Finish (Finalizar)**.

Se crea la imagen.

Cuando una carpeta se agrega como imagen, se crea un archivo **.img** en el escritorio de la estación de administración desde la que se utiliza esta función. Si se mueve o elimina este archivo **.img**, la anotación correspondiente para esta carpeta en el menú **Medios virtuales** no funciona. Por tanto, es recomendable no mover ni eliminar el archivo **.img** mientras se usa la *imagen*. No obstante, el archivo **.img** se puede eliminar después de que se deselecciona la entrada pertinente y esta se quita mediante la opción **Quitar imagen** para quitar la anotación.

Visualización de los detalles del dispositivo virtual

Para ver los detalles del dispositivo virtual, en el visor de la consola virtual haga clic en **Herramientas** → **Estadísticas**. En la ventana **Estadísticas**, la sección **Medios virtuales** muestra los dispositivos virtuales asignados y la actividad de lectura/escritura de cada dispositivo. Si los medios virtuales están conectados, se visualiza esta información. Si los medios virtuales no están conectados, aparece el mensaje "Medios virtuales no conectados".

Si los medios virtuales se inician sin utilizar la consola virtual, la sección **Medios virtuales** aparece como un cuadro de diálogo. Proporciona información acerca de los dispositivos asignados.

Restablecimiento de USB

Para restablecer el dispositivo USB:

1. En el visor de la consola virtual, haga clic en **Herramientas** → **Estadísticas**.
Aparece la ventana **Estadísticas**.
2. En **Medios virtuales**, haga clic en **Restablecimiento de USB**.
Aparece un mensaje que indica al usuario que el restablecimiento de la conexión USB puede afectar a todas las entradas del dispositivo de entrada, incluidos los medios virtuales, el teclado y el mouse.
3. Haga clic en **Sí**.
Se restablece el USB.



NOTA: Los medios virtuales de iDRAC no finalizan ni siquiera después de cerrar la sesión de la interfaz web de iDRAC.

Asignación de la unidad virtual

Para asignar la unidad virtual:




NOTA: Al utilizar los medios virtuales basados en ActiveX, debe disponer de privilegios administrativos para asignar un DVD o unidad Flash USB (conectada a la estación de administración) de sistema operativo. Para asignar las unidades, inicie IE como administrador o agregue la dirección IP de iDRAC a la lista de sitios de confianza.

1. Para establecer una sesión de medios virtuales, en el menú **Medios virtuales**, haga clic en **Conectar medios virtuales**.


Por cada dispositivo disponible para asignar desde el servidor host, aparecerá un elemento en el menú **Medios virtuales**. El elemento de menú recibe un nombre acorde al tipo de dispositivo, por ejemplo:

- Asignar CD/DVD
- Asignar disco extraíble
- Asignar disco flexible

 **NOTA:** Aparece el elemento de menú **Asignar disco flexible** en la lista si la opción **Emulación de disco flexible** está activada en la página **Medios conectados**. Cuando se activa **Emulación de disco flexible**, **Asignar disco extraíble** se reemplaza con **Asignar disco flexible**.

La opción **Asignar DVD/CD** se puede usar para archivos ISO y la opción de **Asignar disco extraíble** puede utilizarse para imágenes.

2. Haga clic en el tipo de dispositivo que desea asignar.

 **NOTA:** Se muestra la sesión activa si hay una sesión de medios virtuales activa actualmente desde la sesión de la interfaz web actual, desde otra sesión de interfaz web o desde VMCLI.

3. En el campo **Unidad/archivo de imagen**, seleccione el dispositivo de la lista desplegable.

La lista contiene todos los dispositivos disponibles (no asignados) que puede asignar (CD/DVD, disco extraíble, disco flexible) y los tipos de archivo de imagen que puede asignar (ISO o IMG). Los archivos de imagen están ubicados en el directorio predeterminado de archivos de imagen (por lo general, el escritorio del usuario). Si el dispositivo no está disponible en la lista desplegable, haga clic en **Explorar** para especificar el dispositivo.

El tipo de archivo correcto para CD/DVD es ISO y para disco extraíble y disco flexible es IMG.

Si la imagen se crea en la ruta de acceso predeterminada (Escritorio), cuando seleccione **Asignar disco extraíble**, la imagen creada estará disponible para la selección en el menú desplegable.

Si crea la imagen en una ubicación diferente, cuando seleccione **Asignar disco extraíble**, la imagen creada no estará disponible para la selección en el menú desplegable. Haga clic en **Examinar** para especificar la imagen.

4. Seleccione **Solo lectura** para asignar dispositivos que admitan escritura como de sólo lectura. Para los dispositivos de CD/DVD, esta opción está activada de manera predeterminada y el usuario no puede desactivarla.
5. Haga clic en **Asignar dispositivo** para asignar el dispositivo al servidor host. Después de asignar el dispositivo/archivo, el nombre de su elemento de menú de **Medios virtuales** cambia para indicar el nombre del dispositivo. Por ejemplo, si el dispositivo de CD/DVD se asigna a un archivo de imagen llamado **foo.iso**, el elemento de menú de CD/DVD del menú de Medios virtuales se denomina **foo.iso asignado a CD/DVD**. La marca de verificación en dicho menú indica que está asignado.

Enlaces relacionados

[Visualización de las unidades virtuales correctas para la asignación](#)

[Adición de imágenes de medios virtuales](#)

Visualización de las unidades virtuales correctas para la asignación

En una estación de administración basada en Linux, la ventana **Cliente** de los medios virtuales puede mostrar discos extraíbles y discos flexibles que no forman parte de la estación de administración. Para

asegurarse de que las unidades virtuales correctas están disponibles para su asignación, debe activar la configuración de puertos para el disco duro SATA conectado. Para hacerlo, siga estos pasos:

1. Reinicie el sistema operativo de la estación de administración. Durante la POST, presione <F2> o ingrese a **Configuración del sistema**.
2. Vaya a **Configuración de SATA**. Se muestran los detalles del puerto.
3. Active los puertos que están presentes en el disco duro y conectados a él.
4. Acceda a la ventana **Ciente** de los medios virtuales. Se mostrarán las unidades correctas que se pueden asignar.

Enlaces relacionados

[Asignación de la unidad virtual](#)

Anulación de la asignación de la unidad virtual

Para anular la asignación de la unidad virtual:

1. Desde el menú **Medios virtuales** realice cualquiera de las siguientes acciones:
 - Haga clic en el dispositivo que desea desasignar.
 - Haga clic en **Desconectar medios virtuales**.


Aparece un mensaje de confirmación.

2. Haga clic en **Sí**.

La marca de verificación para ese elemento del menú no aparece, lo que indica que no está asignado al servidor host.

Configuración del orden de inicio a través del BIOS

Mediante la utilidad de configuración del BIOS del sistema puede establecer el sistema administrado para que se inicie desde unidades ópticas virtuales o unidades de disco flexible virtuales.

 **NOTA:** Si cambia los medios virtuales mientras están conectados, podría detenerse la secuencia de inicio del sistema.

Para activar el sistema administrado para que se inicie:

1. Inicie el sistema administrado.
2. Presione <F2> para abrir la página **Configuración del sistema**.
3. Vaya a **Configuración del BIOS del sistema** → **Configuración de inicio** → **Configuración de inicio del BIOS** → **Secuencia de inicio**.
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 figure como el primer dispositivo con medios de inicio. Si fuera necesario, siga las instrucciones en pantalla para modificar el orden de inicio.
5. Haga clic en **Aceptar**, vuelva a **Configuración del BIOS del sistema** y haga clic en **Terminar**.
6. Haga clic en **Sí** para guardar los cambios y salir.
El sistema administrado reinicia.

El sistema administrado intenta iniciar desde un dispositivo de inicio según el orden de inicio establecido. Si el dispositivo virtual está conectado y hay un medio de inicio presente, el sistema se

inicia con el dispositivo virtual. De lo contrario, el sistema omite el dispositivo, similar a un dispositivo físico sin medios de inicio.

Activación del inicio único para medios virtuales

Puede cambiar el orden de inicio solamente después de conectar un dispositivo de medios virtuales remoto.

Antes de activar la opción de inicio único, asegúrese de lo siguiente:

- Dispone del privilegio *Configurar usuario*.
- Asigne las unidades locales o virtuales (CD/DVD, disco flexible o dispositivo Flash USB) con los medios o la imagen de inicio mediante las opciones de medios virtuales
- Los medios virtuales deben estar en el estado *Conectado* para que las unidades virtuales aparezcan en la secuencia de inicio.

Para activar la opción de inicio único e iniciar el sistema administrado desde los medios virtuales:

1. En la interfaz web de iDRAC, vaya a **Información general** → **Servidor** → **Medios conectados**.
2. En **Medios virtuales**, seleccione la opción **Activar el inicio una vez** y haga clic en **Aplicar**.
3. Encienda el sistema administrado y presione **<F2>** durante el inicio.
4. Cambie la secuencia de inicio para iniciar desde el dispositivo de medios virtuales remoto.
5. Reinicie el servidor.

El sistema administrado se inicia una vez desde los medios virtuales.


Enlaces relacionados

[Asignación de la unidad virtual](#)

[Configuración de medios virtuales](#)

Instalación y uso de la utilidad de VMCLI

La utilidad Interfaz de línea de comandos de medios virtuales (VMCLI) es una interfaz que proporciona funciones de medios virtuales desde la estación de administración a iDRAC en el sistema administrado. Al usar esta utilidad, puede acceder a las funciones de medios virtuales, incluidos los archivos de imagen y las unidades físicas, para implementar un sistema operativo en varios sistemas remotos de una red.

 **NOTA:** Puede ejecutar la utilidad VMCLI solo en la estación de administración que se instala con el sistema operativo de 32 bits.

La utilidad VMCLI proporciona las siguientes funciones:

- Administración de dispositivos extraíbles o imágenes accesibles a través de medios virtuales.
- Finalización automática de la sesión cuando se activa la opción **Iniciar una vez** en el firmware de iDRAC.
- Comunicaciones seguras con iDRAC mediante la capa de sockets seguros (SSL).
- Ejecute comandos VMCLI hasta que:
 - se terminen automáticamente las conexiones.
 - un sistema operativo termine el proceso.

 **NOTA:** Para terminar el proceso en Windows, utilice el Administrador de tareas.

Instalación de VMCLI

La utilidad VMCLI se incluye en el DVD *Herramientas y documentación de Dell Systems Management*. Para instalar la utilidad VMCLI:

1. Inserte el DVD *Herramientas y documentación de Dell Systems Management* en la unidad de DVD.
2. Siga las instrucciones en pantalla para instalar las herramientas de DRAC.
3. Cuando la instalación se haya completado correctamente, compruebe la carpeta **install\Dell\SysMgt\vmcli5** para asegurarse de que existe el archivo **vmcli.exe**. De manera similar, compruebe la ruta de acceso relativa para UNIX.

La utilidad VMCLI se instala en el programa.

Ejecución de la utilidad de VMCLI

- Si el sistema operativo requiere privilegios específicos o una pertenencia a un grupo concreto, deberá disponer de privilegios similares para ejecutar los comandos VMCLI.
- En sistemas Windows, los usuarios que no sean administradores requieren los privilegios **Usuario avanzado** para ejecutar la utilidad VMCLI.
- En sistemas Linux, ejecute la utilidad VMCLI y los comandos de inicio de sesión de usuario para acceder a iDRAC. Los usuarios que no sean administradores deben anexar el prefijo `sudo` en los

comandos de VMCLI. No obstante, para agregar o editar usuarios de los grupos de administradores de VMCLI, utilice el comando `visudo`.

Sintaxis de VMCLI

La interfaz VMCLI es idéntica en los sistemas Windows y Linux, y su sintaxis es la siguiente:

```
VMCLI [parameter] [operating_system_shell_options]
```

Por ejemplo, `vmcli -r iDRAC-IP-address:iDRAC-SSL-port`

Con el valor *parameter*, la interfaz VMCLI puede conectarse al servidor especificado, acceder a iDRAC y asignarse a los medios virtuales especificados.

 **NOTA:** La sintaxis de VMCLI distingue entre mayúsculas y minúsculas.

Para garantizar la seguridad, es recomendable utilizar los siguientes parámetros de VMCLI:

- `vmcli -i`: permite un método interactivo para iniciar VMCLI y garantiza que el nombre de usuario y la contraseña no estarán visibles cuando otros usuarios examinan los procesos.
- `vmcli -r <iDRAC-IP-address[:iDRAC-SSL-port]> -S -u <iDRAC-user-name> -p <iDRAC-user-password> -c {<device-name> | <image-file>}`: indica si el certificado CA de iDRAC es válido. Si el certificado no es válido, se muestra un mensaje de advertencia cuando se ejecuta este comando. Sin embargo, el comando se ejecuta correctamente y se establece una sesión VMCLI. Para obtener más información sobre los parámetros de VMCLI, consulte *Ayuda de VMCLI* o las *páginas principales de VMCLI*.

Enlaces relacionados

- [Comandos de VMCLI para acceder a los medios virtuales](#)
- [Opciones de shell del sistema operativo de VMCLI](#)

Comandos de VMCLI para acceder a los medios virtuales

En la tabla siguiente se proporcionan los comandos VMCLI necesarios para acceder a distintos medios virtuales.

Tabla 29. Comandos VMCLI

| Medios virtuales | Comando |
|---|---|
| Unidad de disco flexible | <code>vmcli -r [iDRAC IP or hostname] -u [iDRAC user name] -p [iDRAC user password] -f [device name]</code> |
| Disco flexible o imagen de memoria de USB de inicio | <code>vmcli -r [iDRAC IP address] [iDRAC user name] -p [iDRAC password] -f [floppy.img]</code> |
| Unidad CD mediante la opción -f | <code>vmcli -r [iDRAC IP address] -u [iDRAC user name] -p [iDRAC password] -f [device name] [image file]-f [cdrom - dev]</code> |
| Imagen CD/DVD de inicio | <code>vmcli -r [iDRAC IP address] -u [iDRAC user name] -p [iDRAC password] -c [DVD.img]</code> |

Si el archivo no está protegido contra escritura, es posible que los medios virtuales escriban en el archivo de imagen. Para evitar esto, realice lo siguiente:

- Configure el sistema operativo para proteger contra escritura una imagen de disco flexible que no desea que se sobrescriba.
- Utilice la función de protegido contra escritura del dispositivo.

Al virtualizar archivos de imagen de solo lectura, varias sesiones pueden utilizar los mismos medios de imagen simultáneamente.

Al virtualizar unidades físicas, solo una sesión a la vez puede acceder a una unidad física determinada.

Opciones de shell del sistema operativo de VMCLI

VMCLI utiliza opciones de shell para activar las siguientes funciones del sistema operativo:

- `stderr/stdout redirection`: dirige los mensajes impresos de la utilidad hacia un archivo. Por ejemplo, al utilizar el carácter mayor que (>), seguido de un nombre de archivo, se sobrescribe el archivo especificado con el mensaje impreso de la utilidad VMCLI.

 **NOTA:** La utilidad VMCLI no realiza una lectura de las entradas estándares (stdin). Por lo tanto, no es necesario realizar un redireccionamiento stdin.

- **Ejecución en segundo plano:** de manera predeterminada, la utilidad VMCLI se ejecuta en primer plano. Utilice las funciones de shell del sistema operativo para que la utilidad se ejecute en segundo plano.

Por ejemplo, en Linux, el carácter & después del comando hace que el programa se genere como un nuevo proceso de segundo plano. Esta técnica es de utilidad en los programas de secuencia de comandos, ya que permite a la secuencia de comandos continuar cuando un nuevo proceso se inicia para el comando VMCLI (de lo contrario, la secuencia de comandos se bloquea hasta que se termine el programa VMCLI).


Cuando se inicial varias sesiones de VMCLI, utilice las prestaciones específicas del sistema operativo para enumerar y terminar los procesos.

Administración de la tarjeta vFlash SD

La tarjeta vFlash SD es una tarjeta Secure Digital (SD) que se inserta en la ranura correspondiente en el sistema. Puede utilizar una tarjeta con una capacidad máxima de 16 GB. Después de insertar la tarjeta, deberá activar la funcionalidad vFlash para crear y administrar particiones. La función vFlash requiere una licencia.


Si la tarjeta no está disponible en la ranura de tarjeta vFlash SD del sistema, aparecerá el siguiente mensaje de error en la interfaz web de iDRAC, en **Información general** → **Servidor** → **vFlash**:

```
SD card not detected. Please insert an SD card of size 256MB or greater.
```

 **NOTA:** Asegúrese de insertar únicamente una tarjeta vFlash SD compatible en la ranura correspondiente. Si inserta una tarjeta SD no compatible, aparecerá el siguiente mensaje de error al inicializar la tarjeta: *Error al iniciar la tarjeta SD*.


Las características claves son las siguientes:

- Proporciona espacio de almacenamiento y emula dispositivos USB.
- Se pueden crear hasta 16 particiones que, cuando se conectan, se exponen a la unidad de disco flexible virtual, la unidad de disco duro o una unidad de CD/DVD en función del modo de emulación seleccionado.
- Se pueden crear particiones desde tipos de archivos admitidos. Se admite el formato **.img** para discos flexibles, el formato **.iso** para CD/DVD y los formatos **.iso** e **.img** para los tipos de emulación de disco duro.
- Se pueden crear dispositivos USB de inicio.
- Se puede realizar un inicio único en un dispositivo USB emulado.

 **NOTA:** Es posible que una licencia de vFlash caduque durante una operación vFlash. Si esto sucede, las operaciones vFlash en curso se completarán con normalidad.

Configuración de la tarjeta vFlash SD

Antes de configurar vFlash, asegúrese de que la tarjeta vFlash SD esté instalada en el sistema. Para obtener información sobre cómo instalar y quitar la tarjeta del sistema, consulte *Hardware Owner's Manual* (Manual del propietario de hardware) del sistema disponible en dell.com/support/manuals.

 **NOTA:** Es necesario tener privilegios de acceso a los medios virtuales para activar o desactivar la funcionalidad vFlash y para inicializar la tarjeta.

Enlaces relacionados

[Visualización de las propiedades de la tarjeta vFlash SD](#)

[Activación o desactivación de la funcionalidad vFlash](#)

[Inicialización de la tarjeta vFlash SD](#)

Visualización de las propiedades de la tarjeta vFlash SD

Una vez activada la función vFlash, se pueden ver las propiedades de la tarjeta SD mediante la interfaz web de iDRAC o RACADM.

Visualización de las propiedades de la tarjeta vFlash SD mediante la interfaz web

Para ver las propiedades de la tarjeta vFlash, en la interfaz web de iDRAC, vaya a **Descripción general** → **Servidor** → **vFlash**. Se mostrará la página **Propiedades de la tarjeta SD**. Para obtener información acerca de las propiedades que se muestran, consulte *iDRAC Online Help* (Ayuda en línea de iDRAC).

Visualización de las propiedades de la tarjeta vFlash SD mediante RACADM

Para ver las propiedades de la tarjeta vFlash SD mediante RACADM, utilice uno de los siguientes procedimientos:

- Utilice el objeto `cfgvFlashSD` con el comando `getConfig`. A continuación se muestran las siguientes propiedades de solo lectura:
 - `cfgVFlashSDSize`
 - `cfgVFlashSDLicensed`
 - `cfgVFlashSDAvailableSize`
 - `cfgVFlashSDHealth`
 - `cfgVFlashSDEnable`
 - `cfgVFlashSDWriteProtect`
 - `cfgVFlashSDInitialized`
- Utilice los siguientes objetos con el comando `get`:
 - `iDRAC.vflashsd.AvailableSize`
 - `iDRAC.vflashsd.Health`
 - `iDRAC.vflashsd.Licensed`
 - `iDRAC.vflashsd.Size`
 - `iDRAC.vflashsd.WriteProtect`

Para obtener más información acerca de estos objetos, consulte *iDRAC8 RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8) disponible en dell.com/support/manuals o dell.com/esmanuals.

Visualización de las propiedades de la tarjeta vFlash SD mediante la utilidad de configuración de iDRAC


Para ver las propiedades de la tarjeta vFlash SD, en la **utilidad de configuración de iDRAC**, vaya a **Configuración de medios y puertos USB**. En la página **Configuración de iDRAC. Configuración de medios y puertos USB** se muestran las propiedades. Para obtener información acerca de las propiedades que se muestran, consulte la *Ayuda en línea de la utilidad de configuración de iDRAC*.

Activación o desactivación de la funcionalidad vFlash

Debe activar la funcionalidad vFlash para realizar la administración de particiones.

Activación o desactivación de la funcionalidad vFlash mediante la interfaz web

Para activar o desactivar la funcionalidad vFlash:

1. En la interfaz web de iDRAC, vaya a **Información general** → **Servidor** → **vFlash**. Aparece la página **Propiedades de la tarjeta SD**.
2. Active o desactive la opción **vFLASH activado** para activar o desactivar la funcionalidad vFlash. Si hay alguna partición vFlash conectada, no podrá desactivar vFlash y se mostrará un mensaje de error.
 **NOTA:** Si se desactiva la funcionalidad vFlash, no se muestran las propiedades de la tarjeta SD.
3. Haga clic en **Aplicar**. La funcionalidad vFlash se activa o desactiva según la opción seleccionada.

Activación o desactivación de la funcionalidad vFlash mediante RACADM

Para activar o desactivar la funcionalidad vFlash mediante RACADM, utilice uno de los siguientes procedimientos:


- Mediante el comando `config`:
 - Para activar vFlash:

```
racadm config -g cfgvFlashsd -o cfgvflashSDEnable 1
```
 - Para desactivar vFlash:

```
racadm config -g cfgvFlashsd -o cfgvflashSDEnable 0
```
- Mediante el comando `set`:
 - Para activar vFlash:

```
racadm set iDRAC.vflashsd.Enable 1
```
 - Para desactivar vFlash:

```
racadm set iDRAC.vflashsd.Enable 0
```

 **NOTA:** El comando RACADM solo funciona si hay una tarjeta vFlash SD presente. Si no hay ninguna tarjeta, aparecerá el mensaje siguiente: *ERROR: tarjeta SD ausente*.


Activación o desactivación de la funcionalidad vFlash mediante la utilidad de configuración de iDRAC

Para activar o desactivar la funcionalidad vFlash:

1. En la utilidad de configuración de iDRAC, vaya a **Configuración de medios y puertos USB**. Aparecerá la página **Configuración de iDRAC.Configuración de medios y puertos USB**.
2. En la sección **Medios vFlash**, seleccione **Activado** para activar la funcionalidad vFlash o **Desactivado** para desactivarla.
3. Haga clic en **Atrás**, en **Terminar** y, a continuación, en **Sí**. La funcionalidad vFlash se activa o desactiva según la opción seleccionada.

Inicialización de la tarjeta vFlash SD

La operación de inicialización reformatea la tarjeta SD y configura la información inicial vFlash en la tarjeta.

 **NOTA:** Si la tarjeta SD está protegida contra escritura, la opción Inicializar estará desactivada.

Inicialización de la tarjeta vFlash SD mediante la interfaz web

Para iniciar la tarjeta vFlash SD:

1. En la interfaz web de iDRAC, vaya a **Información general** → **Servidor** → **vFlash**.
Aparece la página **Propiedades de la tarjeta SD**.
2. Active **vFLASH** y haga clic en **Inicializar**.
Todo el contenido existente se quita y la tarjeta se vuelve a formatear con la información del nuevo sistema vFlash.

Si hay alguna partición vFlash conectada, la operación de inicialización falla y aparece un mensaje de error.

Inicialización de la tarjeta vFlash SD mediante RACADM

Para inicializar la tarjeta vFlash SD mediante RACADM, utilice uno de los siguientes procedimientos:

- Mediante el comando vFlashSD:

```
racadm vflashsd initialize
```
- Mediante el comando set:

```
racadm set iDRAC.vflashsd.Initialized 1
```

Se eliminan todas las particiones existentes y la tarjeta se reformatea.

Para obtener más información acerca de estos comandos, consulte *iDRAC8 RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8), disponible en dell.com/support/manuals y dell.com/esmanuals.

