

Integrated Dell Remote Access Controller 7 (iDRAC7)
Versión 1.00.00 Guía del usuario



Notas, precauciones y avisos



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



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



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

La información contenida en esta publicación puede modificarse sin aviso.

© 2012 Dell Inc. Todos los derechos reservados.

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

Marcas comerciales utilizadas en este texto: Dell™, el logotipo de Dell, Dell Precision™, OptiPlex™, Latitude™, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, EqualLogic™, Compellent™, KACE™, FlexAddress™, Force10™ y Vostro™ son marcas comerciales de Dell Inc. Intel®, Pentium®, Xeon, Core® y Celeron® son marcas comerciales registradas de Intel Corporation en los EE. UU. y otros países. AMD® es una marca comercial registrada y AMD Opteron®, AMD Phenom™ y AMD Sempron™ son marcas comerciales de Advanced Micro Devices, Inc. Microsoft™, Windows®, Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista® y Active Directory® son marcas comerciales o son marcas comerciales registradas de Microsoft Corporation en los Estados Unidos y otros países. Red Hat® y Red Hat Enterprise Linux® son marcas comerciales registradas de Red Hat, Inc. en los Estados Unidos y otros países. Novell® y SUSE® son marcas comerciales registradas de Novell Inc. en los Estados Unidos y otros países. Oracle® es una marca comercial registrada de Oracle Corporation o sus afiliados. Citrix®, Xen®, XenServer® y XenMotion® son marcas comerciales registradas o marcas comerciales de Citrix Systems, Inc. en los Estados Unidos y otros países. VMware®, Virtual SMP®, vMotion®, vCenter® y vSphere® son marcas comerciales registradas o marcas comerciales de VMware, Inc. en los Estados Unidos y otros países. IBM® es una marca comercial registrada de International Business Machines Corporation.

Este documento puede incluir otras marcas y nombres comerciales para referirse a las entidades propietarias o a sus productos. Dell Inc. renuncia a cualquier interés sobre la propiedad de marcas y nombres comerciales que no sean los suyos.

2012 - 03

Rev. A00

Tabla de contenido

Notas, precauciones y avisos.....	2
Capítulo 1: Información general.....	13
Ventajas de utilizar iDRAC7 con Lifecycle Controller.....	13
Funciones clave.....	14
Administración de licencias	15
Tipos de licencias.....	15
Adquisición de licencias.....	15
Operaciones de licencia.....	16
Funciones con licencia en iDRAC7.....	17
Interfaces y protocolos para acceder a iDRAC7.....	20
Información de puertos iDRAC7.....	22
Otros documentos que podrían ser de utilidad.....	23
Cómo ponerse en contacto con Dell.....	24
Capítulo 2: Inicio de sesión en iDRAC7.....	25
Inicio de sesión en iDRAC7 como usuario local de Active Directory o usuario LDAP.....	25
Inicio de sesión en el iDRAC7 mediante una tarjeta inteligente.....	26
Inicio de sesión en iDRAC7 como usuario local mediante una tarjeta inteligente.....	26
Inicio de sesión en iDRAC7 como usuario de Active Directory mediante una tarjeta inteligente.....	27
Inicio de sesión en iDRAC7 mediante inicio de sesión único	27
Inicio de sesión SSO de iDRAC7 mediante la interfaz web de iDRAC7.....	27
Inicio de sesión SSO de iDRAC7 mediante la interfaz web de iDRAC7.....	28
Acceso a iDRAC7 mediante RACADM remoto.....	28
Validación del certificado de CA para usar RACADM remoto en Linux.....	28
Acceso a iDRAC7 mediante RACADM local.....	29
Acceso a iDRAC7 mediante RACADM de firmware.....	29
Acceso a iDRAC7 mediante SMCLP.....	29
Inicio de sesión en iDRAC7 mediante la autenticación de clave pública.....	29
Varias sesiones iDRAC7.....	29
Capítulo 3: Configuración de Managed System y Management Station.....	31
Configuración de la dirección IP de iDRAC7.....	31
Configuración de la IP de iDRAC mediante la utilidad de configuración de iDRAC.....	32
Configuración de la IP de iDRAC7 mediante la interfaz web de CMC.....	35
Activación del descubrimiento automático.....	35
Configuración de Management Station.....	36