Inicialización de la tarjeta vFlash SD mediante la utilidad de configuración de iDRAC

Para inicializar la tarjeta vFlash SD mediante la utilidad de configuración de iDRAC:


1. En la utilidad de configuración de iDRAC, vaya a **Media and USB Port Settings** (Medios y configuración de puerto USB).
Aparece la página **iDRAC Settings - Media and USB Port Settings** (Configuración de iDRAC) - (Medios y configuración de puerto USB).
2. Haga clic en **Inicializar vFlash**.
3. Haga clic en **Sí**. Se inicia la operación de inicialización.
4. Haga clic en **Atrás** y vaya a la misma página de **iDRAC Settings - Media and USB Port Settings** (Configuración de iDRAC - Medios y configuración de puerto USB).
Todo el contenido existente se quita y la tarjeta se vuelve a formatear con la información del nuevo sistema vFlash.

Obtención del último estado mediante RACADM

Para obtener el estado del último comando initialize enviado a la tarjeta SD vFlash:


1. Abra una consola Telnet, SSH o de comunicación en serie al sistema e inicie sesión.
2. Introduzca el comando: `racadm vFlashsd status`
Se muestra el estado de los comandos enviados a la tarjeta SD.
3. Para obtener el último estado de todas las particiones vFlash, utilice el comando: `racadm vflashpartition status -a`

4. Para obtener el último estado de una partición concreta, utilice el comando:
`racadm vflashpartition status -i (index)`


 **NOTA:** Si se reinicia iDRAC, se perderá el estado de la última operación de partición.

Administración de las particiones vFlash

Puede realizar lo siguiente mediante la interfaz web de iDRAC o RACADM:

 **NOTA:** Un administrador puede realizar todas las operaciones en las particiones vFlash. De lo contrario, debe disponer el privilegio **Acceder a los medios virtuales** para crear, eliminar, formatear, conectar, desconectar o copiar el contenido para la partición.

- [Creación de una partición vacía](#)
- [Creación de una partición mediante un archivo de imagen](#)
- [Formateo de una partición](#)
- [Visualización de las particiones disponibles](#)
- [Modificación de una partición](#)
- [Conexión o desconexión de particiones](#)
- [Eliminación de las particiones existentes](#)
- [Descarga del contenido de una partición](#)
- [Inicio de una partición](#)

 **NOTA:** Si hace clic en cualquier opción de las páginas vFlash cuando una aplicación utiliza vFlash, tal como WS-MAN, la utilidad de configuración de iDRAC o RACADM, o si desea desplazarse a otra página de la interfaz gráfica de usuario (GUI), es posible que iDRAC muestre el siguiente mensaje:
`vFlash is currently in use by another process. Try again after some time.`

vFlash puede realizar la creación de particiones rápida cuando no hay otras operaciones vFlash en curso, tal como el formateo, la conexión de particiones, etc. Por lo tanto, es recomendable primero crear las particiones antes de realizar otras operaciones de partición individuales.

Creación de una partición vacía

Una partición vacía, cuando está conectada al sistema, es similar a una unidad Flash USB vacía. Puede crear particiones vacías en una tarjeta vFlash SD. Puede crear particiones de tipo *Disco flexible* o *Disco duro*. Las particiones de CD solo se admiten cuando se crean particiones mediante imágenes.

Antes de crear una partición vacía, asegúrese de lo siguiente:

- Dispone de privilegios **Acceder a los medios virtuales**.
- La tarjeta está inicializada.
- La tarjeta no está protegida contra escritura.
- No se está realizando una operación de inicialización en la tarjeta.

Creación de una partición vacía mediante la interfaz web

Para crear una partición vFlash vacía:

1. En la interfaz web de iDRAC, vaya a **Información general** → **Servidor** → **vFlash** → **Crear partición vacía**.

Aparece la página **Crear partición vacía**.

2. Especifique la información necesaria y haga clic en **Aplicar**. Para obtener más información acerca de las opciones, consulte la *Ayuda en línea de iDRAC*.

Se crea una nueva partición vacía sin formato que es de solo lectura de manera predeterminada.

También se muestra una página que indica el porcentaje del progreso. Aparece un mensaje de error en los casos siguientes:

- La tarjeta está protegida contra escritura.
- El nombre de la etiqueta coincide con la etiqueta de una partición existente.
- Se introduce un valor no entero para el tamaño de la partición, el valor excede el espacio disponible en la tarjeta o el tamaño de la partición es mayor que 4 GB.
- Ya se está realizando una operación de inicialización en la tarjeta.

Creación de una partición vacía mediante RACADM

Para crear una partición vacía de 20 MB:

1. Abra una consola Telnet, SSH o de comunicación en serie al sistema e inicie sesión.
2. Introduzca el comando: `racadm vflashpartition create -i 1 -o drive1 -t empty -e HDD -f fat16 -s 20`


Se crea una partición vacía de 20 MB en el formato FAT16. De manera predeterminada, una partición vacía se crea con derechos de lectura y escritura.

Creación de una partición mediante un archivo de imagen


Puede crear una partición nueva en la tarjeta vFlash SD mediante un archivo de imagen (disponible en el formato **.img** o **.iso**). Las particiones son de tipos de emulación: disco flexible (**.img**), disco duro (**.img**) o CD (**.iso**). El tamaño de la partición creada es igual al tamaño del archivo de imagen.

Antes de crear una partición a partir de un archivo de imagen, asegúrese de lo siguiente:

- Dispone de privilegios Acceder a los medios virtuales.
- La tarjeta está inicializada.
- La tarjeta no está protegida contra escritura.
- No se está realizando una operación de inicialización en la tarjeta.
- El tipo de imagen y el tipo de emulación coinciden.

 **NOTA:** La imagen cargada y el tipo de emulación deben coincidir. Existen problemas cuando iDRAC emula un dispositivo con un tipo de imagen incorrecto. Por ejemplo, si la partición se utiliza con una imagen ISO y el tipo de emulación se especifica como Disco duro, el BIOS no podrá iniciar desde esta imagen.

- El tamaño del archivo de imagen es menor o igual que el espacio disponible en la tarjeta.
- El tamaño del archivo de imagen es menor o igual que 4 GB, ya que el tamaño máximo de la partición admitido es 4 GB. No obstante, cuando crea una partición mediante un explorador web, el tamaño de archivo de imagen debe ser menor que 2 GB.

 **NOTA:** La partición de vFlash es un archivo de imagen que se encuentra en un sistema de archivos FAT32. Por lo tanto, el archivo de imagen tiene la limitación de 4 GB.

Creación de una partición mediante un archivo de imagen utilizando la interfaz web

Para crear una partición vFlash mediante un archivo de imagen:

1. En la interfaz web de iDRAC, vaya a **Información general** → **Servidor** → **vFlash** → **Crear desde imagen**.

Aparece la página **Crear partición a partir de archivo de imagen**.

2. Introduzca la información necesaria y haga clic en **Aplicar**. Para obtener más información acerca de las opciones, consulte la *Ayuda en línea de iDRAC*.

Se crea una partición nueva. Para el tipo de emulación CD, se crea una partición de solo lectura. Para los tipos de emulación Disco flexible o Disco duro, se crea una partición de lectura y escritura.

Aparecerá un mensaje de error en los casos siguientes:


- La tarjeta está protegida contra escritura.
- El nombre de la etiqueta coincide con la etiqueta de una partición existente.
- El tamaño del archivo de 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.


Creación de una partición desde un archivo de imagen mediante RACADM

Para crear una partición a partir de un archivo de imagen mediante RACADM:

1. Abra una consola Telnet, SSH o de comunicación en serie al sistema e inicie sesión.
2. Introduzca el comando: `racadm vflashpartition create -i 1 -o drive1 -e HDD -t image -l //myserver/sharedfolder/foo.iso -u root -p mypassword`

Se crea una partición nueva. De manera predeterminada, la partición creada es de solo lectura. Este comando distingue entre mayúsculas y minúsculas para la extensión de nombre de archivo de la imagen. Si la extensión de nombre de archivo está en mayúscula, por ejemplo, FOO.ISO en lugar FOO.iso, el comando devuelve un error de sintaxis.

 **NOTA:** Esta función no se admite en RACADM local.

 **NOTA:** No se admite la creación de una partición vFlash a partir de un archivo de imagen situado en un recurso compartido CFS o NFS habilitado para IPv6.

Formateo de una partición

Puede formatear una partición existente en la tarjeta vFlash SD en función del tipo del sistema de archivos. Los tipos de sistema de archivos compatibles con EXT2, EXT3, FAT16 y FAT32. Solo puede formatear particiones de tipo disco duro o disco flexible (no CD). No es posible formatear particiones de solo lectura.

Antes de crear una partición a partir de un archivo de image, asegúrese de lo siguiente:

- Dispone de privilegios **Acceder a los medios virtuales**.
- La tarjeta está inicializada.
- 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 de iDRAC, vaya a **Información general** → **Servidor** → **vFlash** → **Formatear**. Aparece la página **Formatear partición**.

2. Introduzca la información necesaria y haga clic en **Aplicar**.

Para obtener más información acerca de estas opciones, consulte la *Ayuda en línea de iDRAC*.

Aparece un mensaje de advertencia que indica que todos los datos de la partición se borrarán.

3. Haga clic en **Aceptar**.

La partición seleccionada se formatea en el tipo de sistema de archivos especificado. Se mostrará un mensaje de error en los casos siguientes:

- La tarjeta está protegida contra escritura.
- Ya se está realizando una operación de inicialización en la tarjeta.

Visualización de las particiones disponibles

Asegúrese de que la función vFlash esté activada para ver la lista de particiones disponibles.


Visualización de las particiones disponibles mediante la interfaz web

Para ver las particiones vFlash disponibles, en la interfaz web de iDRAC vaya a **Descripción general** → **Servidor** → **vFlash** → **Administrar**. Se muestra la página **Administrar particiones** con una lista de las particiones disponibles y la información relacionada a cada una de ellas. Para obtener información acerca de las particiones, consulte *iDRAC Online Help* (Ayuda en línea de iDRAC).

Visualización de las particiones disponibles mediante RACADM

Para ver las particiones disponibles y sus propiedades en mediante RACADM:


1. Abra una consola Telnet, SSH o de comunicación en serie al sistema e inicie sesión.
2. Introduzca los comandos siguientes:
 - Para enumerar todas las particiones existentes y sus propiedades:
`racadm vflashpartition list`
 - Para obtener el estado operativo en la partición 1:
`racadm vflashpartition status -i 1`
 - Para obtener el estado de todas las particiones existentes:
`racadm vflashpartition status -a`

 **NOTA:** La opción -a solo es válida con la acción status.

Modificación de una partición

Puede cambiar una partición de solo lectura a lectura-escritura o viceversa. Antes de modificar la partición, asegúrese de lo siguiente:

- La funcionalidad vFlash está activada.
- Dispone de privilegios **Acceder a los medios virtuales**.

 **NOTA:** De manera predeterminada, se crea una partición de solo lectura.

Modificación de una partición mediante la interfaz web

Para modificar una partición:

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Servidor** → **vFlash** → **Administrar**. Aparece la página **Administrar particiones**.
2. En la columna **Solo lectura**, realice lo siguiente:
 - Seleccione la casilla de las particiones deseadas y haga clic en **Aplicar** para cambiarlas a modo de solo lectura.
 - Desactive la casilla de las particiones deseadas y haga clic en **Aplicar** para cambiarlas a modo de lectura-escritura.

Las particiones se cambian a solo lectura o lectura-escritura según las opciones seleccionadas.



NOTA: Si la partición es de tipo CD, el estado es de solo lectura. No puede cambiar el estado a lectura-escritura. Si la partición está conectada, la casilla aparece atenuada.

Modificación de una partición mediante RACADM

Para ver las particiones disponibles y sus propiedades en la tarjeta:

1. Abra una consola Telnet, SSH o de comunicación en serie al sistema e inicie sesión.
2. Utilice uno de los siguientes métodos:
 - Mediante el comando `config` para cambiar el estado de lectura y escritura de la partición:
 - Para cambiar una partición de solo lectura a lectura y escritura:

```
racadm config -g cfgvflashpartition -i 1 -o
cfgvflashPartitionAccessType 1
```
 - Para cambiar una partición de lectura y escritura a solo lectura:

```
racadm config -g cfgvflashpartition -i 1 -o
cfgvflashPartitionAccessType 0
```
 - Mediante el comando `set` para cambiar el estado de lectura y escritura de la partición:
 - Para cambiar una partición de solo lectura a lectura y escritura:

```
racadm set iDRAC.vflashpartition.<index>.AccessType 1
```
 - Para cambiar una partición de lectura y escritura a solo lectura:

```
racadm set iDRAC.vflashpartition.<index>.AccessType 0
```
 - Mediante el comando `set` para especificar el tipo de emulación escriba:

```
racadm set iDRAC.vflashpartition.<index>.EmulationType <HDD, Floppy, or
CD-DVD>
```

Conexión o desconexión de particiones

Cuando conecta una o más particiones, estas estarán visibles para el sistema operativo y el BIOS como dispositivos de almacenamiento masivo USB. Cuando conecta varias particiones, estas se enumeran en orden ascendente en el sistema operativo y en el menú del orden de inicio de BIOS, en función del índice asignado.

Si desconecta una partición, esta dejará de ser visible en el sistema operativo y en el menú de orden de inicio del BIOS.

Al conectar o desconectar una partición, se restablece el bus USB del sistema administrado. Esto afecta a las aplicaciones que utilizan vFlash y desconecta las sesiones de medios virtuales de iDRAC.

Antes de conectar o desconectar una partición, asegúrese de lo siguiente:

- La funcionalidad vFlash está activada.
- No se está realizando una operación de inicialización en la tarjeta.
- Dispone de privilegios **Acceder a los medios virtuales**.

Conexión o desconexión de particiones mediante la interfaz web

Para conectar o desconectar particiones:

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Servidor** → **vFlash** → **Administrar**. Aparece la página **Administrar particiones**.
2. En la columna **Conectado**, realice lo siguiente:
 - Seleccione la casilla de las particiones deseadas y haga clic en **Aplicar** para conectarlas.
 - Desactive la casilla de las particiones deseadas y haga clic en **Aplicar** para desconectarlas. Las particiones se conectan o desconectan conforme a las selecciones.

Conexión o desconexión de particiones mediante RACADM

Para conectar o desconectar particiones:

1. Abra una consola Telnet, SSH o de comunicación en serie al sistema e inicie sesión.
2. Utilice uno de los siguientes métodos:
 - Mediante el comando `config`:
 - 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
```
 - Mediante el comando `set`:
 - Para conectar una partición:

```
racadm set iDRAC.vflashpartition.<index>.AttachState 1
```
 - Para desconectar una partición:

```
racadm set iDRAC.vflashpartition.<index>.AttachState 0
```

Comportamiento del sistema operativo para particiones conectadas

Para los sistemas operativos Windows y Linux:

- El sistema operativo controla y asigna las letras de unidad a las particiones conectadas.
- Las particiones de solo lectura son unidades de solo lectura en el sistema operativo.
- El sistema operativo debe admitir el sistema de archivos de una partición conectada. De lo contrario, no podrá leer ni modificar el contenido de la partición desde el sistema operativo. Por ejemplo, en un entorno de Windows, el sistema operativo no puede leer una partición tipo EXT2, que es nativa a Linux. Del mismo modo, en un entorno de Linux, el sistema operativo no puede leer una partición de tipo NTFS, que es nativa a Windows.
- La etiqueta de la partición vFlash es diferente del nombre del volumen de sistema de archivos en el dispositivo USB emulado. Puede cambiar el nombre de volumen del dispositivo USB emulado desde el sistema operativo. Sin embargo, el nombre de la etiqueta de partición almacenado en iDRAC no cambiará.

Eliminación de las particiones existentes

Antes de eliminar el contenido de una partición, asegúrese de lo siguiente:

- La funcionalidad vFlash está activada.
- La tarjeta no está protegida contra escritura.
- La partición no está conectada.
- No se está realizando una operación de inicialización en la tarjeta.

Eliminación de las particiones disponibles mediante la interfaz web

Para eliminar una partición existente:

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Servidor** → **vFlash** → **Administrar**. Aparece la página **Administrar particiones**.
2. En la columna **Eliminar**, haga clic en el icono de eliminación de la partición que desee eliminar. Aparece un mensaje en el que se indica que la partición se eliminará definitivamente.
3. Haga clic en **Aceptar**. Se elimina la partición.

Eliminación de las particiones disponibles mediante RACADM

Para eliminar particiones:

1. Abra una consola Telnet, SSH o de comunicación en serie al sistema e inicie sesión.
2. Introduzca los comandos siguientes:
 - Para eliminar una partición:


```
racadm vflashpartition delete -i 1
```
 - Para eliminar todas las particiones, vuelva a inicializar la tarjeta vFlash SD.

Descarga del contenido de una partición

Puede descargar el contenido de una partición vFlash en el formato **.img** o **.iso** en las ubicaciones siguientes:


- Sistema administrado (desde el que se opera iDRAC)
- Ubicación de red asignada a una estación de administración


Antes de descargar el contenido de una partición, asegúrese de lo siguiente:

- Dispone de privilegios Acceder a los medios virtuales.
- La funcionalidad vFlash 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:

1. En la interfaz web de iDRAC, vaya a **Información general** → **Servidor** → **vFlash** → **Descargar**. Aparece la página **Descargar partición**.
2. Desde el menú desplegable **Etiqueta**, seleccione la partición que desee descargar y haga clic en **Descargar**.

 **NOTA:** En la lista se muestran todas las particiones existentes (excepto las conectadas). La primera partición está seleccionada de manera predeterminada.
3. Especifique la ubicación donde desea guardar el archivo. El contenido de la partición seleccionada se descarga en la ubicación especificada.

 **NOTA:** Si solo se especifica la ubicación de la carpeta, se utilizará la etiqueta de partición como nombre de archivo, junto con la extensión **.iso** para particiones de CD y disco duro e **.img** para particiones de disco flexible y disco duro.

Inicio de una partición


Se puede establecer una partición vFlash conectada como el dispositivo de inicio para la siguiente operación de inicio.

Antes de iniciar una partición, asegúrese de lo siguiente:

- La partición vFlash contiene una imagen de inicio (en formato **.img** o **.iso**) para realizar el inicio desde el dispositivo.
- La funcionalidad vFlash está activada.
- Dispone de privilegios Acceder a los medios virtuales.


Inicio de una partición mediante la interfaz web

Para establecer la partición vFlash como primer dispositivo de inicio, consulte [Configuración del primer dispositivo de inicio](#).

 **NOTA:** Si las particiones vFlash conectadas no figuran en el menú desplegable **Primer dispositivo de inicio**, asegúrese de que el BIOS se haya actualizado a la versión más reciente.


Inicio de una partición mediante RACADM

Para establecer una partición vFlash como el primer dispositivo de inicio, utilice `cfgServerInfo`. Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8) disponible en dell.com/support/manuals.

 **NOTA:** Cuando se ejecuta este comando, la etiqueta de la partición vFlash se establece automáticamente en inicio único (la opción `cfgserverBootOnce` se establece en 1). La opción de inicio único inicia el dispositivo en la partición solo una vez y no lo mantiene como primero sistemáticamente en el orden de inicio.


Uso de SMCLP

La especificación Protocolo de la línea de comandos de Server Management (SMCLP) permite la administración de sistemas basada en CLI. Define un protocolo para los comandos de administración transmitidos a través de secuencias orientadas a caracteres estándares. Este protocolo accede a un Administrador de objetos de modelo de información común (CIMOM) mediante un conjunto de comandos orientados al ser humano. SMCLP es un subcomponente de la iniciativa de Distributed Management Task Force (DMTF) SMASH para agilizar la administración de sistemas entre varias plataformas. La especificación SMCLP, junto con la especificación de direccionamiento de elementos administrados y varios perfiles a las especificaciones de asignación SMCLP, describe los verbos y los destinos de las distintas ejecuciones de tareas de administración.

 **NOTA:** Se presupone que el usuario está familiarizado con la iniciativa Arquitectura de administración de sistemas para el hardware de servidor (SMASH) y las especificaciones SMCLP para el grupo de trabajos de administración (SMWG).

Las especificaciones SM-CLP son un subcomponente de la iniciativa Distributed Management Task Force (DMTF) SMASH para agilizar la administración de servidores entre varias plataformas. La especificación SM-CLP, junto con la especificación de direccionamiento de elementos administrados y varios perfiles a las especificaciones de asignación SM-CLP, describen los verbos y destinos estándares de las distintas ejecuciones de tareas de administración.

SMCLP se aloja desde el firmware de la controladora iDRAC y admite interfaces Telnet, SSH y de conexión en serie. La interfaz SMCLP de iDRAC se basa en la especificación SMCLP versión 1.0 que proporciona la organización DMTF.

 **NOTA:** Es posible acceder a la información acerca de los perfiles, las extensiones y los MOF en delltechcenter.com y a toda la información sobre DMTF disponible en dmtf.org/standards/profiles/.

Los comandos SM-CLP implementan un subconjunto de comandos de RACADM local. Los comandos son de utilidad para la creación de secuencias de comandos, ya que puede ejecutarlos desde una línea de comandos de la estación de administración. Puede recuperar la salida de los comandos en formatos bien definidos, incluido XML, lo que facilita la creación de secuencias de comandos e integración con las herramientas de informes y administración existentes.

Capacidades de System Management mediante SMCLP

SMCLP de iDRAC permite:

- Administración de la alimentación del servidor: encender, apagar o reiniciar el sistema
- Administración de registro de sucesos del sistema (SEL): mostrar o borrar las anotaciones del registro de sucesos del sistema
- Administración de la cuenta de usuario de iDRAC

- Ver las propiedades del sistema


Ejecución de los comandos SMCLP

Puede ejecutar los comandos SMCLP mediante la interfaz SSH o Telnet. Abra una interfaz SSH o Telnet e inicie sesión en iDRAC como administrador. Aparecerá el símbolo del sistema de SMCLP (admin ->).

Símbolos del sistema de SMCLP:

- Los servidores Blade yx1x utilizan -\$.
- Los servidores tipo bastidor y torre yx1x utilizan admin->.
- Los servidores Blade, bastidor y torre yx2x utilizan admin->.

donde, y es un carácter alfanumérico, tal como M (para servidores Blade), R (para servidores tipo bastidor) y T (para servidores tipo torre) y x es un número. Esto indica la generación de servidores Dell PowerEdge.

 **NOTA:** Las secuencias de comandos -\$ puede utilizar estos para sistemas yx1x. Sin embargo, a partir de los sistemas yx2x se puede utilizar una secuencia de comandos con admin-> para los servidores tipo Blade, bastidor y torre.

Sintaxis SMCLP de iDRAC

SMCLP de iDRAC utiliza el concepto de verbos y destinos para proporcionar a los sistemas capacidades de administración a través de la CLI. El verbo indica la operación que se debe realizar y el destino determina la entidad o el objeto que ejecuta la operación.

La sintaxis de la línea de comandos de SMCLP es la siguiente:

```
<verb> [<options>] [<target>] [<properties>]
```

En la tabla siguiente se proporcionan los verbos y sus definiciones.

Tabla 30. Verbos de SMCLP

| Verbo | Definición |
|-------|--|
| cd | Navega en el MAP mediante el shell |
| set | Establece una propiedad para un valor específico |
| help | Muestra la ayuda de un destino específico |
| reset | Restablece el destino |
| show | Muestra las propiedades del destino, los verbos y los destinos secundarios |
| start | Activa un destino |
| stop | Desactiva un destino |
| exit | Cierra la sesión del shell de SMCLP |

| Verbo | Definición |
|--------------|---|
| version | Muestra los atributos de versión de un destino |
| load | Lleva una imagen binaria de una URL a una dirección de destino especificada |

En la tabla siguiente se proporciona una lista de destinos.

Tabla 31. Destinos de SMCLP

| Destino | Definiciones |
|--|---|
| admin1 | Dominio de admin |
| admin1/profiles1 | Perfiles registrados en iDRAC |
| admin1/hdwr1 | Hardware |
| admin1/system1 | Destino del sistema administrado |
| admin1/system1/capabilities1 | Capacidades de recopilación del sistema administrado SMASH |
| admin1/system1/capabilities1/pwrcap1 | Capacidades de utilización de la alimentación del sistema administrado |
| admin1/system1/capabilities1/elecapi1 | Capacidades de destino del sistema administrado |
| admin1/system1/logs1 | Destino de las recopilaciones de registro |
| admin1/system1/logs1/log1 | Entrada de registro de sucesos del sistema (SEL) |
| admin1/system1/logs1/log1/record* | Una entrada individual del registro de sucesos del sistema en el sistema administrado |
| admin1/system1/settings1 | Configuración de recopilación del sistema administrado SMASH |
| admin1/system1/capacities1 | Capacidades de recopilación del sistema administrado SMASH |
| admin1/system1/consoles1 | Recopilación SMASH de las consolas del sistema administrado |
| admin1/system1/sp1 | Procesador de servicio |
| admin1/system1/sp1/timesvc1 | Servicio de hora del procesador de servicio |
| admin1/system1/sp1/capabilities1 | Recopilación SMASH de las capacidades del procesador de servicio |
| admin1/system1/sp1/capabilities1/clpcap1 | Capacidades del servicio CLP |

| Destino | Definiciones |
|--|--|
| admin1/system1/sp1/capabilities1/pwrmgtcap1 | Capacidades del servicio de administración del estado de la alimentación en el sistema |
| admin1/system1/sp1/capabilities1/acctmgtcap* | Capacidades del servicio de administración de cuentas |
| admin1/system1/sp1/capabilities1/rolemgtcap* | Capacidades de administración basada en funciones locales |
| admin1/system1/sp1/capabilities/PwrutilmgTCap1 | Capacidades de administración de utilización de la alimentación |
| admin1/system1/sp1/capabilities1/elecapi | Capacidades de autenticación |
| admin1/system1/sp1/settings1 | Recopilación de configuración del procesador de servicio |
| admin1/system1/sp1/settings1/clpsetting1 | Datos de configuración del servicio CLP |
| admin1/system1/sp1/clpsvc1 | Servicio de protocolo del servicio CLP |
| admin1/system1/sp1/clpsvc1/clpendpt* | Punto final del protocolo del servicio CLP |
| admin1/system1/sp1/clpsvc1/tcpendpt* | Punto final TCP del protocolo del servicio CLP |
| admin1/system1/sp1/jobq1 | Cola de trabajo del protocolo del servicio CLP |
| admin1/system1/sp1/jobq1/job* | Trabajo del protocolo del servicio CLP |
| admin1/system1/sp1/pwrmgtsvc1 | Servicio de administración del estado de la alimentación |
| admin1/system1/sp1/account1-16 | Cuenta de usuario local |
| admin1/sysetm1/sp1/account1-16/identity1 | Cuenta de identidad de usuario local |
| admin1/sysetm1/sp1/account1-16/identity2 | Cuenta de identidad de IPMI (LAN) |
| admin1/sysetm1/sp1/account1-16/identity3 | Cuenta de identidad de IPMI (conexión serie) |
| admin1/sysetm1/sp1/account1-16/identity4 | Cuenta de identidad CLP |
| admin1/system1/sp1/acctsvc1 | Servicio de administración de cuentas de usuario local |
| admin1/system1/sp1/acctsvc2 | Servicio de administración de cuentas de IPMI |

| Destino | Definiciones |
|---|---|
| admin1/system1/sp1/acctsvc3 | Servicio de administración de cuentas de CLP |
| admin1/system1/sp1/rolesvc1 | Servicio de autorización basada en roles (RBA) locales |
| admin1/system1/sp1/rolesvc1/Role1-16 | Rol local |
| admin1/system1/sp1/rolesvc1/Role1-16/privilege1 | Privilegio de la rol local |
| admin1/system1/sp1/rolesvc2 | Servicio de RBA de IPMI |
| admin1/system1/sp1/rolesvc2/Role1-3 | Rol de IPMI |
| admin1/system1/sp1/rolesvc2/Role4 | Rol de la comunicación en serie en la LAN (SOL) de IPMI |
| admin1/system1/sp1/rolesvc3 | Servicio CLP de RBA |
| admin1/system1/sp1/rolesvc3/Role1-3 | Rol de CLP |
| admin1/system1/sp1/rolesvc3/Role1-3/privilege1 | Privilegio del rol de CLP |

Enlaces relacionados


[Ejecución de los comandos SMCLP](#)

[Ejemplos de uso](#)

Navegación en el espacio de direcciones de MAP

Los objetos que se pueden administrar mediante SM-CLP se representan mediante destinos organizados en un espacio jerárquico denominado el espacio de direcciones MAP (punto de acceso de capacidad de administración). Una ruta de acceso de dirección específica la ruta de acceso desde la raíz del espacio de direcciones a un objeto de este.

El destino raíz se representa mediante una barra diagonal (/) o una barra diagonal invertida (\). Se trata del punto de inicio predeterminado al iniciar sesión en iDRAC. Navegue hasta la raíz mediante el verbo `cd`.

 **NOTA:** La barra diagonal (/) y la barra diagonal invertida (\) son intercambiables en las rutas de acceso de la dirección SM-CLP. Sin embargo, al final de una línea de comando, el comando continúa en la línea siguiente y se omite cuando el comando se analiza

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 conocer la ubicación actual en el espacio de direcciones. Las abreviaturas `..` y `.` funcionan como en Windows y Linux: `..` hace referencia al nivel principal y `.` hace referencia al nivel actual.

Uso de Show Verb

Para obtener más información acerca de un destino, utilice el verbo `show` en inglés. Este verbo muestra las propiedades, los subdestinos, las asociaciones y una lista de los verbos SM-CLP del destino que se permiten en esa ubicación.

Uso de la opción `-display`

La opción `show -display` permite limitar la salida del comando a una o más propiedades, destinos, asociaciones y verbos. Por ejemplo, para mostrar solamente las propiedades y los destinos de la ubicación actual, utilice el comando siguiente:

```
show -display properties,targets
```

Para mostrar solo ciertas propiedades, indíquelas según se muestra en el siguiente comando:

```
show -d properties=(userid,name) /admin1/system1/sp1/account1
```

Si solo desea mostrar una propiedad, puede omitir los paréntesis.

Uso de la opción `-level`

La opción `show -level` ejecuta la opción `show` sobre niveles adicionales debajo de un destino especificado. Para ver 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 los cuatro formatos para la salida de los verbos de SM-CLP: **text**, **clpcsv**, **keyword** y **clpxml**.

El formato predeterminado es **text** y es la salida que se lee con mayor facilidad. El formato **clpcsv** es un formato de valores separados por coma adecuado para cargar en un programa de hoja de cálculo. El formato **keyword** produce información como una lista de pares de palabras clave=valor en modo de uno por línea. El formato **clpxml** es un documento XML que contiene un elemento XML **response**. DMTF ha especificado los formatos **clpcsv** y **clpxml**, y sus especificaciones se encuentran disponibles en el sitio web de DMTF 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 uso

En esta sección se proporcionan escenarios prácticos para SMCLP:

- [Administración de la alimentación del servidor](#)
- [Administración de SEL](#)

- [Navegación en MAP del destino](#)

Administración de la alimentación del servidor

En los ejemplos siguientes se muestra cómo utilizar SMCLP para realizar operaciones de administración de la alimentación en un sistema administrado.

Escriba los comandos siguientes en el símbolo del sistema SMCLP:

- Para apagar el servidor:

```
stop /system1
```

Aparece el mensaje siguiente:

```
system1 has been stopped successfully
```

- Para activar el servidor:

```
start /system1
```

Aparece el mensaje siguiente:

```
system1 has been started successfully
```

- Para reiniciar el servidor:

```
reset /system1
```

Aparece el mensaje siguiente:

```
system1 has been reset successfully
```

Administración de SEL

En los ejemplos siguientes se muestra cómo utilizar SMCLP para realizar operaciones relacionadas con el SEL en el sistema administrado. Introduzca los comandos siguientes en el símbolo del sistema de SMCLP:

- Para ver el SEL:

```
show/system1/logs1/log1
```

Aparece la siguiente información :

```
/system1/logs1/log1
```

```
Targets:
```

```
Record1
```

```
Record2
```

```
Record3
```

```
Record4
```

```
Record5
```

Properties:

InstanceID = IPMI:BMCI SEL Log

MaxNumberOfRecords = 512

CurrentNumberOfRecords = 5

Name = IPMI SEL

EnabledState = 2

OperationalState = 2

HealthState = 2

Caption = IPMI SEL

Description = IPMI SEL

ElementName = IPMI SEL

Commands:

cd

show

help

exit

version

- Para ver la anotación SEL:

show/system1/logs1/log1

Aparece la siguiente información:

/system1/logs1/log1/record4

Properties:

LogCreationClassName= CIM_RecordLog

CreationClassName= CIM_LogRecord

LogName= IPMI SEL

RecordID= 1

MessageTimeStamp= 20050620100512.000000-000

Description= FAN 7 RPM: fan sensor, detected a failure

ElementName= IPMI SEL Record

Commands:

cd

show

help

exit

version

- Para borrar el SEL:

```
delete /system1/logs1/log1/record*
```

Aparece la siguiente información:

```
All records deleted successfully
```

Navegación en MAP del destino

En los ejemplos siguientes se muestra cómo utilizar el verbo `cd` para navegar por MAP. En todos los ejemplos, se presupone que el destino predeterminado inicial es `/`.

Escriba los comandos siguientes en el símbolo del sistema SMCLP:

- Para navegar al destino del sistema y reiniciar:
cd system1 reset El destino predeterminado actual es `/`.
- Para navegar hacia el registro SEL de destino y mostrar las anotaciones del registro:

```
cd system1
```

```
cd logs1/log1
```

```
show
```

- Para mostrar el destino actual:

```
escriba cd .
```

- Para subir un nivel:


```
escriba cd ..
```

- Para salir:

```
exit
```

Uso del módulo de servicio del iDRAC

El módulo de servicio de iDRAC es una aplicación de software que se recomienda instalar en el servidor (no se instala de manera predeterminada). Este módulo complementa a iDRAC con información de supervisión del sistema operativo. No contiene una interfaz, pero es un complemento para iDRAC, ya que proporciona datos adicionales para trabajar con las interfaces de iDRAC, como la interfaz web, RACADM y WSMAN. Es posible configurar las funciones supervisadas por el módulo de servicio de iDRAC para controlar la CPU y la memoria utilizada en el sistema operativo del servidor.

 **NOTA:** Puede utilizar el módulo de servicio del iDRAC solo si ha instalado la licencia Express o Enterprise del iDRAC.

Antes de utilizar el módulo de servicio del iDRAC, asegúrese de que:


- Tiene privilegios de Inicio de sesión, Configurar y Control del servidor en el iDRAC para activar o desactivar las funciones del módulo de servicio del iDRAC.
- La función de paso del SO a iDRAC está activada a través del bus USB interno en iDRAC.

 **NOTA:**

- Cuando el módulo de servicio del iDRAC se ejecuta por primera vez, activa de manera predeterminada el canal de paso del sistema operativo al iDRAC en el iDRAC. Si desactiva esta función después de instalar el módulo de servicio del iDRAC, debe activarla manualmente en el iDRAC.
- Si el canal de paso del sistema operativo al iDRAC se activa a través de LOM en iDRAC, no se puede utilizar el módulo de servicio de iDRAC.

Instalación del módulo de servicio del iDRAC

Puede descargar e instalar el módulo de servicio del iDRAC desde dell.com/support. Debe tener privilegio de administrador en el sistema operativo del servidor para instalar el módulo de servicio del iDRAC. Para obtener información acerca de la instalación, consulte la *iDRAC Service Module Installation Guide* (Guía de instalación del módulo de servicio del iDRAC) disponible en dell.com/support/manuals.

 **NOTA:** Esta función no es aplicable para los sistemas Dell Precision PR7910.


Sistemas operativos admitidos para el módulo de servicio de iDRAC

Para obtener la lista de sistemas operativos admitidos por el módulo de servicio de iDRAC, consulte *iDRAC Service Module Installation Guide* (Guía de instalación del módulo de servicio de iDRAC) disponible en dell.com/openmanagemanuals.com.

Funciones de supervisión del módulo de servicio del iDRAC

El módulo de servicio del iDRAC proporciona las siguientes funciones de supervisión:

- Ver información sobre el sistema operativo (SO)
- Replicar los registros de Lifecycle Controller en los registros del sistema operativo
- Opciones de recuperación automática del sistema
- Llenado del Instrumental de administración de Windows (WMI) Proveedores de administración
- Integración con el informe de asistencia técnica. Esto se aplica únicamente si se ha instalado el módulo de servicio de iDRAC versión 2.0 o posterior. Para obtener más información, consulte [Generación de un informe de asistencia técnica](#).
- Preparar para quitar SSD PCIe NVMe. Para obtener más información, consulte [iDRACUG_Preparar para quitar SSD PCIe NVMe](#).

 **NOTA:** Las nuevas funciones tales como Proveedores del instrumental de administración de Windows, Preparar para quitar el dispositivo NVMe a través del iDRAC, Automatización de la recopilación del informe de asistencia técnica del SO se admiten solo en los servidores Dell PowerEdge de 13.ª generación con versión del firmware mínima de 2.00.00.00 o posterior.

Información sobre el sistema operativo

OpenManage Server Administrator actualmente comparte la información del sistema operativo y el nombre de host con iDRAC. El módulo de servicio del iDRAC proporciona información similar, como el nombre del sistema operativo, la versión del sistema operativo y el nombre de dominio completamente calificado (FQDN) con el iDRAC. De manera predeterminada, la función de supervisión está activada. No se desactiva si OpenManage Server Administrator está instalado en el sistema operativo host.

En el módulo de servicio del iDRAC versión 2.0 se ha modificado la función de información del sistema operativo con la supervisión de la interfaz de red del sistema operativo. Cuando el iDRAC Service Module versión 2.0 se utiliza con el iDRAC 2.00.00.00, inicia la supervisión de las interfaces de red del sistema operativo. Puede ver esta información mediante la interfaz web del iDRAC, la utilidad RACADM o WSMAN. Para obtener más información, consulte [Visualización de interfaces de red disponibles en el sistema operativo host](#).

Cuando el módulo de servicio del iDRAC versión 2.0 se utiliza con una versión del iDRAC inferior a 2.00.00.00, la información del sistema operativo no proporciona la función de supervisión de la interfaz de red del SO.

Replicar registros de Lifecycle en el registro del sistema operativo

Puede replicar los registros de Lifecycle Controller en los registros del sistema operativo desde el momento en que la función se activa en el iDRAC. Es similar a la replicación del registro de sucesos del sistema (SEL) que realiza OpenManage Server Administrator. Todos los sucesos que tienen la opción **Registro del sistema operativo** seleccionada como destino (en la página **Alertas** o en las interfaces equivalentes de RACADM o WSMAN) se replican en el registro del sistema operativo mediante el módulo de servicio del iDRAC. El conjunto predeterminado de registros que se va a incluir en los registros del sistema operativo es igual que el valor configurado para las alertas o capturas de SNMP.

El módulo de servicio del iDRAC también registra los sucesos ocurridos cuando el sistema operativo no funciona. Los registros del sistema operativo realizados por el módulo de servicio del iDRAC siguen los estándares de registro del sistema IETF para los sistemas operativos basados en Linux.

Si OpenManage Server Administrator está instalado, esta función de supervisión se desactiva para evitar duplicar las anotaciones de SEL en el registro del sistema operativo.

Opciones de recuperación automática del sistema

La función ASR es un temporizador basado en hardware. Si se produce una falla de hardware, es posible que no se invoque el Supervisor de la condición pero el servidor se reinicia como si el interruptor de alimentación estuviera activado. ASR se implementa mediante un temporizador de "pulso" que continuamente cuenta en forma descendente. El Supervisor de la condición con frecuencia recarga el contador para evitar la cuenta regresiva a cero. Si la ASR cuenta en forma descendente hasta cero, se supone que el sistema operativo se ha bloqueado y que el sistema intenta reiniciarse automáticamente.

Puede realizar operaciones de recuperación automática del sistema, tales como reinicio, ciclo de encendido o apagado del servidor después de un intervalo de tiempo especificado. Esta función está activada solo si el temporizador de vigilancia del sistema operativo está desactivado. Si OpenManage Server Administrator está instalado, esta función de supervisión se desactiva para evitar la duplicación de los temporizadores de vigilancia.

Proveedores del Instrumental de administración de Windows

WMI es un conjunto de extensiones para el modelo de controlador de Windows que proporciona una interfaz de sistema operativo a través de la cual los componentes instrumentados proporcionan información y notificaciones. WMI es la implementación de Microsoft de la iniciativa de administración de empresas basadas en web (WBEM) y el Modelo común de información (CIM) de Distributed Management Task Force (DMTF) para administrar el hardware del servidor, los sistemas operativos y las aplicaciones. Los proveedores de WMI permiten la integración con consolas de Systems Management como Microsoft System Center y las secuencias de comandos para administrar servidores Microsoft Windows.

Es posible activar o desactivar la opción de WMI en el iDRAC. El iDRAC expone las clases de WMI a través del módulo de servicio del iDRAC y proporciona la información sobre la condición del servidor. De manera predeterminada, se activa la función de información sobre WMI. El módulo de servicio del iDRAC expone las clases supervisadas de WSMAN en el iDRAC a través de WMI. Las clases se exponen en el espacio de nombres **root/cimv2/dcim**.

Es posible acceder a las clases mediante cualquiera de las interfaces de cliente de WMI estándar. Para obtener más información, consulte los documentos de perfiles.

En el ejemplo siguiente se utiliza la clase DCIM_account para ilustrar la capacidad que proporciona la función de información sobre WMI en el módulo de servicio de iDRAC. Para conocer los detalles de las clases y los perfiles compatibles, consulte la documentación sobre perfiles WSMAN disponible en Dell Tech Center.

| Interfaz CIM | WinRM | WMIC | PowerShell |
|--|---|---|---|
| Enumere las instancias de una clase | <code>winrm e wmi/root/cimv2/dcim/dcim_account</code> | <code>wmic /namespace:\root\cimv2\dcim PATH dcim_account</code> | <code>Get-WmiObject dcim_account -</code> |

| Interfaz CIM | WinRM | WMI | PowerShell |
|--|--|---|---|
| | | | namespace root/
cimv2/dcim |
| Obtenga una instancia específica de una clase | winrm g wmi/root/
cimv2/dcim/
DCIM_Account?
CreationClassName=
DCIM_Account
+Name=iDRAC.Embedded.1#Users.
2+SystemCreationClassName=DCIM_SPComputerSystem
+SystemName=systemmc | wmic /namespace:\
\root\cimv2\dcim
PATH dcim_account
donde
Name="iDRAC.Embedded.1#Users.16" | Get-WmiObject -
Namespace root
\cimv2\dcim -
Class
dcim_account -
filter
"Name='iDRAC.Embedded.1#Users.16'" |
| Obtenga instancias asociadas de una instancia | winrm e wmi/root/
cimv2/dcim/* -
dialect:association
-filter:
{object=DCIM_Account?
CreationClassName=
DCIM_Account
+Name=iDRAC.Embedded.1#Users.
1+SystemCreationClassName=DCIM_SPComputerSystem
+SystemName=systemmc} | wmic /namespace:\
\root\cimv2\dcim
PATH dcim_account
donde
Name='iDRAC.Embedded.1#Users.2'
ASSOC | Get-Wmiobject -
Query "ASSOCIATORS
OF
{DCIM_Account.CreationClassName='DCIM_Account',Name='iDRAC.Embedded.1#Users.2',SystemCreationClassName='DCIM_SPComputerSystem',SystemName='systemmc'}" -namespace
root/cimv2/dcim |
| Obtenga referencias de una instancia | winrm e wmi/root/
cimv2/dcim/* -
dialect:association
-associations -
filter:
{object=DCIM_Account?
CreationClassName=
DCIM_Account
+Name=iDRAC.Embedded.1#Users.
1+SystemCreationClassName=DCIM_SPComputerSystem
+SystemName=systemmc} | No aplicable | Get-Wmiobject -
Query "REFERENCES
OF
{DCIM_Account.CreationClassName='DCIM_Account',Name='iDRAC.Embedded.1#Users.2',SystemCreationClassName='DCIM_SPComputerSystem',SystemName='systemmc'}" -namespace
root/cimv2/dcim |

Coexistencia de OpenManage Server Administrator y módulo de servicio del iDRAC

En un sistema, OpenManage Server Administrator y el módulo de servicio del iDRAC pueden coexistir y seguir funcionando de manera correcta e independiente.

Si ha activado las funciones de supervisión durante la instalación del módulo de servicio del iDRAC, una vez finalizada la instalación y si el módulo de servicio del iDRAC detecta la presencia de OpenManage

Server Administrator, el conjunto de funciones de supervisión que se superponen se desactivan. Si OpenManage Server Administrator se está ejecutando, el módulo de servicio del iDRAC desactiva las funciones de supervisión que se superponen después de iniciar sesión en el sistema operativo y en el iDRAC.

Cuando vuelva a activar estas funciones de supervisión a través de las interfaces del iDRAC después, se realizan las mismas comprobaciones y las funciones se activan según si OpenManage Server Administrator se está ejecutando o no.

Uso del módulo de servicio del iDRAC desde la interfaz web del iDRAC

Para utilizar el módulo de servicio del iDRAC desde la interfaz web del iDRAC:

1. Vaya a **Descripción general** → **Servidor** → **Módulo de servicio**.
Aparece la página **Configuración del módulo de servicio del iDRAC**.
2. Puede ver lo siguiente:
 - Versión del módulo de servicio del iDRAC instalado en el sistema operativo host.
 - Estado de conexión del módulo de servicio del iDRAC con el iDRAC.
3. Para llevar a cabo funciones de supervisión fuera de banda, seleccione una o más de las siguientes opciones:
 - **Información de sistema operativo:** vea la información del sistema operativo.
 - **Replicar registro de Lifecycle en el registro del sistema operativo:** incluya los registros de Lifecycle Controller en los registros del sistema operativo. Esta opción está desactivada si OpenManage Server Administrator está instalado en el sistema.
 - **Información sobre WMI:** incluya la información de WMI.
 - **Acción de recuperación automática del sistema:** realice opciones de recuperación automática en el sistema después de un período de tiempo especificado (en segundos):
 - **Reboot (Reiniciar)**
 - **Apagar el sistema**
 - **Realizar ciclo de encendido del sistema**

Esta opción está desactivada si OpenManage Server Administrator está instalado en el sistema.

Uso del módulo de servicio del iDRAC desde RACADM

Para utilizar el módulo de servicio de iDRAC desde RACADM, use los objetos en el grupo **ServiceModule**. Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8) disponible en dell.com/support/manuals.

Uso de un puerto USB para la administración del servidor

En los servidores Dell PowerEdge de 12.^a generación, todos los puertos USB están dedicados al servidor. En los servidores de 13.^a generación, iDRAC utiliza uno de los puertos USB del panel frontal con propósitos administrativos, tales como el aprovisionamiento previo y la solución de problemas. El puerto tiene un icono para indicar que se trata de un puerto de administración. Todos los servidores de 13.^a generación con panel LCD admiten esta función. Este puerto no está disponible en algunas de las variaciones de modelo 200-500 que se solicitan sin el panel LCD. En tales casos, se recomienda utilizar estos puertos para el sistema operativo del servidor.

Cuando iDRAC utiliza el puerto USB:

- La interfaz de red USB permite el uso de herramientas de administración remota fuera de banda existentes desde un dispositivo portátil, como un equipo portátil, mediante un cable USB de tipo A/A conectado al iDRAC. Se asigna la dirección IP (169.254.0.3) a iDRAC y se asigna la IP 169.254.0.4 al equipo portátil.
- Es posible almacenar un perfil de configuración del servidor en el dispositivo USB y actualizar la configuración del servidor desde el dispositivo USB.

 **NOTA:** Esta función es compatible con:

- Los dispositivos USB con sistema de archivos FAT y una sola partición.
- Toda Tablet Dell Windows 8 y Windows RT, incluidas XPS 10 y Venue Pro 8. Para los dispositivos que contienen el puerto mini USB, como XPS 10 y Venue Pro 8, se debe utilizar la llave On-The-Go (OTG) y un cable de tipo A/A juntos para que funcionen.

Enlaces relacionados

[Configuración de iDRAC mediante el perfil de configuración del servidor en un dispositivo USB](#)

[Acceso a la interfaz de iDRAC por medio de la conexión USB directa](#)

Acceso a la interfaz de iDRAC por medio de la conexión USB directa

En los servidores de 13.^a generación, la nueva función de iDRAC directo permite conectar directamente el puerto USB de un equipo de escritorio o un equipo portátil al puerto USB de iDRAC. Esto permite interactuar directamente con las interfaces de iDRAC (por ejemplo, la interfaz web, RACADM y WSMAN) para lograr una administración y un mantenimiento avanzados de los servidores.

Se debe utilizar un cable tipo A/A para conectar el equipo portátil (una controladora de host USB) al iDRAC en el servidor (un dispositivo USB).


Cuando iDRAC se comporta como un dispositivo USB y el modo de puerto de administración se establece en Automático, el puerto USB siempre está ocupado por iDRAC. El puerto no conmuta automáticamente en el sistema operativo.

Para acceder a la interfaz de iDRAC por medio del puerto USB:

1. Apague las redes inalámbricas y desconéctelas de cualquier otra red de conexión permanente.
2. Asegúrese de que el puerto USB esté activado. Para obtener más información, consulte [Configuración de valores del puerto de administración USB](#).
3. Conecte un cable de tipo A/A del equipo portátil al puerto USB de iDRAC.
El LED de administración (si está presente) se ilumina en color verde y permanece encendido durante dos segundos.
4. Espere a que se asigne la dirección IP a su equipo portátil (169.254.0.3) y al iDRAC (169.254.0.3). Esto puede tardar algunos segundos.
5. Empiece a utilizar las interfaces de red de iDRAC, como la interfaz web, RACADM o WS-Man.
6. Cuando iDRAC utiliza el puerto USB, el indicador LED parpadea indicando actividad. La frecuencia es de cuatro parpadeos por segundo.
7. Después del uso, desconecte el cable.
El LED se apagará.

Configuración de iDRAC mediante el perfil de configuración del servidor en un dispositivo USB

Con la nueva función de iDRAC directo, se puede configurar iDRAC en el servidor. En primer lugar, configure los valores del puerto de administración USB en iDRAC, inserte el dispositivo USB que contiene el perfil de configuración del servidor y, a continuación, importe el perfil de configuración del servidor del dispositivo USB a iDRAC.

 **NOTA:** Los sistemas PowerEdge que no tienen el LCD y el panel de LED no admiten la memoria USB.

Enlaces relacionados

[Configuración de los valores de puerto de administración USB](#)

[Importación de un perfil de configuración del servidor desde un dispositivo USB](#)

Configuración de los valores de puerto de administración USB

Es posible configurar el puerto USB en iDRAC de la siguiente manera:

- Active o desactive el puerto USB del servidor con la configuración del BIOS. Cuando iDRAC se establece en **Todos los puertos apagados** o **Puertos frontales apagados**, también se desactiva el puerto USB administrado. El estado del puerto se puede ver por medio de las interfaces de iDRAC. Si se indica el estado desactivado:
 - iDRAC no procesa un dispositivo USB o el host conectado al puerto USB administrado.
 - Es posible modificar la configuración del puerto USB administrado, pero la configuración no se aplicará hasta que los puertos USB en el panel anterior se activen en el BIOS.
- Establezca el modo de puerto de administración USB que determina si el puerto USB debe ser utilizado por iDRAC o el sistema operativo del servidor:
 - Automático (predeterminado): si un dispositivo USB no es compatible con iDRAC o si el perfil de configuración del servidor no está presente en el dispositivo, el puerto USB se desconecta de iDRAC y se conecta al servidor. Cuando se extrae un dispositivo del servidor, la configuración del puerto se restablece y su uso queda destinado para iDRAC.

- Uso estándar del sistema operativo: el dispositivo USB siempre es utilizado por el sistema operativo.
- iDRAC directo solamente: el dispositivo USB siempre es utilizado por iDRAC.

Es necesario contar con el privilegio de control de servidor para configurar el puerto de administración USB.

Cuando existe un dispositivo USB conectado, la página Inventario del sistema muestra la información del dispositivo USB en la sección Inventario de hardware.

Se registra un suceso en los registros de Lifecycle Controller en las siguientes situaciones:

- El dispositivo se encuentra en modo automático o modo iDRAC y se inserta o se extrae el dispositivo USB.
- El modo de puerto de administración USB se modifica.
- El dispositivo se conmuta automáticamente de iDRAC a sistema operativo.
- El dispositivo se expulsa de iDRAC o de su sistema operativo.

Cuando un dispositivo excede los requisitos de alimentación según lo permitido por la especificación USB, el dispositivo se desconecta y se genera un suceso de sobrecarga con las siguientes propiedades:

- Categoría: condición del sistema
- Tipo: dispositivo USB
- Gravedad: advertencia
- Notificaciones permitidas: correo electrónico, captura SNMP, syslog remoto y sucesos WS.
- Acciones: ninguna

Se muestra un mensaje de error y se registra en el registro de Lifecycle Controller en las siguientes situaciones:

- Se intenta configurar el puerto de administración USB sin el privilegio de usuario de control del servidor.
- iDRAC está usando un dispositivo USB y se intenta modificar el modo de puerto de administración USB.
- iDRAC está usando un dispositivo USB y se extrae el dispositivo.

Configuración de puerto de administración USB mediante la interfaz web

Para configurar el puerto USB:

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Hardware** → **Puerto de administración USB**.
Se mostrará la página **Configurar puerto de administración USB**.
2. En el menú desplegable **Modo de puerto de administración USB**, seleccione cualquiera de las opciones siguientes:
 - **Automático**: iDRAC o el sistema operativo del servidor utilizan el puerto USB.
 - **Uso estándar del sistema operativo**: el sistema operativo del servidor utiliza el puerto USB.
 - **iDRAC directo solamente**: iDRAC utiliza el puerto USB.
3. Desde el iDRAC administrado: en el menú desplegable Configuración XML de USB, seleccione opciones para configurar un servidor mediante la importación de archivos de configuración XML almacenados en una unidad USB:
 - **Desactivado**

- **Activado solamente cuando el servidor contiene configuraciones de credenciales predeterminadas.**
- **Activado**

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

4. Haga clic en **Aplicar** para aplicar la configuración.

Configuración de puerto de administración USB mediante RACADM

Para configurar el puerto de administración USB, utilice los siguientes objetos y subcomandos RACADM:

- Para ver el estado del puerto USB:
`racadm get iDRAC.USB.ManagementPortStatus`
- Para ver la configuración del puerto USB:
`racadm get iDRAC.USB.ManagementPortMode`
- Para modificar la configuración del puerto USB:
`racadm set iDRAC.USB.ManagementPortMode <Automatic|OS|iDRAC|>`
- Para ver el inventario del dispositivo USB:
`racadm hwinventory`
- Para configurar por medio de la configuración de alertas actual:
`racadm eventfilters`

Para obtener más información, consulte *iDRAC RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC) disponible en dell.com/esmmanuals.com.

Configuración del puerto de administración de USB mediante la utilidad de configuración de iDRAC

Para configurar el puerto USB:

1. En la utilidad de configuración de iDRAC, vaya a **Configuración de medios y puertos USB**. Se mostrará la página **Configuración de iDRAC.Configuración de medios y puertos USB**.
2. En el menú desplegable **Modo de puerto de administración de USB**, haga lo siguiente:
 - **Automático:** iDRAC o el sistema operativo del servidor utilizan el puerto USB.
 - **Uso del sistema operativo estándar:** el sistema operativo del servidor utiliza el puerto USB.
 - **iDRAC directo solamente:** iDRAC utiliza el puerto USB.
3. En el menú desplegable **iDRAC directo: XML de configuración USB**, seleccione opciones para configurar un servidor mediante la importación del perfil de configuración del servidor almacenado en una unidad USB:
 - **Desactivado**
 - **Activado mientras el servidor contiene configuraciones de credenciales predeterminadas solamente**
 - **Activado**

Para obtener información acerca de los campos, consulte la *Ayuda en línea de la utilidad de configuración de iDRAC*.

4. Haga clic en **Atrás**, después en **Terminar** y, a continuación, en **Sí** para aplicar la configuración.

Importación de un perfil de configuración del servidor desde un dispositivo USB

Asegúrese de crear un directorio en la raíz de un dispositivo USB denominado **System_Configuration_XML** donde se encuentren los archivos **config.xml** y **control.xml**:

- El perfil de configuración del servidor se encuentra en el subdirectorio **System_Configuration_XML** bajo el directorio raíz del dispositivo USB. Este archivo contiene todos los pares valor-atributo del servidor. Esto incluye atributos de iDRAC, PERC, RAID y BIOS. Es posible editar este archivo para configurar cualquier atributo en el servidor. El nombre de archivo puede ser **<servicetag>-config.xml**, **<modelnumber>-config.xml** o **config.xml**.
- Archivo XML de control: incluye parámetros para controlar la operación de importación y no contiene atributos de iDRAC ni de ningún otro componente del sistema. El archivo de control contiene tres parámetros:
 - Tipo de apagado: ordenado, forzado, sin reinicio.
 - Tiempo de espera (en segundos): 300 como mínimo y 3600 como máximo.
 - Estado de alimentación del host final: encendido o apagado.

Ejemplo de archivo **control.xml**:

```
<InstructionTable> <InstructionRow> <InstructionType>Configuration XML import
Host control Instruction</InstructionType> <Instruction>ShutdownType</
Instruction> <Value>NoReboot</Value>
<ValuePossibilities>Graceful, Forced, NoReboot</ValuePossibilities> </
InstructionRow> <InstructionRow> <InstructionType>Configuration XML import Host
control Instruction</InstructionType> <Instruction>TimeToWait</Instruction>
<Value>300</Value> <ValuePossibilities>Minimum value is 300 -Maximum value is
3600 seconds.</ValuePossibilities> </InstructionRow> <InstructionRow>
<InstructionType>Configuration XML import Host control Instruction</
InstructionType> <Instruction>EndHostPowerState</Instruction> <Value>On</Value>
<ValuePossibilities>On, Off</ValuePossibilities> </InstructionRow></
InstructionTable>
```

Es necesario contar con el privilegio de control del servidor para realizar esta operación.

Para importar el perfil de configuración del servidor desde el dispositivo USB hacia iDRAC:

1. Configure el módulo de administración USB:
 - Establezca **Modo de puerto de administración USB** en **Automático** o **iDRAC**.
 - Establezca el valor de **iDRAC administrado: configuración XML USB** en **Activado con credenciales predeterminadas** o **Activado**.
2. Inserte la memoria USB (que contiene los archivos **configuration.xml** y **control.xml**) en el puerto USB de iDRAC.
3. El perfil de configuración del servidor se descubre en el dispositivo USB en el subdirectorio **System_Configuration_XML** bajo el directorio raíz del dispositivo USB. Se descubre en la secuencia que se indica a continuación:
 - **<servicetag>-config.xml**
 - **<modelnum>-config.xml**
 - **config.xml**
4. Se inicia un trabajo de importación del perfil de configuración del servidor.
Si el perfil no se descubre, la operación se detiene.

Si **iDRAC administrado: configuración XML USB** se establece en **Activado con credenciales predeterminadas** y la contraseña de configuración del BIOS no es nula o si una de las cuentas de usuario de iDRAC se ha modificado, se muestra un mensaje de error y la operación se detiene.

5. El panel LCD y el indicador LED (si está presente) muestran el estado que indica que se ha iniciado un trabajo de importación.
6. Si existe una configuración que debe organizarse y **Tipo de apagado** se especifica como **Sin reinicio** en el archivo de control, se debe reiniciar el servidor para que los valores se configuren. De lo contrario, el servidor se reinicia y la configuración se aplica. Solo cuando el servidor ya está apagado, se aplica la configuración organizada en etapas aunque se establezca la opción **Sin reinicio**.
7. Una vez que se completa el trabajo de importación, el panel LCD o LED indica que el trabajo está completo. Si es necesario reiniciar el sistema, el panel LCD muestra el estado del trabajo como "En pausa, a la espera de reinicio".
8. Si el dispositivo USB queda insertado en el servidor, el resultado de la operación de importación se registra en el archivo **results.xml** en el dispositivo USB.

Mensajes de LCD

Si el panel LCD está disponible, se muestran los siguientes mensajes en una secuencia:

1. Importación: cuando el perfil de configuración del servidor se copia desde el dispositivo USB.
2. Aplicación: cuando el trabajo está en progreso.
3. Completado: cuando el trabajo se ha completado correctamente.
4. Completado con errores: cuando el trabajo se ha completado con errores.
5. Fallido: cuando el trabajo ha fallado.

Para obtener más detalles, consulte el archivo de resultados en el dispositivo USB.

Comportamiento de parpadeo de LED

Si el LED USB está presente, indica lo siguiente:

- Luz verde fija: cuando el perfil de configuración del servidor se copia desde el dispositivo USB.
- Luz verde parpadeante: cuando el trabajo está en progreso.
- Luz verde fija: cuando el trabajo se ha completado correctamente.

Archivo de resultados y registros

Se registra la siguiente información para la operación de importación:

- La importación automática desde USB se registra en el archivo de registro de Lifecycle Controller.
- Si el dispositivo USB queda insertado, los resultados del trabajo se registran en el archivo de resultados que se encuentra en la memoria USB.

Un archivo de resultados denominado **Results.xml** se actualiza o se crea en el subdirectorío con la siguiente información:


- Etiqueta de servicio: los datos se registran después de que la operación de importación ha devuelto un error o una identificación de trabajo.
- ID de trabajo: los datos se registran después de que la operación de importación ha devuelto una identificación de trabajo.
- Fecha de inicio y hora del trabajo: los datos se registran después de que la operación de importación ha devuelto una identificación de trabajo.

- Estado: los datos se registran cuando la operación de importación devuelve un error o cuando los resultados del trabajo están disponibles.

Uso de la sincronización rápida de iDRAC

Unos pocos servidores Dell PowerEdge de 13.^a generación tienen el bisel de sincronización rápida que admite la función de sincronización rápida. Esta función se activa en la administración de servidores con un dispositivo móvil. Esto permite ver y configurar la información de inventario y supervisión, así como configurar los valores básicos de iDRAC (como configuración de credenciales raíz y configuración de primer dispositivo de inicio) que utiliza el dispositivo móvil.

Es posible configurar el acceso a la sincronización rápida del iDRAC para su dispositivo móvil (por ejemplo, OpenManage Mobile) en el iDRAC. Se debe instalar la aplicación OpenManage Mobile en el dispositivo móvil para administrar el servidor mediante la interfaz de Sincronización rápida del iDRAC.

 **NOTA:** Esta función se admite actualmente en los dispositivos móviles con sistema operativo Android.

En la publicación actual, esta característica solo está disponible con los servidores de tipo bastidor Dell PowerEdge R730, R730xd y R630. De manera opcional, se puede comprar un bisel para estos servidores. Por lo tanto, es una venta incremental de hardware y las funcionalidades no dependen de las licencias de software de iDRAC.

El hardware de Sincronización rápida del iDRAC incluye lo siguiente:

- Botón de activación: se debe pulsar este botón para activar la interfaz de sincronización rápida. En una infraestructura de bastidores estrechamente apilados, esto ayuda a identificar y activar el servidor que es el destino para la comunicación. La función de sincronización rápida queda inactiva si no se la utiliza una vez transcurrido el período de inactividad configurado (el valor predeterminado es 30 segundos) o cuando se pulsa la opción para desactivarla.
- LED de actividad: si se desactiva la sincronización rápida, el LED parpadea algunas veces y, a continuación, se apaga. Además, si el temporizador de inactividad configurable se activa, el LED indicador se apaga y desactiva la interfaz.

Después de configurar los valores de sincronización rápida de iDRAC en iDRAC, mantenga el dispositivo móvil cerca del servidor, es decir, a una distancia menor de dos centímetros y, a continuación, lea la información pertinente sobre el servidor y realice la configuración de iDRAC.

Con OpenManage Assistant, es posible:

- Ver información de inventario:
- Ver información de supervisión:
- Configurar los valores de red básicos de iDRAC

Para obtener más información acerca de OpenManage Mobile, consulte *OpenManage Mobile User's Guide* (Guía del usuario de OpenManage Mobile) en dell.com/support/manuals.

Enlaces relacionados

[Configuración de la sincronización rápida de iDRAC](#)

[Uso de dispositivos móviles para ver información de iDRAC](#)

Configuración de la sincronización rápida de iDRAC

Con la interfaz web de iDRAC o RACADM, se puede configurar la función de sincronización rápida de iDRAC para permitir el acceso al dispositivo móvil:

- Acceso: puede especificar cualquiera de las siguientes opciones para configurar el estado de acceso de la función Sincronización rápida del iDRAC:
 - Lectura-escritura: estado predeterminado.
 - Acceso de lectura/escritura: permite configurar los valores básicos de iDRAC.
 - Acceso de solo lectura: permite ver la información de inventario y supervisión.
 - Acceso desactivado: no permite ver información ni configurar valores.
- Tiempo de espera: puede activar o desactivar el temporizador de inactividad de Sincronización rápida del iDRAC:
 - Si está activado, puede especificar una hora después de la cual el modo de Sincronización rápida. Para activarlo, pulse el botón de activación de nuevo.
 - Si está desactivado, el temporizador no le permite introducir un período de tiempo de espera.
- Límite de tiempo de espera: le permite especificar la hora después de la cual se desactiva el modo de Sincronización rápida. El valor predeterminado es 30 segundos.

Es necesario contar con el privilegio de control del servidor para configurar los valores. No se requiere el reinicio del servidor para que la configuración surta efecto.

Se registra una entrada en el registro de Lifecycle Controller cuando se modifica la configuración.

Configuración de los ajustes de sincronización rápida de iDRAC mediante la interfaz web

Para configurar la sincronización rápida de iDRAC:

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Hardware** → **Panel frontal**.
2. En la sección **Sincronización rápida del iDRAC**, en el menú desplegable **Acceso**, seleccione una de las opciones siguientes para proporcionar acceso al dispositivo móvil Android:
 - Lectura/escritura
 - Solo lectura
 - Desactivado
3. Active el temporizador.
4. Especifique el valor de tiempo de espera.
Para obtener más información acerca de los campos, consulte la *Ayuda en línea de iDRAC*.
5. Haga clic en **Aplicar** para aplicar la configuración.

Configuración de los valores de sincronización rápida de iDRAC mediante RACADM

Para configurar la función de sincronización rápida de iDRAC, utilice los objetos racadm en el grupo **System.QuickSync**. Para obtener más información, consulte *iDRAC RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de iDRAC) disponible en dell.com/esmanuals.

Configuración de los valores de sincronización rápida del iDRAC mediante la utilidad de configuración de iDRAC

Para configurar la sincronización rápida del iDRAC:

1. En la utilidad de configuración de iDRAC, vaya a **Seguridad del panel frontal**.
Se mostrará la página **Configuración de iDRAC - Seguridad del panel frontal**.
2. En la sección **Sincronización rápida del iDRAC**:
 - Especifique el nivel de acceso.
 - Active el tiempo de espera.
 - Especifique el límite de tiempo de espera definido por el usuario (de 15 segundos a 3600 segundos).

Para obtener más información acerca de los campos, consulte la *Ayuda en línea de iDRAC*.

3. Haga clic en **Atrás**, en **Terminar** y, a continuación, en **Sí**.
Se aplica la configuración.

Uso de dispositivos móviles para ver información de iDRAC

Para ver la información de iDRAC desde el dispositivo móvil, consulte *OpenManage Mobile User's Guide* (Guía del usuario de OpenManage Mobile) disponible en dell.com/support/manuals para consultar los pasos.

Implementación de los sistemas operativos

Puede utilizar cualquiera de las utilidades siguientes para implementar sistemas operativos en sistemas administrados:

- Interfaz de línea de comandos (CLI) de los medios virtuales
- Consola de medios virtuales
- Recurso compartido de archivos remotos

Enlaces relacionados

[Implementación del sistema operativo mediante VMCLI](#)

[Implementación del sistema operativo mediante recurso compartido de archivos remotos](#)

[Implementación del sistema operativo mediante medios virtuales](#)

Implementación del sistema operativo mediante VMCLI

Antes de implementar el sistema operativo mediante la secuencia de comandos `vmdeploy`, asegúrese de lo siguiente:

- La utilidad VMCLI está instalada en la estación de administración.
- Los privilegios **Configurar Usuario** y **Acceder a los medios virtuales** para iDRAC están activados para el usuario.
- IPMItool está instalada en la estación de administración.
 - ✎ **NOTA:** IPMItool no funciona si IPv6 está configurado en el sistema administrado o en la estación de administración.
- iDRAC está configurado en los sistemas remotos de destino.
- El sistema puede iniciar desde el archivo de imagen.
- IPMI en la LAN está activado en iDRAC.
- El recurso compartido de red contiene controladores y el archivo de imagen iniciable de sistema operativo tiene un formato estándar del sector, tal como **.img** o **.iso**.
 - ✎ **NOTA:** Al crear el archivo de imagen, siga los procedimientos de instalación en red estándares y marque la imagen de implementación como de solo lectura para asegurarse de que cada sistema objetivo inicie y ejecute el mismo procedimiento de implementación.
- Los medios virtuales se encuentran en el estado Conectar.
- La secuencia de comandos **vmdeploy** está instalada en la estación de administración. Consulte este ejemplo de secuencia de comandos `vmdeploy` incluida con VMCLI. Esta describe cómo implementar el sistema operativo en los sistemas remotos de la red. Internamente, utiliza VMCLI e IPMItool.
 - ✎ **NOTA:** La secuencia de comandos **vmdeploy** depende de algunos archivos de compatibilidad del directorio durante la instalación. Para utilizar la secuencia de comandos desde otro directorio, copie todos los archivos correspondientes. Si la utilidad IPMItool no está instalada, copie la utilidad junto con los demás archivos.

Para implementar el sistema operativo en sistemas remotos de destino:

1. Enumere las direcciones IPv4 de iDRAC de los sistemas operativos de destino en el archivo de texto **ip.txt**. Enumere una dirección IPv4 por línea.
2. Inserte un CD o DVD de inicio de sistema operativo en la unidad de la estación de administración.
3. Abra un símbolo del sistema con privilegios de administrador y ejecute la secuencia de comandos **vmdeploy**:

```
vmdeploy.bat -r <iDRAC-IPAddress or file> -u <iDRAC-user> -p <iDRAC-user-  
passwd> [ -f {<floppy-image> | < device-name>} | -c { <device-name>|<image-  
file>} ] [-i <DeviceID>]
```



NOTA: vmdeploy no admite IPv6, porque IPv6 no admite la herramienta IPMI.



NOTA: La secuencia de comandos vmdeploy procesa la opción `-r` de manera ligeramente diferente que la opción `vmcli -r`. Si el argumento para la opción `-r` es el nombre de un archivo existente, la secuencia de comandos lee las direcciones IPv4 o IPv6 de iDRAC desde el archivo especificado y ejecuta la utilidad una vez por línea. Si el argumento para la opción `-r` no es un nombre de archivo, debería ser una única dirección de iDRAC. En este caso, la opción `-r` funciona según se describe para la utilidad VMCLI.

En la tabla siguiente se describen los parámetros de comando de vmdeploy.

Tabla 32. Parámetros de comando de vmdeploy

| Parámetro | Descripción |
|---|--|
| <iDRAC-user> | Nombre de usuario de iDRAC. Debe tener los siguientes atributos: <ul style="list-style-type: none">• Nombre de usuario válido• Permiso de usuario de medios virtuales de iDRAC Si la autenticación de iDRAC falla, aparece un mensaje de error y el comando finaliza. |
| <iDRAC-ip file> | Dirección IP de iDRAC o archivo que contiene la dirección IP de iDRAC. |
| <iDRAC-user-password> or <iDRAC-passwd> | Contraseña del usuario de iDRAC. Si la autenticación de iDRAC falla, aparece un mensaje de error y el comando finaliza. |
| -c {<device-name> <image-file>} | Ruta de acceso a una imagen ISO9660 del CD o DVD de instalación del sistema operativo. |
| <floppy-device> | Ruta de acceso al dispositivo que contiene el CD, DVD o disco flexible de instalación del sistema operativo. |
| <floppy-image> | Ruta de acceso a una imagen de disco flexible válido. |

| Parámetro | Descripción |
|-------------|-------------------------------------|
| <Device ID> | ID del dispositivo de inicio único. |

Enlaces relacionados


[Configuración de medios virtuales](#)

[Configuración de iDRAC](#)

Implementación del sistema operativo mediante recurso compartido de archivos remotos

Antes de implementar el sistema operativo mediante el recurso compartido de archivos remotos (RFS), asegúrese de lo siguiente:

- Los privilegios **Configurar Usuario** y **Acceder a los medios virtuales** para iDRAC están activados para el usuario.
- El recurso compartido de red contiene controladores y el archivo de imagen iniciable de sistema operativo tiene un formato estándar del sector, tal como **.img** o **.iso**.

 **NOTA:** Al crear el archivo de imagen, siga los procedimientos de instalación en red estándares y marque la imagen de implementación como de solo lectura para asegurarse de que cada sistema objetivo inicie y ejecute el mismo procedimiento de implementación.

Para implementar un sistema operativo mediante RFS:

1. Con el recurso compartido de archivos remotos (RFS), coloque la imagen ISO o IMG en el sistema administrado a través de NFS o CIFS.
2. Vaya a **Descripción general** → **Configuración** → **Primer dispositivo de inicio**.
3. Establezca el orden de inicio de la lista desplegable **Primer dispositivo de inicio** en **Recurso compartido de archivos remotos**.
4. Seleccione la opción **Inicio único** para activar el sistema administrado de modo que se reinicie mediante el archivo de imagen solo para la instancia siguiente.
5. Haga clic en **Apply (Aplicar)**.
6. Reinicie el sistema administrado y siga las instrucciones en pantalla para completar la implementación.

Enlaces relacionados

[Administración de recursos compartidos de archivos remotos](#)

[Configuración del primer dispositivo de inicio](#)


Administración de recursos compartidos de archivos remotos

Mediante la función de recursos compartidos de archivos remotos (RFS), puede establecer un archivo de imagen ISO o IMG en un recurso compartido de red y ponerlo a disposición del sistema operativo del servidor administrado como una unidad virtual. Para ello, móntelo como un CD o DVD mediante NFS o CIFS. Esta función requiere licencia.

 **NOTA:** Las direcciones IPv4 se admiten para CIFS y NFS, y las direcciones IPv6 solo se admite para CIFS.

Los recursos compartidos de archivos remotos solo admiten formatos de archivo **.img** e **.iso**. Un archivo **.img** se redirige como un disco flexible virtual y un archivo **.iso** se redirige como un CDROM virtual.

Debe tener privilegios de medios virtuales para realizar un montaje de RFS.


 **NOTA:** Si ESXi se está ejecutando en el sistema administrado y monta una imagen de disco flexible (.img) mediante RFS, la imagen del disco flexible conectado no está disponible para el sistema operativo ESXi.

Las funciones RFS y Medios virtuales son mutuamente exclusivas.

- Si el cliente de medios virtuales no está activo e intenta establecer una conexión con RFS, la conexión se establecerá y la imagen remota estará disponible para el sistema operativo host.
- Si el cliente de medios virtuales está activo e intenta establecer una conexión con RFS, aparecerá el siguiente mensaje de error:

Los medios virtuales están desconectados o redirigidos para la unidad virtual seleccionada.

El estado de conexión de RFS está disponible en el registro de iDRAC. Una vez conectada, una unidad virtual montada mediante RFS no se desconecta aunque se cierre la sesión de iDRAC. La conexión de RFS se cierra si iDRAC se reinicia o si se interrumpe la conexión de red. También existen opciones de la interfaz web y de la línea de comandos disponibles en CMC e iDRAC para cerrar la conexión de RFS. La conexión de RFS de CMC siempre invalida una unidad montada mediante RFS existente en iDRAC.

 **NOTA:** La función vFlash de iDRAC y RFS no tienen relación.

Si actualiza el firmware del iDRAC de la versión de firmware 1.30.30 a la 1.50.50 mientras existe una conexión de RFS activa y el modo de conexión de medios virtuales está establecido en **Conectar** o **Conectar automáticamente**, el iDRAC intenta volver a establecer la conexión del RFS una vez finalizada la actualización del firmware y el iDRAC se reinicia.

Si actualiza el firmware del iDRAC de la versión de firmware 1.30.30 a la 1.50.50 mientras existe una conexión de RFS activa y el modo de conexión de medios virtuales está establecido en **Desconectar**, el iDRAC no intenta volver a establecer la conexión del RFS una vez finalizada la actualización del firmware y el iDRAC se reinicia.


Configuración de recursos compartidos de archivos remotos mediante la interfaz web

Para activar el uso compartido de archivos remotos:

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Servidor** → **Medios conectados**. Aparece la página **Medios conectados**.
2. En **Medios conectados**, seleccione **Conectar** o **Conectar automáticamente**.
3. En **Recurso compartido de archivos remoto**, especifique la ruta de acceso del archivo de imagen, el nombre de dominio, el nombre de usuario y la contraseña. Para obtener información acerca de los campos, consulte la *Ayuda en línea de iDRAC7*.

Ejemplo de ruta de acceso de un archivo de imagen:

- CIFS: //<IP para conexión para sistema de archivos CIFS>/<ruta de archivo>/<nombre de imagen>
- NFS: <IP para conexión para sistema de archivos NFS>:/<ruta de archivo>/<nombre de imagen>


 **NOTA:** Los caracteres '/' o '\' se pueden utilizar para la ruta de archivo.

CIFS admite las dos direcciones IPv4 e IPv6 pero NFS admite solamente la dirección IPv4.

Si está utilizando un recurso compartido de NFS, asegúrese de introducir la <ruta de acceso del archivo> y el <nombre de la imagen> exactos ya que distingue mayúsculas de minúsculas.


Se admiten los siguientes caracteres para la ruta de acceso del archivo de imagen, el nombre de usuario y la contraseña:

- Caracteres en mayúsculas
- Caracteres en minúsculas
- dígitos de 0 a 9
- `_`, `-`, `?`, `<`, `>`, `/`, `\`, `:`, `*`, `|`, `@`
- Espacio en blanco

 **NOTA:** Mientras se especifica la configuración para el recurso compartido de red, se recomienda evitar el uso de caracteres especiales en el nombre de usuario y la contraseña o codificar por porcentaje los caracteres especiales.

4. Haga clic en **Aplicar** y, después, en **Conectar**.

Una vez establecida la conexión, la opción **Estado de conexión** muestra la opción **Conectado**.

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

Para los distribuidores de Linux, es posible que esta función requiera un comando de montaje manual cuando se trabaja en el nivel de ejecución init 3. La sintaxis del comando es la siguiente:

```
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 flexible es `/dev/sdc`. Para asegurarse de utilizar el dispositivo correcto (para SLES o RHEL), al conectarse al dispositivo virtual, en Linux debe ejecutar el comando siguiente inmediatamente:

```
tail /var/log/messages | grep SCSI
```

Esto muestra texto que identifica el dispositivo (por ejemplo, `sdc` del dispositivo SCSI). Este procedimiento también se aplica a los medios virtuales cuando utiliza distribuciones Linux en el nivel de ejecución init 3. De manera predeterminada, los medios virtuales no se montan automáticamente en init 3.

Configuración de recursos compartidos de archivos remotos mediante RACADM

Para configurar el uso compartido de archivos remotos mediante RACADM, utilice los comandos siguientes:

```
racadm remoteimage
```

```
racadm remoteimage <options>
```

Las opciones son:

`-c`: conectar imagen


-d: desconectar imagen

-u <nombredeusuario>: nombre de usuario para acceder al recurso compartido de red

-p <contraseña>: contraseña para acceder al recurso compartido de red

-l <ubicación_de_imagen>: ubicación de la imagen en el recurso compartido de red; use comillas alrededor de la ubicación. Para ver ejemplos de rutas de acceso de archivos de imagen, consulte la sección Configuración de recursos compartidos de archivos remotos con la interfaz web

-s: mostrar el estado actual

 **NOTA:** Todos los caracteres, incluidos los especiales y alfanuméricos, están permitidos para nombre de usuario, contraseña y ubicación_de_imagen excepto los siguientes caracteres: ' (comilla simple), " (comillas), , (comas), < (signo de menor que) y > (signo de mayor que).

Implementación del sistema operativo mediante medios virtuales

Antes de implementar el sistema operativo mediante medios virtuales, asegúrese de lo siguiente:

- Los medios virtuales deben estar en el estado *Conectado* para que las unidades virtuales aparezcan en la secuencia de inicio.
- Si los medios virtuales se encuentran en modo *Conectado automáticamente*, la aplicación de medios virtuales debe iniciarse antes de iniciar el sistema.
- El recurso compartido de red contiene controladores y el archivo de imagen iniciable de sistema operativo tiene un formato estándar del sector, tal como **.img** o **.iso**.

Para implementar un sistema operativo mediante medios virtuales:

1. Realice uno de los siguientes pasos:
 - Inserte el CD o DVD de instalación del sistema operativo en la unidad correspondiente de la estación de administración.
 - Conecte la imagen del sistema operativo.
2. Seleccione la unidad en la estación de administración con la imagen necesaria para asignarla.
3. Utilice uno de los métodos siguientes para iniciar el dispositivo necesario:
 - Establezca el orden de inicio de inicio único desde **Disco flexible virtual** o **CD/DVD/ISO virtual** mediante la interfaz web de iDRAC.
 - Establezca el orden de inicio a través de **Configuración del sistema** → **Configuración del BIOS del sistema** presionando <F2> durante el inicio.
4. Reinicie el sistema administrado y siga las instrucciones en pantalla para completar la implementación.

Enlaces relacionados

[Configuración de medios virtuales](#)

[Configuración del primer dispositivo de inicio](#)

[Configuración de iDRAC](#)

Instalación del sistema operativo desde varios discos

1. Anule la asignación del CD/DVD existente.
2. Inserte el siguiente CD/DVD en la unidad óptica remota.
3. Vuelva a asignar la unidad CD/DVD.

Implementación del sistema operativo incorporado en la tarjeta SD

Para instalar un hipervisor incorporado en una tarjeta SD:

1. Inserte dos tarjetas SD en las ranuras IDSDM (módulo SD dual interno) del sistema.
2. Active el módulo SD y la redundancia del BIOS (si fuera necesario).
3. Compruebe que la tarjeta SD está disponible en una de las unidades al presionar <F11> durante el inicio.
4. Implemente el sistema operativo incorporado y siga las instrucciones de instalación correspondientes.

Enlaces relacionados

[Acerca de IDSDM](#)

[Activación del módulo SD y la redundancia del BIOS](#)

Activación del módulo SD y la redundancia del BIOS

Para activar el módulo SD y la redundancia del BIOS:

1. Presione <F2> durante el inicio.
2. Vaya a **Configuración del sistema** → **Configuración del BIOS del sistema** → **Dispositivos integrados**.
3. Configure la opción **Puerto USB interno** como **Activado**. Si se configura como **Desactivado**, el IDSDM no estará disponible como dispositivo de inicio.
4. Si no se necesita redundancia (una sola tarjeta SD), configure la opción **Puerto de tarjeta SD interno** como **Activado** y la opción **Redundancia de la tarjeta SD interna** como **Desactivado**.
5. Si se necesita redundancia (dos tarjetas SD), establezca la opción **Puerto de tarjeta SD interno** en **Activado** y la opción **Redundancia de la tarjeta SD interna** en **Reflejar**.
6. Haga clic en **Atrás** y luego en **Terminar**.
7. Haga clic en **Sí** para guardar la configuración y presione <Esc> para salir de **Configuración del sistema**.

Acerca de IDSDM

IDSDM (módulo SD dual interno) solo está disponible en las plataformas aplicables y proporciona redundancia en la tarjeta SD del hipervisor al utilizar otra tarjeta SD que refleja el contenido de la primera tarjeta SD.

Cualquiera de las dos tarjetas SD puede ser el maestro. Por ejemplo, si se instalan dos tarjetas SD nuevas en el IDSDM, SD1 es la tarjeta activa (maestra) y SD2 es la tarjeta de respaldo. Los datos se graban en ambas tarjetas, pero se leen de la tarjeta SD1. Si la tarjeta SD1 falla o se quita, la tarjeta SD2 se convierte automáticamente en la tarjeta activa (maestra).

Es posible ver el estado, la condición y la disponibilidad de IDSDM mediante la interfaz web de iDRAC o RACADM. El estado de redundancia de la tarjeta SD y sus sucesos de falla se registran en SEL, que se muestra en el panel anterior, y se generan alertas PET si se ha activado esa opción.

Enlaces relacionados

[Visualización de la información del sensor](#)

Solución de problemas de Managed System mediante iDRAC

Puede diagnosticar y solucionar los problemas de un sistema administrado mediante los elementos siguientes:

- Consola de diagnósticos
- Código de la POST
- Videos de captura de inicio y bloqueo
- Pantalla de último bloqueo del sistema
- Registros de sucesos del sistema
- Registros de Lifecycle
- Estado del panel frontal
- Indicadores de problemas
- Condición del sistema

Enlaces relacionados

- [Uso de la consola de diagnósticos](#)
- [Programación del diagnóstico automatizado remoto](#)
- [Visualización de los códigos de la POST](#)
- [Visualización de videos de captura de inicio y bloqueo](#)
- [Visualización de registros](#)
- [Visualización de la pantalla de último bloqueo del sistema](#)
- [Visualización del estado del panel frontal](#)
- [Indicadores de problemas del hardware](#)
- [Visualización de la condición del sistema](#)
- [Generación de un informe de asistencia técnica](#)

Uso de la consola de diagnósticos

iDRAC proporciona un conjunto estándar de herramientas de diagnóstico de red similares a las herramientas que se incluyen con sistemas basados en Microsoft Windows o Linux. Mediante la interfaz web de iDRAC, es posible acceder a las herramientas de depuración de la red.

Para acceder a la consola de diagnósticos:

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Servidor** → **Solución de problemas** → **Diagnósticos**.
2. En el cuadro **Comando**, introduzca un comando y haga clic en **Enviar**. Para obtener más información acerca de los comandos, consulte *iDRAC Online Help* (Ayuda en línea de iDRAC). Los resultados se muestran en la misma página.

Programación del diagnóstico automatizado remoto

Puede invocar en forma remota el diagnóstico automatizado fuera de línea en un servidor como un suceso de una sola vez y devolver los resultados. Si el diagnóstico requiere un reinicio, puede reiniciar inmediatamente o apilarlo para un ciclo de reinicio o mantenimiento subsiguiente (similar a las actualizaciones). Cuando se ejecutan los diagnósticos, los resultados se recopilan y almacenan en el almacenamiento interno del iDRAC. A continuación, puede exportar los resultados en un recurso compartido de red CIFS o NFS mediante el comando `racadm diagnostics export`. También puede ejecutar los diagnósticos mediante el comando adecuado de WSMAN. Para obtener más información, consulte la documentación de WSMAN.

Es necesario tener la licencia iDRAC Express para usar los diagnósticos automatizados remotos.

Puede realizar los diagnósticos inmediatamente o programarlos para un día y horario determinados y especificar el tipo de diagnóstico y el tipo de reinicio.

Para el programa debe especificar lo siguiente:

- Hora de inicio: ejecute el diagnóstico en un día y horario futuros. Si especifica TIME NOW, el diagnóstico se ejecuta en el próximo reinicio.
- Hora de finalización: ejecute el diagnóstico hasta un día y horario posterior a la hora de inicio. Si no se inicia en la hora de finalización, se marca como fallido con Hora de finalización caducada. Si especifica TIME NA, no se aplica el tiempo de espera.

Los tipos de pruebas de diagnóstico son:

- Prueba rápida
- Prueba extendida
- Ambas en una secuencia

Los tipos de reinicio son:

- Ciclo de encendido del sistema
- Apagado ordenado (se espera a que se apague o reinicie el sistema operativo)
- Apagado ordenado forzado (le indica al sistema operativo que debe apagarse y espera 10 minutos. Si no se apaga, el iDRAC realiza un ciclo de encendido del sistema)

Solo puede programarse o ejecutarse un trabajo de diagnóstico a la vez. Un trabajo de diagnóstico puede finalizar satisfactoriamente, finalizar con errores o finalizar de manera incorrecta. Los sucesos de diagnóstico y los resultados se graban en el registro de Lifecycle Controller. Puede recuperar los resultados de la última ejecución del diagnóstico mediante RACADM remoto o WSMAN.

Puede exportar los resultados del diagnóstico de los últimos diagnósticos finalizados que se programaron en forma remota a un recurso compartido de red como CIFS o NFS. El tamaño máximo del archivo es de 5 MB.

Puede cancelar un trabajo de diagnóstico cuando el estado del trabajo es No programado o Programado. Si el diagnóstico se está ejecutando, reinicie el sistema para cancelarlo.

Antes de ejecutar el diagnóstico remoto, asegúrese de lo siguiente:

- Lifecycle Controller está activado.

- Cuenta con privilegios de Inicio de sesión y Control del servidor.

Programación de diagnóstico automatizado remoto mediante RACADM

Para ejecutar los diagnósticos remotos y guardar los resultados en el sistema local, utilice el siguiente comando:

```
racadm diagnostics run -m <Mode> -r <reboot type> -s <Start Time> -e  
<Expiration Time>
```

Para exportar los resultados del último diagnóstico remoto ejecutado, utilice el siguiente comando:

```
racadm diagnostics export -f <file name> -l <NFS / CIFS share> -u <username> -p  
<password>
```

Para obtener más información acerca de las opciones, consulte *iDRAC8 RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8) disponible en dell.com/support/manuals.

Visualización de los códigos de la POST

Los códigos de la POST son indicadores de progreso del BIOS del sistema que indican las distintas etapas de la secuencia de inicio a partir de la operación de encendido al restablecer. También permiten diagnosticar los errores relacionados con el inicio del sistema. En la página **Códigos de la POST** se muestra el último código de la POST del sistema antes de iniciar el sistema operativo.

Para ver los códigos de la POST, vaya a **Información general** → **Servidor** → **Solución de problemas** → **Código de la POST**.

En la página **Código de la POST** se muestra un indicador de la condición del sistema, un código hexadecimal y una descripción del código.


Visualización de videos de captura de inicio y bloqueo

Puede ver las grabaciones de video de los elementos siguientes:

- Últimos tres ciclos de inicio: un vídeo de ciclo de inicio registra la secuencia de los sucesos para un ciclo de inicio. Estos videos se organizan en el orden del más reciente al más antiguo.
- Último video de bloqueo: un video de bloqueo registra la secuencia de sucesos que llevan al error.

Esta es una función con licencia.

iDRAC registra cincuenta fotogramas durante el tiempo de inicio. La reproducción de las pantallas de inicio se realiza a una velocidad de 1 fotograma por segundo. Si se restablece iDRAC, el vídeo de captura de inicio no estará disponible, ya que se almacena en la memoria RAM y se elimina durante el proceso.

 **NOTA:** Debe disponer privilegios de acceso a la consola virtual o de administrador para reproducir los videos de captura de inicio y captura de bloqueo.

Para ver la pantalla **Captura de inicio**, haga clic en **Descripción general** → **Servidor** → **Solución de problemas** → **Captura de video**.

Se muestra la pantalla **Captura de video**. Para obtener más información, consulte *iDRAC Online Help* (Ayuda en línea de iDRAC).

Configuración de los valores de captura de video

Para configurar los valores de captura de video:

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Servidor** → **Solución de problemas** → **Captura de video**.
Aparecerá la página **Captura de video**.
2. En el menú desplegable **Configuración de captura de video**, seleccione cualquiera de las opciones siguientes:
 - **Desactivar**: se desactiva la captura de inicio.
 - **Capturar hasta que el búfer esté completo**: la secuencia de inicio se captura hasta que haya alcanzado el tamaño del búfer.
 - **Capturar hasta el final de POST**: la secuencia de inicio se captura hasta el final de POST.
3. Haga clic en **Aplicar** para aplicar la configuración.

Visualización de registros

Es posible visualizar los registros de sucesos del sistema (SEL) y los registros de Lifecycle. Para obtener más información, consulte [Visualización del registro de sucesos del sistema](#) y [Visualización del registro de Lifecycle](#).

Visualización de la pantalla de último bloqueo del sistema

La función de la pantalla de último bloqueo captura una pantalla del bloqueo del sistema más reciente, la guarda y la muestra en iDRAC. Esta función requiere una licencia.

Para ver la pantalla de último bloqueo:

1. Asegúrese de que la función de pantalla de último bloqueo esté activada.
2. En la interfaz web de iDRAC, vaya a **Descripción general** → **Servidor** → **Solución de problemas** → **Pantalla de último bloqueo**.

La página **Pantalla de último bloqueo** muestra la pantalla de último bloqueo guardada desde el sistema administrado.

Haga clic en **Borrar** para eliminar la pantalla de último bloqueo.

Enlaces relacionados

[Activación de la pantalla de último bloqueo](#)

Visualización del estado del panel frontal

En el panel frontal del sistema administrado se proporciona un resumen del estado de los siguientes componentes del sistema:

- Baterías
- Ventiladores
- Intrusión
- Fuentes de alimentación
- Medios flash extraíbles

- Temperaturas
- Voltajes

Puede ver el estado del panel frontal del sistema administrador:

- Servidores tipo bastidor y torre: estado del LED de ID del sistema y del panel frontal LCD o el estado del LED de ID del sistema de panel frontal LED.
- Servidores Blade: solo los LED de ID del sistema.

Visualización del estado del LCD del panel frontal del sistema

Para ver el estado de panel anterior LCD para los servidores tipo bastidor y torre aplicables, en la interfaz web de iDRAC, vaya a **Descripción general** → **Hardware** → **Panel anterior**. Se muestra la página **Panel anterior**.

En la sección **Fuente en directo del panel frontal** se muestran las fuentes en directo de los mensajes que aparecen en el panel frontal LCD. Cuando el sistema funciona correctamente (indicado por un color azul sólido en el panel frontal LCD), las opciones **Ocultar error** y **Mostrar error** están atenuadas. Puede ocultar o mostrar los errores solamente para los servidores tipo bastidor y torre.

Para ver el estado de panel anterior LCD con RACADM, utilice los objetos en el grupo `System.LCD`. Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8) disponible en dell.com/support/manuals.

Enlaces relacionados

[Configuración de los valores de LCD](#)

Visualización del estado del LED del panel frontal del sistema

Para ver el estado actual de un LED de ID del sistema, en la interfaz web de iDRAC, vaya a **Descripción general** → **Hardware** → **Panel frontal**. En la sección **Fuente de panel de panel frontal en directo**, se muestra el estado actual del panel frontal:

- Azul sólido: no hay errores presentes en el sistema administrado.
- Azul parpadeante: el modo de identificación está activado (independientemente de la presencia de un error del sistema administrado).
- Ámbar sólido: el sistema administrado está en el modo a prueba de fallas.
- Ámbar parpadeante: hay errores presentes en el sistema administrado.

Cuando el sistema funciona correctamente (indicado por un icono de estado de color azul en el panel frontal LED), las opciones **Ocultar error** y **Mostrar error** quedan atenuadas. Puede ocultar o mostrar los errores solamente para los servidores tipo bastidor y torre.

Para ver el estado de un LED de identificación del sistema mediante RACADM, utilice el comando **getled**. Para obtener más información, consulte *iDRAC8 RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8) disponible en dell.com/support/manuals.

Enlaces relacionados

[Configuración del valor LED del Id. del sistema](#)

Indicadores de problemas del hardware


Entre los problemas relacionados con el hardware se incluyen los siguientes:

- Falla de encendido
- Ventiladores ruidosos
- Pérdida de conectividad de red
- Falla del disco duro
- Falla de soportes USB
- Daños físicos

Según el programa, utilice los métodos siguientes para corregir el problema:

- Vuelva a insertar el módulo o el componente y reinicie el sistema.
- En el caso de un servidor Blade, inserte el módulo en una bahía diferente del chasis.
- Reemplace las unidades de disco duro o las unidades Flash USB.
- Vuelva a conectar o reemplace los cables de alimentación y de red.

Si el problema persiste, consulte el *Manual del propietario de hardware* para obtener información específica para la solución de problemas del dispositivo de hardware.

 **PRECAUCIÓN:** Solo debería realizar la solución de problemas y tareas de reparación sencillas según permita la documentación del producto o según el equipo de asistencia técnica y servicio en línea o telefónico. Los datos debidos a reparaciones no autorizadas por Dell no están cubiertos por la garantía. Lea y siga las instrucciones de seguridad suministradas con el producto.