Acceso a iDRAC7 de manera remota.....	36
Configuración de Managed System.....	37
Modificación de la configuración de la cuenta de administrador local.....	37
Configuración de la ubicación de Managed System.....	37
Configuración de exploradores web compatibles.....	38
Adición de iDRAC7 a la lista de dominios de confianza.....	40
Desactivación de la función de lista blanca en Firefox.....	41
Visualización de las versiones traducidas de la interfaz web.....	41
Actualización del firmware de iDRAC7.....	41
Descarga del firmware de iDRAC7.....	42
Actualización del firmware mediante la interfaz web de iDRAC7.....	42
Actualización del firmware mediante la interfaz web de CMC.....	44
Actualización del firmware mediante DUP.....	44
Actualización del firmware mediante RACADM remoto.....	44
Actualización del firmware mediante Lifecycle Controller Remote Services.....	45
Reversión del firmware de iDRAC7.....	45
Reversión del firmware mediante la interfaz web de iDRAC7.....	45
Reversión del firmware mediante la interfaz web de CMC.....	46
Reversión del firmware mediante RACADM.....	46
Reversión del firmware mediante Lifecycle Controller.....	46
Reversión del firmware mediante Lifecycle Controller Remote Services.....	46
Recuperación de iDRAC7.....	46
Uso del servidor TFTP.....	47
Supervisión de iDRAC7 mediante otras herramientas de administración del sistema.....	47

Capítulo 4: Configuración de iDRAC7..... 49

Visualización de la información iDRAC7.....	50
Visualización de la información de iDRAC7 mediante la interfaz web.....	50
Visualización de la información de iDRAC7 mediante RACADM.....	50
Modificación de la configuración de red.....	50
Modificación de la configuración de red mediante la interfaz web.....	51
Modificación de la configuración de red mediante RACADM local.....	51
Configuración del filtrado de IP y bloqueo de IP.....	51
Configuración de servicios.....	53
Configuración de servicios mediante la interfaz web.....	53
Configuración de los servicios mediante RACADM.....	54
Configuración del panel frontal.....	54
Configuración de los valores de LCD.....	54
Configuración del valor LED del ID del sistema.....	55
Configuración del primer dispositivo de inicio.....	56
Configuración del primer dispositivo de inicio mediante la interfaz web.....	56
Configuración del primer dispositivo de inicio mediante RACADM.....	56

Activación de la comunicación de la administración de sistemas internos.....	57
Activación de la pantalla de último bloqueo.....	57
Obtención de certificados.....	58
Certificados de servidor SSL.....	59
Generación de una nueva solicitud de firma de certificado.....	59
Carga del certificado del servidor.....	60
Visualización del certificado del servidor.....	60
Configuración de varios iDRAC7s mediante RACADM.....	61
Creación de un archivo de configuración de iDRAC7.....	61
Reglas de análisis.....	62
Modificación de la dirección IP de iDRAC7.....	63
Desactivación del acceso para modificar los valores de configuración de iDRAC7 en el sistema host.....	64
Capítulo 5: Visualización de la información de iDRAC7 y Managed System.....	65
Visualización de la condición y las propiedades de Managed System.....	65
Visualización del inventario del sistema.....	65
Visualización de la información del sensor.....	66
Inventario y supervisión de dispositivos de almacenamiento.....	67
Supervisión de dispositivos de almacenamiento mediante la interfaz web.....	68
Supervisión de dispositivos de almacenamiento mediante RACADM.....	68
Inventario y supervisión de dispositivos de red.....	68
Supervisión de dispositivos de red mediante la interfaz web.....	69
Supervisión de dispositivos de red mediante RACADM.....	69
Visualización de las conexiones de red Fabric de la tarjeta mezzanine FlexAddress.....	69
Visualización o terminación de sesiones iDRAC7.....	70
Terminación de las sesiones de iDRAC7 mediante la interfaz web.....	70
Terminación de las sesiones de iDRAC7 mediante RACADM.....	70
Capítulo 6: Configuración de la comunicación de iDRAC7.....	71
Comunicación con iDRAC7 a través de una conexión serie mediante un cable DB9.....	72
Configuración del BIOS para la conexión serie.....	72
Activación de la conexión serie RAC.....	73
Activación de los modos básicos y de terminal de la conexión serie básica IPMI.....	73
Cambio entre la comunicación en serie RAC y la consola de comunicación en serie mediante el cable DB9.....	75
Cambio de una consola de comunicación en serie a la comunicación en serie RAC.....	75
Cambio de una comunicación en serie RAC a consola de comunicación en serie.....	75
Comunicación con iDRAC7 mediante IPMI SOL.....	76
Configuración del BIOS para la conexión serie.....	76
Configuración de iDRAC7 para utilizar SOL.....	76
Activación del protocolo compatible.....	77
Comunicación con iDRAC7 mediante IPMI en la LAN.....	81
Configuración de IPMI en la LAN mediante la interfaz web.....	81