Visualización de la condición del sistema


Las interfaces web de iDRAC y CMC (para servidores blade) muestran el estado de los elementos siguientes:




- Baterías
- Ventiladores
- Intrusión
- Fuentes de alimentación
- Medios flash extraíbles
- Temperaturas
- Voltajes
- CPU

En la interfaz web de iDRAC, vaya a la sección **Descripción general** → **Servidor** → **Resumen del sistema** → **Condición del servidor**.

Para ver la condición de la CPU, vaya a **Información general** → **Hardware** → **CPU**.

Los indicadores de condición del sistema son los siguientes:

-  — indica un estado normal.

-  — indica un estado de advertencia.
-  — indica un estado de error.
-  — indica un estado desconocido.

Haga clic en cualquier nombre de componente de la sección **Condición del sistema** para ver los detalles acerca del componente.

Generación de un informe de asistencia técnica

Si debe trabajar con la Asistencia técnica en un problema con un servidor pero las políticas de seguridad restringen la conexión a Internet, puede proporcionarle a la Asistencia técnica los datos necesarios para facilitar la solución de problemas sin tener que instalar software o descargar herramientas de Dell y sin tener acceso a la Internet desde el sistema operativo del servidor o iDRAC. Puede enviar el informe desde un sistema alternativo y garantizar que los usuarios no autorizados no puedan ver los datos recopilados de su servidor durante la transmisión a la Asistencia técnica.

Puede generar un informe de condición del servidor y luego exportarlo a una ubicación en la estación de administración (local) o a una ubicación de red compartida, como un sistema de archivos de Internet comunes (CIFS) o recurso compartido de archivos de red (NFS). A continuación, puede compartir este informe directamente con la Asistencia técnica. Para exportar a un recurso compartido de red CIFS o NFS, se necesita conectividad de red directa al puerto de red compartido o dedicado del iDRAC.

El informe se genera en el formato ZIP convencional. Este informe contiene información similar a la información disponible en el informe DSET, por ejemplo:

- Inventario de hardware para todos los componentes
- Sistema, Lifecycle Controller y los atributos del componente
- Sistema operativo e información de las aplicaciones
- Registros de Lifecycle Controller activos (las anotaciones archivadas no están incluidas)
- Registros de SSD PCIe
- Registros de la controladora de almacenamiento

Una vez que se genera el informe, es posible verlo. El informe contiene un conjunto de archivos XML y archivos de registro. El informe debe compartirse con el servicio de asistencia técnica para solucionar el problema.

Cada vez que se recopilan datos, se graba un suceso en el registro de Lifecycle Controller. El suceso incluye información como la interfaz utilizada, la fecha y la hora de la exportación y el nombre de usuario de iDRAC.

El informe de registros y aplicaciones del sistema operativo puede generarse de dos maneras:

- Automática: el uso del módulo de servicio del iDRAC que automáticamente invoca la herramienta OS Collector.
- Manual: se realiza una ejecución manual del ejecutable de OS Collector desde el sistema operativo del servidor. iDRAC expone el ejecutable de OS Collector en el sistema operativo del servidor como un dispositivo USB con la etiqueta DRACRW.

NOTA:

- La herramienta OS Collector no es aplicable para los sistemas Dell Precision PR7910.
- La función de recopilación de registros del sistema operativo no es compatible con el sistema operativo CentOS.

Antes de generar el informe de condición, compruebe lo siguiente:

- Lifecycle Controller está activado.
- La función Collect System Inventory on Restart (CSIOR) (Recopilar inventario de sistema al Reiniciar) está activada.
- Cuenta con privilegios de Inicio de sesión y Control del servidor.

Enlaces relacionados

[Generación de un informe de asistencia técnica de forma automática](#)

[Generación de informe de asistencia técnica de forma manual](#)

Generación de un informe de asistencia técnica de forma automática

Si el módulo de servicio de iDRAC está instalado y en ejecución, es posible generar automáticamente el informe de asistencia técnica. El módulo de servicio de iDRAC invoca el archivo de OS Collector correspondiente en el sistema operativo host, recopila los datos y los transfiere a iDRAC. A continuación, se puede guardar el informe en la ubicación requerida.

Generación de un informe de asistencia técnica de forma automática mediante la interfaz web de iDRAC


Para generar el informe de asistencia técnica de forma automática:

1. En la interfaz web del iDRAC, vaya a **Descripción general** → **Servidor** → **Solución de problemas** → **Informe de asistencia técnica**.

Se muestra la página **Informe de asistencia técnica**.

2. Seleccione las opciones para las cuales desea recopilar los datos:

- **Hardware**
- **Datos del sistema operativo y de la aplicación**

 **NOTA:** Mientras se especifica la configuración para el recurso compartido de red, se recomienda evitar el uso de caracteres especiales en el nombre de usuario y la contraseña o codificar por porcentaje los caracteres especiales.

- Haga clic en **Opciones avanzadas de exportación** para seleccionar las siguientes opciones adicionales:
 - **Registro de la controladora RAID**
 - **Activar filtrado de informes en Datos de aplicación y SO**

Según las opciones seleccionadas, el tiempo que lleva recopilar los datos se muestra junto a estas opciones.

3. Seleccione la opción **Acepto permitir que la asistencia técnica use estos datos** y, a continuación, haga clic en **Exportar**.
4. Una vez que el módulo de servicio de iDRAC haya terminado de transferir los datos de la aplicación y el sistema operativo a iDRAC, se empaquetarán esos datos junto con los datos de hardware y se generará el informe final. Se mostrará un mensaje para guardar el informe.
5. Especifique la ubicación donde desea guardar el informe de asistencia técnica.

Generación de informe de asistencia técnica de forma manual

Cuando no se ha instalado iSM, se puede ejecutar manualmente la herramienta OS Collector para generar el informe de asistencia técnica. Es necesario ejecutar la herramienta OS Collector en el sistema operativo del servidor para exportar los datos de la aplicación y el sistema operativo. Un dispositivo USB virtual con la etiqueta DRACRW aparece en el sistema operativo de servidor. Este dispositivo contiene el archivo de OS Collector específico para el sistema operativo host. Ejecute el archivo específico para el sistema operativo desde el sistema operativo del servidor para recopilar y transferir los datos a iDRAC. A continuación, puede exportar el informe a una ubicación compartida de red o local.

En los sistemas Dell PowerEdge de 13.^a generación, el DUP de OS Collector se instala en la fábrica. Sin embargo, si se determina que OS Collector no está presente en el iDRAC, se puede descargar el archivo DUP desde el sitio de asistencia de Dell y, a continuación, cargar el archivo en iDRAC mediante el proceso de actualización de firmware.

Antes de generar el informe de asistencia técnica manualmente mediante la herramienta OS Collector, realice el procedimiento siguiente en el sistema operativo host:

- En el sistema operativo Linux: verifique si el servicio IPMI está en ejecución. Si no está en ejecución, debe iniciarlo manualmente. En la siguiente tabla se proporcionan los comandos que se pueden utilizar para comprobar el estado del servicio IPMI e iniciar el servicio (si es necesario) para cada sistema operativo Linux.

| Sistema operativo LINUX | Comando IPMI para comprobar el estado del servicio | Comando para iniciar el servicio IPMI |
|---------------------------------------|--|--|
| Red Hat Enterprise Linux 5 de 64 bits | <code>\$ service ipmi status</code> | <code>\$ service ipmi start</code> |
| Red Hat Enterprise Linux 6 | | |
| SUSE Linux Enterprise Server 11 | | |
| CentOS 6 | | |
| Oracle VM | | |
| Oracle Linux 6.4 | | |
| Red Hat Enterprise Linux 7 | <code>\$ systemctl status ipmi.service</code> | <code>\$ systemctl start ipmi.service</code> |


NOTA:

- CentOS se admite solamente en el módulo de servicio de iDRAC versión 2.0 o posterior.
 - Si los módulos IPMI no están presentes, es posible instalar los módulos respectivos desde los medios de distribución del sistema operativo. El servicio se inicia una vez completada la instalación.
- En el sistema operativo Windows:
 - Compruebe si el servicio WMI está en ejecución:
 - * Si WMI se detiene, OS Collector inicia el WMI automáticamente y continúa con la recopilación.

- * Si WMI se desactiva, la recopilación de OS Collector se detiene y se muestra un mensaje de error.
- Verifique los niveles de privilegio adecuados y asegúrese de que no haya ninguna configuración de servidor de seguridad o de seguridad que impida obtener los datos desde el software o el registro.

Generación de informe de asistencia técnica mediante la interfaz web del iDRAC manualmente

Para generar el informe de asistencia técnica manualmente:

1. En la interfaz web del iDRAC, vaya a **Descripción general** → **Servidor** → **Solución de problemas** → **Informe de asistencia técnica**.
Se muestra la página **Informe de asistencia técnica**.
2. Seleccione las opciones para las que desea recopilar los datos:
 - **Local** para exportar el informe a una ubicación del sistema local.
 - **Datos del sistema** para exportar el informe a un recurso compartido de red y especificar los valores de red.
 -  **NOTA:** Mientras que especifica la configuración del recurso compartido de red, se recomienda evitar el uso de caracteres especiales en el nombre de usuario y la contraseña o codificar por porcentaje los caracteres especiales.
 - Haga clic en **Opciones avanzadas para exportar** para seleccionar las siguientes opciones adicionales:
 - **Registro de la controladora RAID**
 - **Activación del filtrado de informes** en **Datos del sistema operativo y de la aplicación**

Según las opciones seleccionadas, el tiempo que lleva recopilar los datos se muestra junto a estas opciones.

Si la herramienta OS Collector no se ejecutó en el sistema, la opción Datos de la aplicación y el sistema operativo aparece atenuada y no se puede seleccionar. Aparece el mensaje OS and Application Data (Last Collected: Never).

Si el OS Collector se ejecutó en el sistema en el pasado, aparecen la fecha y la hora de la última vez que se recopilaron los datos del sistema operativo y de la aplicación: Last Collected: <timestamp>

3. Haga clic en **Adjuntar recopilador de sistema operativo**.
Esto le conducirá a acceder al SO host. Aparecerá un mensaje para pedirle que inicie la consola virtual.
4. Una vez que haya iniciado la consola virtual, haga clic en el mensaje emergente para ejecutar y usar la herramienta OS Collector para recopilar los datos.
5. Vaya a la DRACRW dispositivo USB virtual que iDRAC presenta al sistema.
6. Invoque el recopilador de sistema operativo de archivo adecuado para el sistema operativo host:
 - Para Windows, ejecute **Windows_OSCollector_Startup.bat**.
 - Para Linux, ejecute **Linux_OSCollector_Startup.exe**.
7. Después de que el recopilador del SO haya completado la transferencia de datos a iDRAC, iDRAC eliminará automáticamente el dispositivo USB.
8. Vuelva a la página **Informe de soporte técnico**, haga clic en el icono **Actualizar** para reflejar la nueva fecha y hora.
9. Para exportar los datos, en **Export Location (Ubicación)**, seleccione **Local** o **Network (red)**.
10. Si seleccionó **Red**, introduzca los detalles de la ubicación de la red.

11. Seleccione la opción **Acepto permitir a la asistencia técnica que use estos datos** y, a continuación, haga clic en **Exportar** para exportar los datos a la ubicación especificada.

Generación de un informe de asistencia técnica mediante RACADM de forma manual

Para generar elementos TSR con RACADM, utilice el subcomando **techsupreport**. Para obtener más información, consulte *iDRAC RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de iDRAC) disponible en dell.com/esmanuals.com.

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

Cuando el LED parpadea con una luz ámbar y un servidor concreto tiene un error, la pantalla de estado de servidor del LCD resalta en naranja el servidor afectado. Utilice los botones de navegación LCD para resaltar el servidor afectado y haga clic en el botón central. Los mensajes de error y advertencia se mostrarán en la segunda línea. Para obtener una lista de los mensajes de error que se muestran en el panel LCD, consulte el manual del propietario

Reinicio de iDRAC

Puede realizar un reinicio por hardware o por software de iDRAC sin apagar el servidor:

- Reinicio por hardware: en el servidor, mantenga presionado el botón LED durante 15 segundos.
- Reinicio por software: utilice la interfaz web de iDRAC o RACADM.

Reinicio de iDRAC mediante la interfaz web de iDRAC

Para reiniciar iDRAC, realice una de las siguientes acciones en la interfaz web de iDRAC:

- Vaya a **Información general** → **Servidor** → **Resumen**. En **Tareas de inicio rápido**, haga clic en **Restablecer iDRAC**.
- Vaya a **Información general** → **Servidor** → **Solución de problemas** → **Diagnósticos**. Haga clic en **Restablecer iDRAC**.

Reinicio de iDRAC mediante RACADM

Para reiniciar iDRAC, utilice el comando **racreset**. Para obtener más información, consulte *RACADM Reference Guide for iDRAC and CMC* (Guía de referencia de RACADM para iDRAC y CMC), disponible en dell.com/support/manuals.

Borrado de datos del sistema y del usuario


Es posible borrar componentes del sistema y datos del usuario para dichos componentes. Los componentes del sistema incluyen:

- Datos de Lifecycle Controller
- Diagnósticos incorporados
- Driver Pack para el sistema operativo incorporado
- Restablecimiento de los valores predeterminados del BIOS
- Restablecimiento de los valores predeterminados de iDRAC

Antes de llevar a cabo el borrado del sistema, asegúrese de que:

- Cuenta con el privilegio de control del servidor de iDRAC.
- Lifecycle Controller está activado.

La opción Datos de Lifecycle Controller borra cualquier contenido, como el registro de LC, la base de datos de configuración, el firmware de reversión, los registros enviados de fábrica y la información de configuración de FP SPI (o soporte vertical de administración).

 **NOTA:** El registro de Lifecycle Controller contiene la información sobre la solicitud de borrado del sistema y cualquier información generada cuando el iDRAC se reinicia. No existe información previa.

Es posible eliminar componentes del sistema individuales o múltiples mediante el comando **SystemErase**:

```
racadm systemErase <BIOS | DIAG | DRVPACK | LCDATA | IDRAC >
```

donde:

- BIOS: restablecimiento de los valores predeterminados del BIOS
- DIAG: diagnósticos incorporados
- DRVPACK: driver pack para el sistema operativo incorporado
- LCDATA: se borran los datos de Lifecycle Controller
- IDRAC: restablecimiento de los valores predeterminados de iDRAC

Para obtener más información, consulte *iDRAC RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de iDRAC) disponible en dell.com/esmmanuals.

Restablecimiento de iDRAC a los valores predeterminados de fábrica

Es posible restablecer iDRAC a la configuración predeterminada de fábrica mediante la utilidad de configuración de iDRAC o la interfaz web de iDRAC.

Restablecimiento de iDRAC a los valores predeterminados de fábrica mediante la interfaz web de iDRAC

Para restablecer iDRAC a los valores predeterminados de fábrica mediante la interfaz web de iDRAC:

1. Vaya a **Descripción general** → **Servidor** → **Solución de problemas** → **Diagnósticos**.

Se muestra la página **Consola de diagnósticos**.

2. Haga clic en **Restablecer iDRAC a los valores predeterminados**.

El estado de finalización se muestra en forma de porcentaje. iDRAC se reinicia y se restablece a los valores predeterminados de fábrica. La IP de iDRAC se restablece pero no es posible acceder a esa dirección. Puede configurar la IP mediante el panel anterior o el BIOS.

Restablecimiento de iDRAC a los valores predeterminados de fábrica mediante la utilidad de configuración de iDRAC

Para restablecer iDRAC a los valores predeterminados de fábrica mediante la utilidad de configuración de iDRAC:

1. Vaya a **Restablecer la configuración de iDRAC a los valores predeterminados**.
Aparece la página **Restablecimiento de los valores predeterminado de iDRAC de la configuración de iDRAC**.
2. Haga clic en **Sí**.
Se inicia el restablecimiento de iDRAC.
3. Haga clic en **Atrás** y vaya a la misma página **Restablecer valores predeterminados de iDRAC** para ver el mensaje de que la operación se ha realizado correctamente.

Preguntas frecuentes

En esta sección se enumeran las preguntas frecuentes para los elementos siguientes:

- [Registro de sucesos del sistema](#)
- [Seguridad de la red](#)
- [Active Directory](#)
- [Inicio de sesión único](#)
- [Inicio de sesión mediante tarjeta inteligente](#)
- [Consola virtual](#)
- [Medios virtuales](#)
- [Tarjeta vFlash SD](#)
- [Autenticación SNMP](#)
- [Dispositivos de almacenamiento](#)
- [iDRAC Service Module](#)
- [RACADM](#)
- [Varios](#)

Registro de sucesos del sistema

Al utilizar la interfaz web de iDRAC a través de Internet Explorer, ¿por qué el registro SEL no se puede guardar mediante la opción Guardar como?

Esto se debe a un parámetro del explorador. Para solucionar este problema, realice lo siguiente:

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 se encuentra 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 estén activadas:
 - Preguntar automáticamente si se debe descargar un archivo: (si está disponible)
 - Descarga de archivos

 **PRECAUCIÓN:** Para garantizar la seguridad del equipo que se utiliza para acceder a iDRAC, bajo **Varios**, desactive la opción **Inicio de aplicaciones y archivos no seguros**.

Seguridad de la red

Al acceder a la interfaz web de iDRAC, se muestra una advertencia de seguridad donde se indica que el certificado emitido por la autoridad de certificados (CA) no es de confianza.

iDRAC incluye un certificado de servidor de iDRAC predeterminado para garantizar la seguridad de la red cuando se accede a ella a través de la interfaz web y RACADM remoto. Este certificado no lo emite una CA de confianza. Para resolver esta advertencia, cargue un certificado de servidor iDRAC emitido por una CA de confianza (por ejemplo, Microsoft Certificate Authority, Thawte o Verisign).

¿Por qué el servidor DNS no registra iDRAC?

Algunos servidores DNS registran nombres de iDRAC que contienen solo hasta 31 caracteres.

Al acceder a la interfaz web de iDRAC, se muestra una advertencia de seguridad que indica que el nombre de host del certificado SSL no coincide con el nombre de host de iDRAC.

iDRAC incluye un certificado de servidor de iDRAC para garantizar la seguridad de la red cuando se accede a ella a través de la interfaz web y RACADM remoto. Cuando se utiliza este certificado, el explorador de web muestra una advertencia de seguridad por el certificado predeterminado que se emite a iDRAC no coincide con el nombre de host de iDRAC (por ejemplo, la dirección IP).

Para solucionar esto, cargue un certificado de servidor de iDRAC a la dirección IP o el nombre de host de iDRAC. Al generar la CSR (que se utiliza para emitir el certificado), asegúrese de que el nombre común (CN) de la CSR coincide con la dirección IP de iDRAC (si el certificado se ha emitido a la IP) o con el nombre DNS registrado de iDRAC (si el certificado se ha emitido al nombre registrado de iDRAC).

Para asegurarse de que la CSR coincida con el nombre DNS de iDRAC:

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Configuración de iDRAC** → **Red**. Se mostrará la página **Red**.
2. En la sección **Valores comunes**:
 - Seleccione la opción **Registrar iDRAC en DNS**.
 - En el campo **Nombre DNS de iDRAC**, introduzca el nombre de iDRAC.
3. Haga clic en **Apply (Aplicar)**.

Active Directory

Error de inicio de sesión de Active Directory. ¿Cómo se resuelve este problema?

Para diagnosticar el problema, en la página **Configuración y administración de Active Directory**, haga clic en **Probar configuración**. Revise los resultados de la prueba y corrija el problema. Cambie la configuración y ejecute la prueba hasta que el usuario supere el paso de autorización.

En general, compruebe lo siguiente:

- Al iniciar sesión, asegúrese de usar el nombre de dominio de usuario correcto y no el nombre de NetBIOS. Si tiene una cuenta de usuario de iDRAC local, inicie sesión en iDRAC mediante las credenciales locales. Tras iniciar sesión, compruebe lo siguiente:

- La opción **Active Directory activado** está seleccionada en la página **Configuración y administración de Active Directory**.
- La configuración de DNS se ha configurado correctamente en la página **Configuración de redes iDRAC**.
- Se ha cargado el certificado de CA raíz de Active Directory correcto en iDRAC si se ha activado la validación de certificados.
- El nombre de iDRAC y el nombre de dominio de iDRAC coinciden con la configuración del entorno de Active Directory si utiliza el esquema extendido.
- El nombre de grupo y el nombre de dominio de grupo coinciden con la configuración del entorno de Active Directory si utiliza el esquema estándar.
- Si el usuario y el objeto iDRAC se encuentran en un dominio diferente, no seleccione la opción **Dominio de usuario desde inicio de sesión**. En su lugar, seleccione la opción **Especificar un dominio** e introduzca el nombre del dominio en el que reside el objeto de iDRAC.
- Verifique los certificados SSL de la controladora de dominio para asegurarse de que la hora de iDRAC se encuentre en el plazo de vigencia del certificado.

El inicio de sesión de Active Directory falla incluso si la validación de certificados está activada. Los resultados de la prueba muestran el siguiente mensaje de error. ¿Por qué sucede esto y cómo se resuelve?

```
ERROR: Can't contact LDAP server, error:14090086:SSL
routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed: Please check
the correct Certificate Authority (CA) certificate has been uploaded to iDRAC.
Please also check if the iDRAC date is within the valid period of the
certificates and if the Domain Controller Address configured in iDRAC matches
the subject of the Directory Server Certificate.
```

Si se ha activado la validación de certificados, cuando iDRAC establece la conexión SSL con el servidor de directorios, iDRAC utiliza el certificado de CA cargado para verificar el certificado de servidor de directorios. Los motivos más comunes del fallo de esta validación son los siguientes:

- La fecha de iDRAC no se encuentra en el período de validación del certificado de servidor o de CA. Compruebe la hora de iDRAC y el período de validación del certificado.
- Las direcciones de controladora de dominio configuradas en iDRAC no coinciden con el asunto o el nombre alternativo del asunto del certificado de servidor de directorios. Si utiliza una dirección IP, lea la pregunta siguiente. Si utiliza FQDN, asegúrese de utilizar el FQDN de la controladora de dominio y no el dominio. Por ejemplo, **nombreservidor.ejemplo.com** en lugar de **ejemplo.com**.

La validación de certificados falla incluso si la dirección IP se utiliza como dirección de la controladora de dominio. ¿Cómo se resuelve esto?

Compruebe el campo Asunto o Nombre alternativo del asunto del certificado de controladora de dominio. Normalmente, Active Directory utiliza el nombre de host y no la dirección IP de la controladora de dominio en el campo Asunto o Nombre alternativo del asunto del certificado de controladora de dominio. Para resolver esto, realice cualquiera de las acciones siguientes:

- Configure el nombre del host (FQDN) de la controladora de dominio como las *direcciones de controladora de dominio* en iDRAC para que coincidan con el Asunto o el Nombre alternativo del asunto del certificado del servidor.
- Vuelva a emitir el certificado del servidor de modo que use una dirección IP en el campo Asunto o Nombre alternativo del asunto y que coincida con la dirección IP configurada en iDRAC.
- Desactive la validación de certificados si prefiere confiar en esta controladora de dominio sin validación de certificados durante el protocolo de enlace SSL.

¿Cómo se configuran las direcciones de controladora de dominio cuando se utiliza el esquema extendido en un entorno de varios dominios?

Debe usar el nombre del host (FQDN) o la dirección IP de las controladoras de dominio que sirven al dominio donde reside el objeto iDRAC.

¿Cuándo deben configurarse las direcciones del catálogo global?

Si utiliza el esquema estándar y los usuarios y grupos de roles son de dominios diferentes, se requieren direcciones de catálogo global. En este caso, solo puede utilizar el grupo universal.

Si está utilizando un esquema estándar y todos los usuarios y grupos de roles se encuentran en el mismo dominio, no son necesarias las direcciones de catálogo global.

Si utiliza un esquema extendido, no se utiliza la dirección de catálogo global.

¿Cómo funciona la consulta del esquema estándar?

iDRAC primero se conecta a las direcciones de la controladora de dominio configuradas; si el usuario y los grupos de roles están en el dominio, se guardarán los privilegios.

Si existen direcciones de controladora global configuradas, iDRAC sigue consultando el catálogo global. Si se recuperan privilegios adicionales desde el catálogo global, estos privilegios se acumulan.

¿iDRAC siempre usa LDAP a través de SSL?

Sí. Todo el transporte se realiza a través del puerto seguro 636 o 3269. Durante la prueba de la configuración, iDRAC realiza una conexión LDAP para aislar el problema, pero no realiza un enlace LDAP en una conexión no segura.

¿Por qué iDRAC activa la validación de certificados de manera predeterminada?

iDRAC aplica una seguridad fuerte para garantizar la identidad de la controladora de dominio a la que se conecta. Sin la validación de certificados, un pirata informático puede suplantar una controladora de dominio y tomar el control de la conexión SSL. Si opta por confiar en todas las controladoras de dominio en el límite de seguridad sin activar la validación de certificados, puede desactivarla a través de la interfaz web o RACADM.

¿Admite iDRAC el nombre NetBIOS?

No en esta versión.

¿Por qué se demora hasta cuatro minutos para iniciar sesión en iDRAC mediante el inicio de sesión único de Active Directory o mediante tarjeta inteligente?

El inicio de sesión único de Active Directory o mediante tarjeta inteligente suele tardar menos de 10 segundos. Sin embargo, puede tardar hasta cuatro minutos si ha especificado el servidor DNS preferido y el servidor DNS alternativo y el primero ha fallado. Se espera que se produzcan tiempos de espera DNS cuando un servidor DNS está fuera de servicio. iDRAC le inicia la sesión mediante el servidor DNS alternativo.

Active Directory está configurado para un dominio presente en Windows Server 2008 Active Directory. Hay un dominio secundario o un subdominio presente para el dominio, el usuario y grupo está presente en el mismo dominio secundario y el usuario es miembro de este grupo. Al intentar iniciar sesión en iDRAC mediante el usuario presente en el dominio secundario, falla el inicio de sesión único de Active Directory.

Esto puede deberse a un tipo de grupo incorrecto. Hay dos tipos de grupo 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 solo como listas de distribución por correo electrónico.

Asegúrese siempre que el tipo de grupo sea Seguridad. No puede utilizar grupos de distribución para asignar permisos a objetos. Sin embargo, puede usarlos para filtrar la configuración de la política de grupo.

Inicio de sesión único

El inicio de sesión SSO falla en Windows Server 2008 R2 x64. ¿Cuál es la configuración necesaria para resolver este problema?

1. Realice el procedimiento que se indica en [http://technet.microsoft.com/es-es/library/dd560670\(WS.10\).aspx](http://technet.microsoft.com/es-es/library/dd560670(WS.10).aspx) para la controladora de dominio y la política de dominio.
2. Configure los equipos para que utilice el conjunto de cifrado DES-CBC-MD5. Estos valores pueden afectar a la compatibilidad con los equipos cliente o los servicios y las aplicaciones del entorno. Los tipos de cifrado de configuración para la política Kerberos se encuentran en **Configuración del equipo** → **Configuración de seguridad** → **Políticas locales** → **Opciones de seguridad**.
3. Asegúrese de que los clientes del dominio tienen el GPO actualizado.
4. En la línea de comandos, escriba `gpupdate /force` y elimine el archivo keytab antiguo mediante el comando `klist purge`.
5. Una vez actualizado el GPO, cree el nuevo archivo keytab.
6. Cargue el archivo keytab en iDRAC.

Ahora puede iniciar sesión en el iDRAC mediante el inicio de sesión único.

¿Por qué falla el inicio de sesión único para los usuarios de Active Directory en Windows 7 y Windows Server 2008 R2?

Debe activar los tipos de cifrado para Windows 7 y Windows Server 2008 R2. Para ello:

1. Inicie sesión como administrador o como usuario con privilegios administrativos.
2. Vaya a **Inicio** y ejecute `gpedit.msc`. Aparecerá la ventana **Editor de directivas de grupo local**.
3. Vaya a **Configuración del equipo local** → **Configuración de Windows** → **Configuración de seguridad** → **Directivas 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.

6. Haga clic en **Aceptar**. Ahora puede iniciar sesión en iDRAC mediante SSO.

Indique los siguientes valores adicionales para el esquema extendido:

1. En la ventana **Editor de directivas de grupo local**, vaya a **Configuración del equipo local** → **Configuración de Windows** → **Configuración de seguridad** → **Directivas locales** → **Opciones de seguridad**.
2. Haga clic con el botón derecho del mouse en **Seguridad de la red: Restricción de NTLM: Tráfico de NTLM de salida al servidor remoto** y seleccione **Propiedades**.
3. Seleccione **Permitir todo**, haga clic en **Aceptar** y, a continuación, cierre la ventana **Editor de directivas de grupo local**.
4. Vaya a **Inicio** y ejecute el comando cmd. Aparecerá la ventana del símbolo del sistema.
5. Ejecute el comando `gpupdate /force`. Se actualizan las políticas de grupo. Cierre la ventana de símbolo del sistema.
6. Vaya a **Inicio** y ejecute el comando regedit. Aparecerá la ventana **Editor del registro**.
7. Vaya a **HKEY_LOCAL_MACHINE** → **System** → **CurrentControlSet** → **Control** → **LSA**.
8. En el panel derecho, haga clic con el botón derecho del mouse y seleccione **Nuevo** → **DWORD (32-bit) Value**.
9. Asigne a la nueva clave el nombre **SuppressExtendedProtection**.
10. Haga clic con el botón derecho del mouse en **SuppressExtendedProtection** y haga clic en **Modificar**.
11. En el campo de datos **Valor**, escriba **1** y haga clic en **Aceptar**.
12. Cierre **Editor del Registro**. Ahora puede iniciar sesión en iDRAC mediante SSO.

Si ha activado el inicio de sesión único para iDRAC y está utilizando Internet Explorer para iniciar sesión en iDRAC, el inicio de sesión único falla y solicita que se introduzca el nombre de usuario y contraseña. ¿Cómo se resuelve esto?

Asegúrese de que la dirección IP de iDRAC figura en **Herramientas** → **Opciones de Internet** → **Seguridad** → **Sitios de confianza**. Si no figura en la lista, SSO falla y se le solicitará que introduzca el nombre de usuario y la contraseña. Haga clic en **Cancelar** y continúe.

Inicio de sesión mediante tarjeta inteligente

Puede tardar hasta cuatro minutos iniciar sesión en iDRAC mediante el inicio de sesión único de Active Directory o mediante tarjeta inteligente.

El inicio de sesión único de Active Directory o mediante tarjeta inteligente suele tardar menos de 10 segundos. Sin embargo, puede tardar hasta cuatro minutos si ha especificado el servidor DNS preferido y el servidor DNS alternativo en la página **Red** y el primero ha fallado. Se espera que se produzcan tiempos de espera DNS cuando un servidor DNS está fuera de servicio. iDRAC le inicia la sesión mediante el servidor DNS alternativo.

El complemento ActiveX no puede detectar el lector de tarjetas inteligentes.

Asegúrese de que la tarjeta inteligente es compatible con el sistema operativo de Microsoft Windows. Windows admite un número limitado de proveedores de servicios criptográficos (CPS) de tarjeta inteligente.

En general 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 compruebe si Windows detecta esa tarjeta y muestra el cuadro de diálogo para introducir el PIN.

PIN incorrecto de la tarjeta inteligente.

Verifique si la tarjeta está bloqueada debido a demasiados intentos con un PIN incorrecto. En estos casos, póngase en contacto con el emisor de la tarjeta inteligente de la organización para obtener una tarjeta nueva.

Consola virtual

La sesión de consola virtual se activa aunque se haya cerrado la sesión de la interfaz web de iDRAC.

¿Este comportamiento es esperado?

Sí. Cierre la ventana Visor de consola virtual para cerrar 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. Después de que iDRAC recibe la solicitud de encendido de vídeo local, el vídeo se enciende instantáneamente.

¿El usuario local puede desactivar el vídeo?

Cuando la consola local está desactivada, el usuario local no puede apagar el vídeo.

¿La desactivación del vídeo local también desactiva el teclado y el mouse locales?

No

¿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 de iDRAC active o desactive el vídeo del servidor local?

Cualquier usuario con privilegios de configuración de iDRAC puede activar o desactivar la consola local.

¿Cómo se puede ver el estado actual del vídeo del servidor local?

El estado se muestra en la página de la consola virtual.

Utilice el comando RACADM `racadm getconfig -g cfgRacTuning` para ver el estado en el objeto `cfgRacTuneLocalServerVideo`.

O bien, utilice el siguiente comando RACADM desde una sesión Telnet, SSH o remota:

```
racadm -r (iDrac IP) -u (username) -p (password) getconfig -g cfgRacTuning
```

El estado también se puede ver en la pantalla OSCAR de la consola virtual. Cuando se activa la consola local, se muestra un estado verde junto al nombre del servidor. Cuando se desactiva, un punto amarillo indica que iDRAC ha bloqueado la consola local.

¿Por qué la parte inferior de la pantalla del sistema no se puede ver desde la ventana de la consola virtual?

Compruebe que la resolución del monitor de la estación de administración sea de 1280 x 1024.

¿Por qué la ventana Visor de la consola virtual está corrupta en el sistema operativo Linux?

El visor de la consola en Linux requiere un conjunto de caracteres UTF-8. Compruebe la configuración regional y restablezca el conjunto de caracteres si fuera necesario.

¿Por qué el mouse no se sincroniza bajo la consola de texto de Linux en Lifecycle Controller?

La consola virtual requiere el controlador de mouse USB, pero este solo está disponible para el sistema operativo X-Window. En el visor de la consola virtual, realice cualquiera de las acciones siguientes:

- Vaya a la ficha **Herramientas** → **Opciones de la sesión** → **Mouse**. En **Aceleración del mouse**, seleccione **Linux**.
- En el menú **Herramientas**, seleccione la opción **Cursor único**.

¿Cómo se sincronizan los punteros del mouse en la ventana Visor de la consola virtual?

Antes de iniciar una sesión de consola virtual, asegúrese de seleccionar el mouse correcto para el sistema operativo.

Asegúrese de seleccionar la opción **Cursor sencillo** bajo **Herramientas** en el menú de la consola virtual de iDRAC del cliente de la consola virtual de iDRAC. El valor predeterminado es el modo de dos cursores.

¿Se puede usar un teclado o mouse al instalar el sistema operativo Microsoft de forma remota a través de la consola virtual?

No. Cuando instala un sistema operativo de Microsoft en un sistema con la consola virtual activada en el BIOS, se envía un mensaje de conexión EMS que requiere la selección de **Aceptar** de manera remota. Debe seleccionar **Aceptar** en el sistema local o reiniciar el servidor administrado de manera remota, reinstalar y luego apagar la consola virtual en el BIOS.

Este mensaje lo genera Microsoft para alertar al usuario que la consola virtual está activada. Para asegurarse de que este mensaje no aparezca, siempre apague la consola virtual en la utilidad de configuración iDRAC antes de instalar un sistema operativo de manera remota.

¿Por qué el indicador Bloq Num en la estación de administración no refleja el estado de Bloq Num en el servidor remoto?

Al acceder a través de iDRAC, el indicador Bloq Num de la estación de trabajo no coincide necesariamente con el estado de Bloq Num del servidor remoto. El estado de este depende de la

configuración del servidor remoto cuando se establezca la sesión remota, independientemente del estado de Bloq Num de la estación de trabajo.

¿Por qué aparecen varias ventanas de Session Viewer cuándo se establece una sesión de consola virtual desde el host local?

Se está configurando la sesión de consola virtual desde el sistema local. Esta acción no se admite.

Si hay una sesión de consola virtual en curso y un usuario local accede al servidor administrado ¿el primer usuario recibe un mensaje de advertencia?

Si un usuario local accede al sistema, ambos tendrán el control del mismo.

¿Cuánto ancho de banda se necesita para ejecutar una sesión de consola virtual?

Se recomienda disponer de una conexión de 5 MBPS para un rendimiento adecuado. Se requiere una conexión de 1 MBPS para un rendimiento mínimo.

¿Cuáles son los requisitos mínimos del sistema para que la 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.

¿Por qué la ventana del visor de consola virtual a veces muestra el mensaje Sin señal?

Este mensaje puede aparecer porque el complemento Consola virtual de iDRAC no recibe el vídeo de escritorio del servidor remoto. Por lo general, este comportamiento se produce cuando el servidor remoto está apagado. De vez en cuando, el mensaje puede aparecer debido a un funcionamiento erróneo de la recepción de vídeo en el escritorio del servidor remoto.

¿Por qué la ventana del visor de consola virtual a veces muestra un mensaje Fuera de alcance?

Este mensaje puede aparecer debido a que un parámetro necesario para capturar el vídeo está fuera del alcance de captura de vídeo de iDRAC. Si parámetros, tal como la resolución de visualización o la tasa de actualización, se establecen en valores muy altos, se podría provocar una condición de fuera de alcance. Normalmente, las limitaciones físicas, tal como el tamaño de la memoria de vídeo o el ancho de banda, establecen el alcance máximo de los parámetros.

Cuando se inicia una sesión de consola virtual en la interfaz web de iDRAC, ¿por qué aparece una ventana emergente sobre la seguridad de ActiveX?

Es posible que iDRAC no se encuentre en una lista de sitios de confianza. Para evitar que aparezca la ventana emergente sobre la seguridad cada vez que inicie una sesión de consola virtual, agregue iDRAC a la lista de sitios de confianza en el explorador del cliente. Para ello, realice lo siguiente:

1. Seleccione **Herramientas** → **Opciones de Internet** → **Seguridad** → **Sitios de confianza**.
2. Haga clic en **Sitios** e introduzca la dirección IP o el nombre DNS de iDRAC.
3. Haga clic en **Agregar**.
4. Haga clic en **Nivel personalizado**.
5. En la ventana **Configuración de seguridad**, seleccione **Petición** en **Descargar controles ActiveX no firmados**.

¿Por qué la ventana del visor de consola virtual está en blanco?

Si dispone de privilegios de medios virtuales pero no para la consola virtual, puede iniciar el visor para acceder a la función de medios virtuales pero la consola del servidor administrado no se mostrará.

¿Por qué el mouse no se sincroniza en DOS cuando se ejecuta la consola virtual?

El Dell BIOS emula el controlador del mouse como un mouse PS/2. Por diseño, el mouse PS/2 utiliza la posición relativa del puntero del mouse, lo que produce un retraso en la sincronización. iDRAC tiene un controlador de mouse USB, lo que permite la posición absoluta y un seguimiento más cercano del puntero del mouse. Incluso si iDRAC para la posición absoluta USB del mouse al Dell BIOS, la emulación del BIOS lo vuelve a convertir a la posición relativa y el comportamiento sigue siendo igual. Para solucionar este problema, establezca el modo del mouse en USC/Cuadros de diálogo en la pantalla Configuración.

Después de iniciar la consola virtual, el cursor del mouse está activo en la consola virtual pero no en el sistema local. ¿Por qué sucede esto y cómo se resuelve?

Esto sucede si **Modo de mouse** se establece en **USC/Cuadros de diálogo**. Pulse las teclas **Alt + M** para utilizar el mouse en el sistema local y vuelva a presionar **Alt + M** para utilizar el mouse en la consola virtual.

Cuando la interfaz web de iDRAC se inicia desde la interfaz web de CMC poco después de haberse iniciado la consola virtual, ¿por qué se agota el tiempo de espera de la sesión de la GUI?

Al iniciar la consola virtual en iDRAC desde la interfaz web de CMC se abre una ventana emergente para iniciar la consola virtual. Esta ventana se cierra poco después de abrirse la consola virtual.


Al iniciar la GUI y la consola virtual en el mismo sistema iDRAC en una estación de administración, se agota el tiempo de espera de la GUI de iDRAC si la GUI se inicia antes de que se cierre la ventana emergente. Si la GUI de iDRAC se inicia desde la interfaz web de CMC después de que se cierre la ventana emergente de la consola virtual, es problema no se produce.

¿Por qué la clave Linux SysRq no funciona con Internet Explorer?

El comportamiento de la clave Linux SysRq es diferente cuando se utiliza la consola virtual desde Internet Explorer. Para enviar la clave SysRq, pulse la tecla **Impr Pant** y suéltela mientras mantiene presionada las teclas **Ctrl** y **Alt**. Para enviar la clave SysRq a un servidor Linux remoto a través de iDRAC, al utilizar Internet Explorer:

1. Active la función de tecla mágica en el servidor Linux remoto. Puede utilizar el comando siguiente para activarla en la terminal de Linux:

```
echo 1 > /proc/sys/kernel/sysrq
```
2. Active el modo Paso a través de teclado del visor de Active X.
3. Presione **Ctrl + Alt + Impr Pant**.
4. Suelte solamente la tecla **Impr Pant**.
5. Presione **Impr Pant+Ctrl+Alt**.

 **NOTA:** La función SysRq no es actualmente compatible con Internet Explorer y Java.

¿Por qué parece el mensaje "Vínculo interrumpido" en la parte inferior de la consola virtual?

Cuando se utiliza un puerto de red compartido durante el reinicio de un servidor, iDRAC se desconecta mientras el BIOS restablece la tarjeta de red. El tiempo es más largo para las tarjetas de 10 Gb y puede ser excepcionalmente largo si el conmutador de red conectado tiene activado el protocolo de árbol de expansión (STP). En este caso, es recomendable activar "portfast" para el puerto de conmutador conectado al servidor. En la mayoría de los casos, la consola virtual se restablece sola.

Medios virtuales

¿Por qué a veces se interrumpe la conexión del cliente de medios virtuales?

Cuando se agota el tiempo de espera de la red, el firmware de iDRAC abandona la conexión y desconecta el vínculo entre el servidor y la unidad virtual.

Si cambia el CD en el sistema cliente, es posible que el CD tenga una función de inicio automático. En dicho caso, el tiempo de espera del firmware puede agotarse y es posible que se pierda la conexión si el sistema cliente lleva mucho tiempo para leer el CD. Si una conexión se interrumpe, vuelva a conectarse desde la GUI y siga con la operación anterior.

Si los valores de configuración de los medios virtuales se cambian en la interfaz web de iDRAC o mediante los comandos de RACADM local, se desconectarán todos los medios conectados en el momento de aplicar el cambio de configuración.

Para volver a conectar la unidad virtual, utilice la ventana **Vista del cliente** de los medios virtuales.

¿Por qué una instalación del sistema operativo Windows a través de medios virtuales lleva mucho tiempo?

Si instala el sistema operativo Windows mediante el DVD *Herramientas y documentación de Dell Systems Management* y la conexión de red es lenta, el procedimiento de instalación puede llevar tiempo para acceder a la interfaz web de iDRAC debido a la latencia de red. La ventana de instalación no indica el progreso de instalación.

¿Cómo se configura el dispositivo virtual como dispositivo de inicio?

En el sistema administrado, acceda a la configuración del BIOS y vaya al menú de inicio. Busque el CD virtual, el disco flexible virtual o la tarjeta vFlash y cambie el orden de inicio de los dispositivos según sea necesario. Asimismo, presione la barra espaciadora en la secuencia de inicio de la configuración de CMOS para hacer que el dispositivo virtual sea de inicio. Por ejemplo, para iniciar desde una unidad de CD, configure la unidad de CD como el primer dispositivo en el orden de inicio.

¿Cuáles son los tipos de medios que se pueden configurar como disco de inicio?

iDRAC 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 a la que el sistema operativo reconoce como disco extraíble
- Una imagen de memoria USB

¿Cómo se configura el dispositivo USB como dispositivo de inicio?

También puede iniciar con un disco de inicio de Windows 98 y copiar los sistemas de archivo desde el disco de inicio al dispositivo USB. Por ejemplo, en el símbolo del sistema, escriba el comando siguiente:

```
sys a: x: /s
```

donde, x: es el dispositivo USB que se debe configurar como dispositivo de inicio.

Los medios virtuales se adjuntan y conectan a disco flexible remoto. Sin embargo, no se encuentra el dispositivo de disco flexible virtual o CD virtual en un sistema que ejecuta el sistema operativo Red Hat Enterprise Linux o SUSE Linux. ¿Cómo se resuelve este problema?

Algunas versiones de Linux no montan automáticamente la unidad de disco flexible virtual y la unidad de CD virtual en el mismo método. Para montar la unidad de disco flexible virtual, busque el nodo de dispositivo que Linux asigna a la unidad de disco flexible virtual. Para montar esta unidad realice lo siguiente:

1. Abra un símbolo del sistema de Linux y ejecute el siguiente comando:

```
grep "Disco virtual" /var/log/messages
```

2. Busque 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
```

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 busque el nombre del dispositivo que se asigna al disco flexible virtual.
5. Asegúrese de estar 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 de dispositivo que se encuentra en el paso 4 y /mnt/floppy es el punto de montaje.

Para montar la unidad de CD virtual, busque el nodo del dispositivo que Linux asigna a la unidad de CD virtual. Para montar esta unidad realice lo siguiente:

1. Abra un símbolo del sistema de Linux y ejecute el siguiente comando:

```
grep "CD virtual" /var/log/messages
```

2. Busque 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
```

hh:mm:ss es la fecha y hora del mensaje que devuelve el comando grep en el paso 1.

4. En el paso 3, lea el resultado del comando grep y busque el nombre del dispositivo que se asignó a *CD virtual* de Dell.
5. Asegúrese de que la unidad de CD virtual está conectada.
6. En la línea de comandos de Linux, ejecute el siguiente comando:

```
mount /dev/sdx /mnt/CD
```

donde, /dev/sdx es el nombre de dispositivo que se encuentra en el paso 4 y /mnt/floppy es el punto de montaje.

¿Por qué las unidades virtuales conectadas al servidor que se quita después de realizar una actualización remota del firmware mediante la interfaz web de iDRAC?

Las actualizaciones del firmware restablecen el iDRAC y hacen que este interrumpa la conexión remota y desmonte las unidades virtuales. Las unidades vuelven a aparecer una vez finalizada el restablecimiento de iDRAC.

¿Por qué todos los dispositivos USB se desconectan después de conectar un dispositivo USB?


Los dispositivos de medios virtuales y los dispositivos vFlash se conectan como dispositivo USB compuesto al BUS de USB de host y comparten un puerto USB común. Cuando se conectan o desconectan dispositivos de medios virtuales o USB vFlash del bus de USB de host, se desconectan temporalmente todos los dispositivos de medios virtuales y vFlash de él. Si el sistema operativo host utiliza un dispositivo de medios virtuales, no conecte ni desconecte uno o más dispositivos de medios virtuales o vFlash. Es recomendable conectar primero todos los dispositivos USB necesarios antes de utilizarlos.

¿Qué hace la opción Restablecer USB?

Restablece los dispositivos USB remotos y locales conectados al servidor.

¿Cómo se maximiza el rendimiento de los medios virtuales?

Para maximizar el rendimiento de los medios virtuales, inicie estos últimos con la consola virtual desactivada o realice una de las acciones siguientes:

- Cambie el control deslizante de rendimiento a la velocidad máxima.
 - Desactive el cifrado tanto para los medios virtuales como para la consola virtual.
-  **NOTA:** En este caso, la transferencia de datos entre el servidor administrado y el iDRAC para los medios virtuales y la consola virtual no estará protegida.
- Si utiliza cualquiera de los sistemas operativos de Windows Server, detiene el servicio de Windows denominado Windows Event Collector. Para ello, vaya a **Inicio** → **Herramientas administrativas** → **Servicios**. Haga clic con el botón derecho del mouse en **Windows Event Collector** y haga clic en **Detener**.

Mientras visualiza el contenido de una unidad de disco flexible o USB, ¿aparece un mensaje de error de conexión si se conecta la misma unidad a través de los medios virtuales?

No se permite el acceso simultáneo a las unidades de disco flexible. Cierre la aplicación que se utiliza para ver el contenido de la unidad antes de intentar virtualizar la unidad.

¿Qué tipo de sistemas de archivos admite la unidad de disco flexible virtual?

La unidad de disco flexible virtual admite los sistemas de archivos FAT16 o FAT32.

¿Por qué se muestra un mensaje de error al intentar conectarse a una unidad DVD/USB a través de medios virtuales aunque estos no estén en uso?

El mensaje de error se muestra si la función Recurso compartido de archivos remotos (RFS) también está en uso. Al mismo tiempo, puede utilizar RFS o medios virtuales, pero no ambos.

Tarjeta vFlash SD

¿Cuándo se bloquea la tarjeta vFlash SD?

La tarjeta vFlash SD se bloquea cuando hay una operación en curso. Por ejemplo, durante una operación de inicialización.

Autenticación SNMP

¿Por qué se muestra el mensaje 'Acceso remoto: error de autenticación SNMP'?