Configuración de IPMI en la LAN mediante la utilidad de configuración de iDRAC.....	81
Configuración de IPMI en la LAN mediante RACADM.....	82
Activación o desactivación de RACADM remoto.....	82
Activación o desactivación de RACADM remoto mediante la interfaz web.....	82
Activación o desactivación de RACADM remoto mediante RACADM.....	82
Desactivación de RACADM local.....	82
Activación de IPMI en Managed System.....	83
Configuración de Linux para la consola de comunicación en serie durante el inicio.....	83
Activación del inicio de sesión en la consola virtual después del inicio.....	83
Esquemas de criptografía SSH compatibles.....	84
Uso de la autenticación de clave pública para SSH.....	85

Capítulo 7: Configuración de cuentas de usuario y privilegios.....89

Configuración de usuarios locales.....	89
Configuración de usuarios locales mediante la interfaz web de iDRAC7.....	89
Configuración de los usuarios locales mediante RACADM.....	90
Configuración de usuarios de Active Directory.....	92
Prerrequisitos del uso de la autenticación de Active Directory para iDRAC7.....	93
Mecanismos de autenticación compatibles de Active Directory.....	95
Generalidades del esquema estándar de Active Directory.....	95
Configuración del esquema estándar de Active Directory.....	96
Información general sobre el esquema extendido de Active Directory.....	99
Configuración del esquema extendido de Active Directory.....	101
Prueba de la configuración de Active Directory.....	109
Configuración de los usuarios LDAP genéricos.....	110
Configuración del servicio de directorio de LDAP genérico mediante la interfaz web de iDRAC7.....	110
Configuración del servicio de directorio LDAP genérico mediante RACADM.....	111
Prueba de la configuración del servicio de directorio de LDAP.....	111

Capítulo 8: Configuración de iDRAC7 para inicio de sesión único o inicio de sesión mediante tarjeta inteligente..... 113

Prerrequisitos para el inicio de sesión único de Active Directory o el inicio de sesión mediante tarjeta inteligente.....	113
Registro de iDRAC7 como equipo en el dominio raíz de Active Directory.....	114
Generación del archivo Keytab de Kerberos.....	114
Creación de objetos de Active Directory y establecimiento de privilegios.....	115
Configuración del explorador para activar el inicio de sesión único de Active Directory.....	115
Configuración del inicio de sesión SSO de iDRAC7 para usuarios de Active Directory.....	116
Configuración del inicio de sesión SSO de iDRAC7 para usuarios de Active Directory mediante la interfaz web.....	116
Configuración del inicio de sesión SSO de iDRAC7 para usuarios de Active Directory mediante RACADM.....	116

Configuración del inicio de sesión mediante tarjeta inteligente de iDRAC7 para usuarios locales.....	116
Carga del certificado de usuario de tarjeta inteligente.....	117
Carga del certificado de CA de confianza para tarjeta inteligente.....	117
Configuración del inicio de sesión mediante tarjeta inteligente de iDRAC7 para usuarios de Active Directory.....	118
Activación o desactivación del inicio de sesión mediante tarjeta inteligente.....	118
Activación o desactivación del inicio de sesión mediante tarjeta inteligente utilizando la interfaz web.....	119
Activación o desactivación del inicio de sesión mediante tarjeta inteligente utilizando RACADM.....	119
Activación o desactivación del inicio de sesión mediante tarjeta inteligente mediante la utilidad de configuración de iDRAC.....	119
Capítulo 9: Configuración de iDRAC7 para enviar alertas.....	121
Activación o desactivación de alertas.....	121
Activación o desactivación de alertas mediante la interfaz web.....	121
Activación o desactivación de alertas mediante RACADM.....	122
Activación o desactivación de alertas mediante la utilidad de configuración de iDRAC.....	122
Filtrado de alertas	122
Filtrado de alertas mediante la interfaz web de iDRAC7.....	122
Filtrado de alertas mediante RACADM.....	123
Configuración de alertas de suceso.....	123
Configuración de alertas de suceso mediante la interfaz web.....	123
Configuración de alertas de suceso mediante RACADM.....	123
Configuración de acciones del suceso.....	123
Configuración de acciones del suceso mediante la interfaz web.....	124
Configuración de acciones del suceso mediante RACADM.....	124
Configuración de la captura SNMP o IPMI para alertas por correo electrónico.....	124
Configuración de destinos de alerta IP.....	124
Configuración de los valores de alerta por correo electrónico.....	126
ID de mensaje de alertas.....	127
Capítulo 10: Administración de registros.....	131
Visualización del registro de sucesos del sistema.....	131
Visualización del registro de sucesos del sistema mediante la interfaz web.....	131
Visualización del registro de sucesos del sistema mediante RACADM.....	131
Visualización del registro de Lifecycle	132
Visualización del registro de Lifecycle mediante la interfaz web.....	132
Visualización del registro de Lifecycle mediante RACADM.....	133
Adición de notas de trabajo.....	133
Configuración del registro del sistema remoto.....	133
Configuración del registro del sistema remoto mediante la interfaz web.....	133
Configuración del registro del sistema remoto mediante RACADM.....	133
Capítulo 11: Supervisión y administración de la alimentación.....	135

Supervisión de la alimentación.....	135
Supervisión de la alimentación mediante la interfaz web.....	135
Supervisión de la alimentación mediante RACADM.....	136
Ejecución de las operaciones de control de alimentación.....	136
Ejecución de las operaciones de control de alimentación mediante la interfaz web.....	136
Ejecución de las operaciones de control de alimentación mediante RACADM.....	136
Límites de alimentación.....	136
Límites de alimentación en servidores Blade.....	136
Visualización y configuración de la política de límites de alimentación.....	137
Configuración de las opciones de suministro de energía.....	138
Configuración de las opciones de suministro de energía mediante la interfaz web.....	139
Configuración de las opciones de suministro de energía mediante RACADM.....	139
Configuración de las opciones de suministro de energía mediante la utilidad de configuración de iDRAC.....	139
Activación o desactivación del botón de encendido.....	139
Capítulo 12: Configuración y uso de la consola virtual.....	141
Resoluciones de pantalla y velocidades de actualización admitidas.....	141
Configuración de exploradores web para utilizar la consola virtual.....	142
Configuración de exploradores web para utilizar el complemento Java.....	142
Configuración de IE para utilizar el complemento ActiveX.....	143
Importación de certificados de CA a Management Station.....	144
Configuración de la consola virtual.....	145
Configuración de la consola virtual mediante la interfaz web.....	145
Configuración de la consola virtual mediante RACADM.....	145
Vista previa de la consola virtual.....	146
Inicio de la consola virtual.....	146
Inicio de la consola virtual mediante la interfaz web.....	147
Inicio de la consola virtual mediante URL.....	147
Uso del visor de la consola virtual.....	148
Sincronización de los punteros del mouse.....	148
Pulsación de teclas a través de la consola virtual.....	149
Capítulo 13: Administración de medios virtuales.....	153
Unidades y dispositivos compatibles.....	154
Configuración de medios virtuales.....	154
Configuración de medios virtuales mediante la interfaz web de iDRAC7.....	154
Configuración de medios virtuales mediante RACADM.....	155
Configuración de medios virtuales mediante la utilidad de configuración de iDRAC.....	155
Estado de medios conectados y respuesta del sistema.....	155
Acceso a medios virtuales.....	155
Inicio de medios virtuales mediante la consola virtual.....	155