Como parte del descubrimiento, IT Assistant intenta verificar los nombres de comunidad get y set del dispositivo. En IT Assistant, existe el nombre de comunidad get = public y el nombre de comunidad set = private. De manera predeterminada, el nombre de comunidad del agente SNMP para el agente iDRAC es public. Cuando IT Assistant envía una solicitud set, el agente iDRAC genera un error de autenticación SNMP porque acepta solicitudes solamente de community = public.

Para evitar la generación de errores de autenticación SNMP, debe introducir nombres de comunidad aceptados por el agente. Dado que iDRAC solo permite un nombre de comunidad, deberá utilizar el mismo nombre de comunidad get y set para la configuración de descubrimiento de IT Assistant.

Dispositivos de almacenamiento

La información para todos los dispositivos de almacenamiento conectados al sistema no se muestra y OpenManage Storage Management muestra un mayor número de dispositivos de almacenamiento que iDRAC. ¿Por qué?

iDRAC muestra información solamente para los dispositivos capacidad CEM (administración incorporada completa).

iDRAC Service Module


Antes de instalar o ejecutar el módulo de servicio de iDRAC, ¿es necesario desinstalar Open Manage Server Administrator?

No, no es necesario desinstalar Server Administrator. Antes de instalar o ejecutar el módulo de servicio de iDRAC, asegúrese de que haber detenido las funciones de Server Administrator que el módulo de servicio de iDRAC proporciona.

¿Cómo se verifica si el módulo de servicio de iDRAC está instalado en el sistema?

Para saber si el módulo de servicio de iDRAC está instalado en el sistema:

- En Windows:
Ejecute el comando `service.msc`. Busque en la lista de servicios que se muestra si existe un servicio con el nombre **DSM iDRAC Service Module**.
- En Linux:
Ejecute el comando `/etc/init.d/dcismeng status`. Si el módulo de servicio de iDRAC está instalado y en ejecución, el estado que se muestra es **En ejecución**.

 **NOTA:** Utilice el comando `systemctl status dcismeng.service` en lugar del comando `init.d` para verificar si el módulo de servicio de iDRAC está instalado en el sistema operativo Red Hat Enterprise Linux 7.

¿Cómo se verifica el número de versión del módulo de servicio de iDRAC que se encuentra instalado en el sistema?

Para comprobar la versión del módulo de servicio de iDRAC en el sistema, realice cualquiera de las acciones siguientes:

- Haga clic en **Inicio** → **Panel de control** → **Programas y características**. La versión del módulo de servicio de iDRAC instalado aparece en la ficha **Versión**.
- Vaya a **Mi PC** → **Desinstalar o cambiar un programa**.

¿Cuál es el nivel de permisos mínimo necesario para instalar el iDRAC Service Module?

Para instalar el módulo de servicio de iDRAC, es necesario tener privilegios de nivel de administrador.

Al instalar el módulo de servicio de iDRAC, se muestra el mensaje de error No se admite este servidor. Consulte la Guía del usuario para obtener información adicional sobre los servidores admitidos.

¿Cómo se resuelve este problema?

Antes de instalar el módulo de servicio de iDRAC, asegúrese de que el servidor es un servidor PowerEdge de 12.^a generación o posterior. Asimismo, asegúrese de que dispone de un sistema de 64 bits.

Se muestra el siguiente mensaje en el registro del sistema operativo, incluso cuando el paso de sistema operativo a iDRAC mediante USBNIC se ha configurado correctamente. ¿Por qué?

```
The iDRAC Service Module is unable to communicate with iDRAC using the OS to iDRAC Pass-through channel
```

El módulo de servicio de iDRAC utiliza la función de paso de sistema operativo a iDRAC por medio de la NIC de USB para establecer la comunicación con iDRAC. A veces, la comunicación no se establece a través de la interfaz de la NIC de USB configurada con los puntos finales correctos de IP. Esto puede ocurrir cuando la tabla de enrutamiento del sistema operativo host contiene varias entradas para la misma máscara de destino y el destino de la NIC de USB de destino no aparece en la lista como el primero en el orden de enrutamiento.

| Destino | Puerta de enlace | Máscara de red de destino | Indicadores | Métrica | Ref. | Usar Iface |
|----------------|------------------|---------------------------|-------------|---------|------|----------------|
| Predeterminado | 10.94.148.1 | 0.0.0.0 | UG | 1 024 | 0 | 0 em1 |
| 10.94.148.0 | 0.0.0.0 | 255.255.255.0 | U | 0 | 0 | 0 em1 |
| vínculo local | 0.0.0.0 | 255.255.255.0 | U | 0 | 0 | 0 em1 |
| vínculo local | 0.0.0.0 | 255.255.255.0 | U | 0 | 0 | 0 enp0s20u12u3 |

En el ejemplo, **enp0s20u12u3** es la interfaz de la NIC de USB. La máscara de destino de vínculo local se repite y la NIC de USB no es la primera en el orden. Esto genera el problema de conectividad entre el módulo de servicio de iDRAC e iDRAC mediante el paso de sistema operativo a iDRAC. Para solucionar el problema de conectividad, asegúrese de que la dirección IPv4 de la NIC de USB de iDRAC (el valor predeterminado es 169.254.0.1) sea accesible desde el sistema operativo host.


Caso contrario:

- Cambie la dirección de la NIC de USB de iDRAC en una máscara de destino única.
- Elimine las entradas que no son necesarias de la tabla de enrutamiento a fin de asegurarse de que la NIC de USB quede seleccionada por ruta cuando el host desea alcanzar la dirección IPv4 de la NIC de USB de iDRAC.

Cuando se desinstala el módulo de servicio de iDRAC desde un servidor VMware ESXi, el conmutador virtual se denomina como vSwitchiDRACvusb y el grupo de puertos como la red de iDRAC en vSphere Client. ¿Cómo se deben eliminar?

Durante la instalación de VIB para el módulo de servicio de iDRAC en un servidor VMware ESXi, el módulo de servicio de iDRAC crea el conmutador vSwitch y el grupo de puertos Portgroup para comunicarse con iDRAC mediante el paso de sistema operativo a iDRAC en el modo NIC de USB. Después de la desinstalación, el conmutador virtual **vSwitchiDRACvusb** y el grupo de puertos de **red de iDRAC** no se eliminan. Para eliminarlos manualmente, realice uno de los pasos siguientes:

- Vaya al asistente de configuración de vSphere Client y elimine las entradas.
- Vaya a Esxcli y escriba los comandos siguientes:
 - Para desmontar el grupo de puertos: `esxcfg-vmknic -d -p "iDRAC Network"`
 - Para desmontar vSwitch: `esxcfg-vswitch -d vSwitchiDRACvusb`

 **NOTA:** Es posible volver a instalar el módulo de servicio de iDRAC en el servidor VMware ESXi, ya que esto no es un problema funcional para el servidor.

¿En qué parte del sistema operativo se encuentra disponible el registro de Lifecycle replicado?

Para ver los registros de Lifecycle replicados:

| Sistema operativo | Ubicación |
|--|---|
| Microsoft Windows | Visualizador de sucesos → Registros de Windows → Sistema. Todos los registros de Lifecycle del módulo de servicio de iDRAC se replican en el nombre de origen del módulo de servicio de iDRAC . |
| Red Hat Enterprise Linux , SUSE Linux, CentOS y Citrix XenServer | <code>/var/log/messages</code> |
| VMware ESXi | <code>/var/log/syslog.log</code> |

¿Cuáles son los paquetes o ejecutables dependientes de Linux disponibles para la instalación mientras se completa la instalación en Linux?

Para ver la lista de paquetes dependientes de Linux, consulte la sección *Dependencias de Linux* en *iDRAC Service Module Installation Guide* (Guía de instalación del módulo de servicio de iDRAC).

RACADM

Después de realizar un restablecimiento de iDRAC (mediante el comando `racreset` de RACADM), si se emite algún comando, aparece el mensaje siguiente. ¿Qué significa esto?

```
ERROR: Unable to connect to RAC at specified IP address
```

El mensaje indica que antes de emitir otro comando, debe esperar hasta que iDRAC complete el restablecimiento.

Al utilizar comandos y subcomandos de RACADM, algunos errores no quedan claros.

Es posible que reciba uno o más de los siguientes errores cuando use los comandos y subcomandos de RACADM:

- Mensajes de error de RACADM local: problemas de sintaxis, errores tipográficos, nombres incorrectos, etc.
- Mensajes de error de RACADM remota: problemas como, por ejemplo, una dirección IP, un nombre de usuario o una contraseña incorrectos.

Durante una prueba de ping a iDRAC, si el modo de red cambia del modo Dedicado al modo Compartido, no hay respuesta de ping.

Borre la tabla ARP en el sistema.

RACADM remoto no se puede conectar a iDRAC desde SUSE Linux Enterprise Server (SLES) 11 SP1.

Asegúrese de que están instaladas las versiones oficiales de openssl y libopenssl. Ejecute el comando siguiente para instalar los paquetes RPM:

```
rpm -ivh --force < filename >
```

donde `filename` es el archivo de los paquetes openssl o libopenssl.

Por ejemplo:

```
rpm -ivh --force openssl-0.9.8h-30.22.21.1.x86_64.rpm
```

```
rpm -ivh --force libopenssl0_9_8-0.9.8h-30.22.21.1.x86_64.rpm
```

¿Por qué no están disponibles RACADM remoto y los servicios web después de un cambio de propiedad?

Es posible que los servicios de RACADM remota y la interfaz web tarden un poco en estar disponibles después de restablecer el servidor web de iDRAC.

El servidor web iDRAC se restablece en los casos siguientes:

- Cuando la configuración de la red o las propiedades de seguridad de la red se cambian mediante la interfaz web de usuario de iDRAC.
- Cuando la propiedad `cfgRacTuneHttpsPort` cambia (incluso cuando un comando `config -f (config file)` la cambia).
- Cuando se utiliza el comando `racresetcfg`.
- iDRAC se restablece.
- Se carga un nuevo certificado del servidor SSL.

¿Por qué se muestra un mensaje de error si se intenta eliminar una partición después de crearla mediante RACADM local?

Esto sucede debido a que la operación de creación de partición está en curso. Sin embargo, la partición se elimina después de cierto tiempo y se muestra un mensaje donde se confirma la eliminación. De lo

contrario, espere hasta que se complete la operación de creación de partición y luego elimine la partición.

Varios

¿Cómo se busca una dirección IP de iDRAC para un servidor Blade?

Puede buscar la dirección IP de iDRAC mediante uno de los métodos siguientes:

Con la interfaz web de CMC: vaya a **Chasis** → **Servidores** → **Configuración** → **Implementar**. En la tabla que se muestra, consulte la dirección IP del servidor.

Con la consola virtual: reinicie el servidor para consultar la dirección IP de iDRAC durante la prueba POST. Seleccione la consola "Dell CMC" en OSCAR para iniciar sesión en CMC a través de una conexión en serie local. Los comandos RACADM de CMC se pueden enviar desde esta conexión. Consulte *iDRAC8 RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8) para obtener una lista completa de los subcomandos RACADM de CMC.

Desde RACADM local: utilice el comando `racadm getsysinfo`. Por ejemplo:

```
$ racadm getniccfg -m server-1 DHCP Enabled = 1 IP Address = 192.168.0.1 Subnet Mask = 255.255.255.0 Gateway = 192.168.0.1
```


Mediante la pantalla LCD: en el menú principal, resalte el servidor y presione el botón de comprobación. Seleccione el servidor necesario y presione el botón de comprobación.

¿Cómo se busca una dirección IP de CMC relacionada con un servidor Blade?

En la interfaz web de iDRAC: haga clic en **Descripción general** → **Configuración de iDRAC** → **CMC**. Se mostrará la página **Resumen de CMC** con la dirección IP de CMC.

En la consola virtual: seleccione la consola "Dell CMC" en OSCAR para iniciar sesión en CMC a través de una conexión en serie local. Los comandos RACADM de CMC se pueden emitir desde esta conexión. Consulte *iDRAC8 RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC8) para obtener una lista completa de los subcomandos RACADM de CMC.

```
$ racadm getniccfg -m chassis NIC Enabled = 1 DHCP Enabled = 1 Static IP Address = 192.168.0.120 Static Subnet Mask = 255.255.255.0 Static Gateway = 192.168.0.1 Current IP Address = 10.35.155.151 Current Subnet Mask = 255.255.255.0 Current Gateway = 10.35.155.1 Speed = Autonegotiate Duplex = Autonegotiate
```

 **NOTA:** También puede hacer esto mediante RACADM remota.

¿Cómo se busca una dirección IP de iDRAC para un servidor tipo bastidor o torre?

Desde la interfaz web de iDRAC: vaya a **Descripción general** → **Servidor** → **Propiedades** → **Resumen**. Se mostrará la página **Resumen del sistema** con la dirección IP de iDRAC.

Desde RACADM local: utilice el comando `racadm getsysinfo`.

Desde el panel LCD: en el servidor físico, utilice los botones de navegación en el panel LCD para ver la dirección IP de iDRAC. Vaya a **Vista de la configuración** → **Vista** → **IP de iDRAC** → **IPv4** o **IPv6** → **IP**.

Desde OpenManage Server Administrator: en la interfaz web de Server Administrator, vaya a **Gabinete modular** → **Módulo de sistema/servidor** → **Chasis del sistema principal/Sistema principal** → **Acceso remoto**.

La conexión de red de iDRAC no funciona.

Servidores Blade:

- 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.

Servidores tipo bastidor y torre:

- En el modo compartido, asegúrese de que el cable LAN esté conectado al puerto NIC donde aparezca el símbolo de llave inglesa.
- En el modo dedicado, asegúrese de que el cable LAN esté conectado al puerto LAN de iDRAC.
- Asegúrese de que esté activada en el sistema la configuración de NIC, la de IPv4 e IPv6, y que además esté activada la modalidad estática o DHCP.

El servidor Blade se ha insertado en el chasis y se ha presionado el interruptor de corriente, pero el servidor no se encendió.

- iDRAC requiere hasta dos minutos para inicializar antes de que el servidor pueda encenderse.
- Compruebe el presupuesto de alimentación de CMC. Es posible que se haya superado el presupuesto de alimentación del chasis.

¿Cómo se recupera el nombre de usuario y la contraseña de usuario administrativo de iDRAC?

El iDRAC se debe restaurar a sus valores predeterminados. Para obtener más información, consulte [Restablecimiento de iDRAC a la configuración predeterminada de fábrica](#).

¿Cómo se cambia el nombre de la ranura para el sistema en un chasis?

1. Inicie sesión en la interfaz web de CMC y vaya a **Chasis** → **Servidores** → **Configuración**.
2. Introduzca el nuevo nombre para la ranura en la fila del servidor y haga clic en **Aplicar**.

iDRAC en el servidor blade no responde durante el inicio.

Retire el servidor e insértelo nuevamente.

Compruebe la interfaz web de CMC para ver si iDRAC se muestra como componente que se puede actualizar. De ser así, siga las instrucciones disponibles en [Actualización del firmware mediante la interfaz web de CMC](#).

Si el problema persiste, póngase en contacto con el servicio de asistencia técnica.

Cuando se intenta iniciar el servidor administrado, el indicador de alimentación es de color verde, pero no hay POST ni video.

Esto sucede debido a 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 acceder a ella.
- Falta la tarjeta vertical de video o esta no está conectada correctamente.

Asimismo, consulte los mensajes de error del registro de iDRAC mediante la interfaz web de iDRAC o desde el panel LCD del servidor.

Situación de uso

En esta sección se proporciona información que ayuda a navegar por secciones específicas del manual con el fin de utilizar escenarios prácticos típicos.


Solución de problemas de un Managed System inaccesible

Tras recibir alertas de OpenManage Essentials, Dell Management Console o un recopilador de capturas locales, cinco servidores de un centro de datos no están accesibles debido a problemas como, por ejemplo, bloqueo del sistema operativo o el servidor. Se necesita identificar la causa para la solución de problemas y poner el servidor en servicio mediante iDRAC.

Antes de realizar la solución de problemas de un servidor inaccesible, asegúrese de que se cumplan los siguientes prerrequisitos:

- Activación de la última pantalla de último bloqueo
- Activación de las alertas en iDRAC

Para identificar la causa, compruebe lo siguiente en la interfaz web de iDRAC y restablezca la conexión al sistema:

 **NOTA:** Si no puede acceder a la interfaz web de iDRAC, vaya al servidor, acceda al panel LCD, escriba la dirección IP o el nombre de host y luego realice las siguientes operaciones mediante la interfaz web del iDRAC desde su estación de administración:

- Estado del LED del servidor: parpadea en color ámbar o permanece sólido en ámbar.
- Estado del LCD del panel anterior o mensaje de error: color ámbar del LCD o mensaje de error.
- La imagen del sistema operativo se muestra en la consola virtual. si puede ver la imagen, restablezca el sistema (reinicio mediante sistema operativo) y vuelva a iniciar sesión. Si puede iniciar sesión, el problema se habrá corregido.
- Pantalla de último bloqueo.
- Video de captura de inicio.
- Video de captura de error.
- Estado de condición del sistema: iconos x rojos para los componentes del sistema con error.
- Estado de la matriz de almacenamiento: matriz posiblemente fuera de línea o con error.
- Registro de Lifecycle para sucesos críticos relacionados con el hardware y el firmware del sistema y las entradas del registro grabadas en el momento del error del sistema.
- Genere un informe de asistencia técnica y vea los datos recopilados.
- Utilizar funciones de supervisión proporcionadas por el módulo de servicio de iDRAC

Enlaces relacionados

[Vista previa de la consola virtual](#)

- [Visualización de videos de captura de inicio y bloqueo](#)
- [Visualización de la condición del sistema](#)
- [Visualización de registros](#)
- [Generación de un informe de asistencia técnica](#)
- [Inventario y supervisión de dispositivos de almacenamiento](#)
- [Uso del módulo de servicio del iDRAC](#)

Obtención de la información del sistema y evaluación de la condición del sistema

Para obtener la información del sistema y evaluación de la condición del sistema:

- En la interfaz web de iDRAC, vaya a **Descripción general** → **Servidor** → **Resumen del sistema** para ver la información del sistema y acceder a los distintos vínculos de esta página y evaluar la condición del sistema. Por ejemplo, puede comprobar la condición del ventilador del chasis.
- También puede configurar el LED de localización del chasis y, en función del color, evaluar la condición del sistema.
- Si el módulo de servicio del iDRAC está instalado, se muestra la información del host del sistema operativo.

Enlaces relacionados

- [Visualización de la condición del sistema](#)
- [Uso del módulo de servicio del iDRAC](#)
- [Generación de un informe de asistencia técnica](#)


Establecimiento de alertas y configuración de alertas por correo electrónico

Para establecer alertas y configurar alertas por correo electrónico:

1. Active las alertas.
2. Configure la alerta por correo electrónico y compruebe los puertos.
3. Realice un reinicio, un apagado o un ciclo de encendido del sistema administrado.
4. Envíe una alerta de prueba.

Visualización y exportación del registro de Lifecycle y el registro de sucesos del sistema

Para ver y exportar el registro de lifecycle y el registro de sucesos del sistema (SEL):

1. En la interfaz web de iDRAC, vaya a **Descripción general** → **Servidor** → **Registros** para ver SEL y **Descripción general** → **Servidor** → **Registros** → **Registro de Lifecycle** para ver el registro de Lifecycle.
 -  **NOTA:** El SEL también se graba en el registro de lifecycle mediante las opciones de filtrado para ver el SEL.
2. Exporte el SEL o el registro de lifecycle en el formato XML a una ubicación externa (estación de administración, USB, recurso compartido de red, etc.). Como alternativa, puede activar el registro de sistema remoto de modo que los registros que se graban en el registro de lifecycle también se escriben simultáneamente en los servidores de remoto configurado.

3. Si está utilizando el módulo de servicio del iDRAC, exporte el registro de Lifecycle al registro del sistema operativo. Para obtener más información, consulte [Uso del módulo de servicio del iDRAC](#).

Interfaces para actualizar el firmware de iDRAC

Utilice las interfaces siguientes para actualizar el firmware de iDRAC:

- Interfaz web del iDRAC
- CLI de RACADM (iDRAC y CMC)
- Dell Update Package (DUP)
- Interfaz web del CMC
- Lifecycle Controller–Remote Services
- Lifecycle Controller
- Dell Remote Access Configuration Tool (DRACT)

Realización de un apagado ordenado del sistema

Para realizar un apagado ordenado, vaya a una de las ubicaciones siguientes en la interfaz web de iDRAC:

- **Información general** → **Servidor** → **Alimentación/Térmico** → **Configuración de alimentación** → **Control de alimentación**. Se muestra la página **Control de alimentación**. Seleccione **Apagado ordenado** y haga clic en **Aplicar**.
- **Descripción general** → **Servidor** → **Alimentación/Térmico** → **Supervisión de alimentación**. En el menú desplegable **Control de alimentación**, seleccione **Apagado ordenado** y haga clic en **Aplicar**.

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

Creación de una nueva cuenta de usuario de administrador

Puede modificar la cuenta de usuario de administrador local predeterminada o crear una cuenta de usuario de administrador nueva. Para modificar la cuenta local, consulte [Modificación de la configuración de la cuenta de administrador local](#).

Para crear una cuenta de usuario de administrador nueva, consulte las secciones siguientes:

- [Configuración de usuarios locales](#)
- [Configuración de usuarios de Active Directory](#)
- [Configuración de los usuarios LDAP genéricos](#)

Inicio de la consola remota de servidores y montaje de una unidad USB

Para iniciar la consola remota de servidores y montaje de una unidad USB:

1. Conecte una unidad flash USB (con la imagen necesaria) a una estación de administración.
2. Utilice uno de los métodos siguientes para iniciar la consola virtual a través de la interfaz web de iDRAC:

- Vaya a **Información general** → **Servidor** → **Consola virtual** y haga clic en **Iniciar consola virtual**.
- Vaya a **Información general** → **Servidor** → **Propiedades** y haga clic en **Iniciar** bajo **Vista previa de consola virtual**.

Se muestra el **Vista previa de consola virtual**.

3. En el menú **Archivo**, haga clic en **Medios virtuales** → **Iniciar medios virtuales**.
4. Haga clic en **Agregar imagen** y seleccione la imagen situada en la unidad flash USB.
La imagen se agrega a la lista de unidades disponibles.
5. Seleccione la unidad para asignarla. La imagen de la unidad flash USB se asigna al sistema administrado.

Instalación del sistema operativo básico conectado a los medios virtuales y los recursos compartidos de archivos remotos

Para ello, consulte [Implementación del sistema operativo mediante recurso compartido de archivos remotos](#).

Administración de la densidad de bastidor

Supongamos que se han instalado dos servidores en un bastidor. Para agregar dos servidores adicionales, se debe determinar cuánta capacidad queda en el bastidor.

Para evaluar la capacidad de un bastidor con el fin de agregar servidores adicionales:

1. Consulte los datos de consumo de alimentación actuales y los históricos de los servidores.
2. Según los datos, la infraestructura de alimentación y las limitaciones del sistema de refrigeración, active la política de límites de alimentación y establezca los valores de los límites.



NOTA: Es recomendable establecer una limitación cercana al pico y luego utilizar ese nivel de limitación para determinar cuánta capacidad queda en el bastidor para la adición de servidores adicionales.

Instalación de una nueva licencia electrónica

Para obtener más información, consulte [Operaciones de licencia](#).

Aplicación de valores de configuración de la identidad de E/S para varias tarjetas de red en un reinicio del sistema host individual

Si tiene varias tarjetas de red en un servidor que es parte de un entorno de red de área de almacenamiento (SAN) y desea aplicar distintas direcciones virtuales y valores de configuración de iniciador y destino para dichas tarjetas, utilice la función Optimización de la identidad de E/S para reducir el tiempo de configuración de los valores. Para hacerlo:

1. Asegúrese de que el BIOS, el iDRAC y las tarjetas de red están actualizadas a la versión de firmware más reciente.
2. Active la Optimización de la identidad de E/S.

3. Exporte el archivo de configuración XML desde el iDRAC.
4. Edite los valores de configuración de la optimización de la identidad de E/S en el archivo XML.
5. Importe el archivo de configuración XML al iDRAC.

Enlaces relacionados

[Actualización del firmware de dispositivos](#)

[Activación o desactivación de la optimización de la identidad de E/S](#)