Inicio de medios virtuales sin usar la consola virtual.....	156
Adición de imágenes de medios virtuales.....	156
Eliminación de imágenes de medios virtuales.....	157
Visualización de los detalles del dispositivo virtual.....	157
Restablecimiento de USB.....	157
Asignación de la unidad virtual.....	157
Anulación de la asignación de la unidad virtual.....	158
Configuración del orden de inicio a través del BIOS.....	158
Activación del inicio único para medios virtuales.....	159
Capítulo 14: Instalación y uso de la utilidad de VMCLI.....	161
Instalación de VMCLI.....	161
Ejecución de la utilidad de VMCLI.....	161
Sintaxis de VMCLI.....	161
Comandos de VMCLI para acceder a los medios virtuales	162
Opciones de shell del sistema operativo de VMCLI	163
Capítulo 15: Administración de la tarjeta vFlash SD.....	165
Configuración de la tarjeta vFlash SD.....	165
Visualización de las propiedades de la tarjeta vFlash SD.....	165
Activación o desactivación de la funcionalidad vFlash.....	166
Inicialización de la tarjeta vFlash SD.....	167
Obtención del último estado mediante RACADM.....	168
Administración de las particiones vFlash.....	168
Creación de una partición vacía.....	168
Creación de una partición mediante un archivo de imagen.....	169
Formateo de una partición.....	170
Visualización de las particiones disponibles.....	171
Modificación de una partición.....	171
Conexión o desconexión de particiones.....	172
Eliminación de las particiones existentes.....	173
Descarga del contenido de una partición.....	174
Inicio de una partición.....	174
Capítulo 16: Uso de SMCLP.....	177
Capacidades de System Management mediante SMCLP.....	177
Ejecución de los comandos SMCLP.....	177
Sintaxis SMCLP de iDRAC7.....	178
Navegación en el espacio de direcciones de MAP.....	180
Uso de Show Verb.....	181
Uso de la opción -display.....	181
Uso de la opción -level.....	181

Uso de la opción -output.....	181
Ejemplos de uso.....	181
Administración de la alimentación del servidor.....	182
Administración de SEL.....	182
Navegación en MAP del destino.....	183
Capítulo 17: Implementación de los sistemas operativos.....	185
Implementación del sistema operativo mediante VMCLI	185
Implementación del sistema operativo mediante recurso compartido de archivos remotos.....	186
Administración de recursos compartidos de archivos remotos.....	187
Configuración de recursos compartidos de archivos remotos mediante la interfaz web.....	187
Configuración de recursos compartidos de archivos remotos mediante RACADM.....	188
Implementación del sistema operativo mediante medios virtuales.....	188
Instalación del sistema operativo desde varios discos.....	189
Implementación del sistema operativo incorporado en la tarjeta SD.....	189
Activación del módulo SD y la redundancia del BIOS.....	189
Capítulo 18: Solución de problemas de Managed System mediante iDRAC7.....	191
Uso de la consola de diagnósticos.....	191
Visualización de los códigos de la POST.....	191
Visualización de videos de captura de inicio y bloqueo.....	192
Visualización de registros.....	192
Visualización de la pantalla de último bloqueo del sistema.....	192
Visualización del estado del panel frontal.....	193
Visualización del estado del LCD del panel frontal del sistema.....	193
Visualización del estado del LED del panel anterior del sistema.....	193
Indicadores de problemas del hardware.....	194
Visualización de la condición del sistema.....	194
Consulta de la pantalla de estado del servidor en busca de mensajes de error.....	195
Reinicio de iDRAC7.....	195
Reinicio de iDRAC7 mediante la interfaz web de iDRAC7.....	195
Restablecimiento de iDRAC7 mediante RACADM.....	195
Restablecimiento de iDRAC7 a la configuración predeterminada de fábrica.....	195
Capítulo 19: Preguntas más frecuentes.....	197
Registro de sucesos del sistema.....	197
Seguridad de la red.....	197
Active Directory.....	198
Inicio de sesión único.....	200
Inicio de sesión mediante tarjeta inteligente.....	201
Consola virtual.....	202
Medios virtuales.....	205

Tarjeta vFlash SD.....	207
Autenticación SNMP.....	207
Dispositivos de almacenamiento.....	207
RACADM.....	208
Varios.....	208
Capítulo 20: Situación de uso.....	211
Solución de problemas de un Managed System inaccesible.....	211
Obtención de la información del sistema y evaluación de la condición del sistema.....	211
Configuración de alertas y alertas por correo electrónico.....	212
Visualización y exportación del registro de Lifecycle y el registro de sucesos del sistema.....	212
Interfaces para actualizar el firmware de iDRAC.....	212
Realización de un apagado ordenado del sistema.....	212
Creación de una cuenta de usuario de administrador.....	213
Inicio de la consola remota de servidores y montaje de una unidad USB.....	213
Instalación del sistema operativo básico conectado a los medios virtuales y los recursos compartidos de archivos remotos.....	213
Administración de la densidad de bastidor.....	213
Instalación de una nueva licencia electrónica.....	214

Información general

Integrated Dell Remote Access Controller 7 (iDRAC7) está diseñado para mejorar la productividad de los administradores de servidor y mejorar la disponibilidad global de los servidores de Dell. iDRAC7 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.

iDRAC7 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 iDRAC7 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

iDRAC7 está disponible en las variantes siguientes:

- Administración básica con IPMI
- iDRAC7 Express
- iDRAC7 Express para servidores Blade
- iDRAC7 Enterprise

Para obtener más información, consulte la *iDRAC7 Overview and Feature Guide* (Guía de información general y funciones de iDRAC7) disponible en support.dell.com.

Ventajas de utilizar iDRAC7 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 servicios remotos de Dell Lifecycle Controller) disponible en support.dell.com/manuals.

Funciones clave

Entre las funciones clave de iDRAC7 se incluye lo siguiente:

Inventario y supervisión

- Visualización de la condición del servidor administrado
- Inventario y supervisión de los adaptadores de red y los subsistemas de almacenamiento sin agentes de sistema operativo
- Visualización del inventario del sistema
- Visualización de la información del sensor
- Supervisión y control del uso de la alimentación
- 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 iDRAC7 a través del panel LCD del chasis M1000E y conexiones de consola local. Para obtener más información, consulte la *Chassis Management Controller User's Guide* (Guía del usuario de Chassis Management Controller) disponible en support.dell.com/manuals.

Implementación

- Administración de las particiones de tarjeta vFlash SD
- Configuración de los valores de visualización del panel frontal
- Inicio de Lifecycle Controller, que permite configurar y actualizar el BIOS y los adaptadores de red y de almacenamiento compatibles
- Administración de la configuración de red de iDRAC7
- 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

Actualización

- Administración de licencias de iDRAC7
- Actualización o reversión del firmware de iDRAC7


Mantenimiento y solución de problemas

- Operaciones relacionadas con la alimentación y supervisión del consumo de alimentación
- Independencia de Server Administrator para la generación de alertas
- Registro de datos de sucesos: registro de ciclos de vida y registros
- Configuración de alertas por correo electrónico, IPMI o SNMP 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

Conectividad segura

Proteger el acceso a recursos de red críticos es una prioridad. iDRAC7 implementa una variedad de funciones de seguridad entre las que se incluye lo siguiente:

- Capa de sockets seguros (SSL)
- Actualizaciones de firmware firmadas
- Autenticación de usuarios por medio de Microsoft Active Directory, servicio de directorio de LDAP genérico o identificaciones y contraseñas de usuario administradas a nivel 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
- Configuración de la identificación y contraseña del usuario
- 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 (for 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 iDRAC7
- Adaptador Gigabit Ethernet dedicado en servidores tipo bastidor y torre con licencia empresarial.

Administración de licencias

Las funciones de iDRAC7 están disponibles según la licencia adquirida (Basic Management, iDRAC7 Express, iDRAC7 Express for Blades o iDRAC7 Enterprise). Solo las funciones con licencia están disponibles en la interfaces que permite configurar o utilizar iDRAC7. Por ejemplo, la interfaz web de iDRAC7, RACADM, WS-MAN, OpenManage Server Administrator, etc. Algunas funciones, tal 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 administración y actualización del firmware de licencias de iDRAC7 siempre está disponible a través de la interfaz web de iDRAC7 y RACADM.

Tipos de licencias

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

- Evaluación de 30 días y extensión: la licencia caduca después de 30 días y puede extenderse otros 30 días. Las licencias de evaluación se basan en períodos de tiempo 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 del centro de asistencia técnica.

- Portal de autoservicio: en iDRAC7 hay un vínculo disponible al portal de autoservicio. haga clic en él para abrir la sección de licencias en Internet desde la que podrá comprar licencias. Para obtener más información, consulte la ayuda en línea de la página del portal de autoservicio.
- Punto de venta: la licencia se adquiere al realizar un pedido de un sistema.


Operaciones de licencia

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


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

Puede realizar las siguientes operaciones de licencia mediante iDRAC7, 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 iDRAC7 mediante una de las interfaces admitidas. La licencia se importa si supera todas las comprobaciones de validación.

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

- Exportar: exporte la licencia instalada en un dispositivo de almacenamiento externo como copia de seguridad o para reinstalarla después de reemplazar la placa base parcial o completamente. El nombre de archivo y el formato de la licencia exportada es `<EntitlementID>.xml`.
- Eliminar: elimine la licencia asignada a un componente cuando este no esté presente. Una vez eliminada la licencia, esta no se almacena en iDRAC7 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 la *Dell License Manager User's Guide* (Guía del usuario de Dell License Manager) disponible en support.dell.com/manuals.

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

Administración de licencias mediante la interfaz web de iDRAC7

Para administrar licencias mediante la interfaz web de iDRAC7, vaya a **Información general Licencias de servidor**.

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 iDRAC7*.

Administración de licencias mediante RACADM

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

Consulte también:

- Administración de licencias
- Tipos de licencias
- Adquisición de licencias
- Funciones con licencia en iDRAC7

Funciones con licencia en iDRAC7

En la tabla siguiente se proporcionan las funciones de iDRAC7 activadas según la licencia adquirida.

Tabla 2. Funciones con licencia de iDRAC7

Característica	Administración básica con IPMI	iDRAC7 Express	iDRAC7 Express para servidores Blade	iDRAC7 Enterprise
Compatibilidad con interfaces y estándares				
IPMI 2.0	Sí	Sí	Sí	Sí
Interfaz basada en web [1]	No	Sí	Sí	Sí
SNMP	No	Sí	Sí	Sí
WS-MAN	Sí	Sí	Sí	Sí
SCHEMA-CLIP (SSH)	No	Sí	Sí	Sí

Característica	Administración básica con IPMI	iDRAC7 Express	iDRAC7 Express para servidores Blade	iDRAC7 Enterprise
RACADM (SSH, local y remoto) [1]	No	Sí	Sí	Sí
Telnet	No	Sí	Sí	Sí
Conectividad				
Modos de red compartida y protección contra fallas (solo servidores tipo bastidor y torre)	Sí	Sí	No	Sí
NIC dedicado	No	No	Sí [2]	Sí [2,6]
DNS	Sí	Sí	Sí	Sí
VLAN Settings (Etiquetado VLAN)	Sí	Sí	Sí	Sí
IPv4	Sí	Sí	Sí	Sí
IPv6	No	Sí	Sí	Sí
DNS dinámico	No	Sí	Sí	Sí
Seguridad y autenticación				
Autoridad basada en roles	Sí	Sí	Sí	Sí
Local Uses	Sí	Sí	Sí	Sí
Servicios de directorio (Active Directory y LDAP genérico)	No	No	No	Sí
Cifrado SSL	Sí	Sí	Sí	Sí
Autenticación de factor doble [3]	No	No	No	Sí
Inicio de sesión único (SSO)	No	No	No	Sí
Autenticación de PE (para SSH)	No	No	No	Sí
Bloqueo de seguridad	No	Sí	Sí	Sí
Corrección y administración remota				
Diagnóstico incorporado	Sí	Sí	Sí	Sí
Comunicación en serie en la LAN (con proxy)	Sí	Sí	Sí	Sí
Comunicación en serie en la LAN (sin proxy)	No	Sí	Sí	Sí
Captura de pantalla de bloqueo	No	Sí	Sí	Sí
Captura de video de bloqueo	No	No	No	Sí
Captura de inicio	No	No	No	Sí
Medios virtuales [4]	No	No	Sí	Sí
Consola virtual [4]	No	No	Sí [5]	Sí
Colaboración de consola [4]	No	No	No	Sí

Característica	Administración básica con IPMI	iDRAC7 Express	iDRAC7 Express para servidores Blade	iDRAC7 Enterprise
Carpeta virtual	No	No	No	Sí
Chat de consola virtual	No	No	No	Sí
Recurso compartido de archivos remotos	No	No	No	Sí
vFlash [6]	No	No	No	Sí
Particiones vFlash [6]	No-	No	No	Sí
Descubrimiento automático	No	Sí	Sí	Sí
Supervisión y alimentación				
Alerta y supervisión de sensor	Sí	Sí	Sí	Sí
Supervisión de dispositivos	No	Sí	Sí	Sí
Supervisión de almacenamiento	No	Sí	Sí	Sí
Alertas por correo electrónico	No-	Sí	Sí	Sí
Contadores de datos históricos de alimentación	Sí	Sí	Sí	Sí
Límites de alimentación	No	No	No	Sí
Supervisión de alimentación en tiempo real	Sí	Sí	Sí	Sí
Gráficos de alimentación en tiempo real	No	Sí	Sí	Sí
Registro				
Registro de sucesos del sistema	Sí	Sí	Sí	Sí
Registro del RAC [7]	No	Sí	Sí	Sí
Registro de rastreo [7]	No	Sí	Sí	Sí
Registro del sistema remoto	No	No	No	Sí

[1] La funcionalidad de administración y actualización del firmware de licencias de iDRAC7 siempre está disponible a través de la interfaz web de iDRAC7 y RACADM.

[2] Todos los servidores Blade utilizan una NIC dedicada para iDRAC7 en todo momento, pero la velocidad está limitada a 100 Bps. Una tarjeta GIGABIT Ethernet no funciona en servidores Blade debido a las limitaciones del chasis, pero sí funciona en servidores tipo bastidor y torre con licencia Enterprise. La LOM no está activada para servidores Blade.

[3] La autenticación de factor doble está disponible a través de Active-X y, por tanto, solo admite Internet Explorer.

[4] La consola virtual y los medios virtuales están disponibles a través de los complementos tanto de Java como de Active-X.

[5] Consola virtual de usuario único con lanzamiento remoto.

[6] En algunos sistemas la tarjeta de puerto iDRAC7 opcional es obligatoria.

[7] Los registros de RAC y de seguimiento están disponibles en la versión base a través de WS-MAN.

Interfaces y protocolos para acceder a iDRAC7

En la tabla siguiente se enumeran las interfaces para acceder a iDRAC7.




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

Tabla 3. Interfaces y protocolos para acceder a iDRAC7

Interfaz o protocolo	Descripción
Utilidad de configuración de iDRAC	<p>Utilice la utilidad de configuración de iDRAC para realizar operaciones previas al sistema operativo. Esta cuenta con un conjunto de funciones disponibles en la interfaz web de iDRAC7, además de otras funciones.</p> <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>
Interfaz web de iDRAC7	<p>Utilice la interfaz web de iDRAC7 para administrar iDRAC7 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>Utilice esta utilidad de línea de comandos para realizar la administración de iDRAC7 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 iDRAC7 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. • RACADM remoto es una utilidad cliente que se ejecuta en una estación de trabajo. Utilice la interfaz de red fuera de banda para ejecutar los comandos RACADM en los sistemas administrados y utiliza el canal HTTPS. La opción <code>-r</code> ejecuta el comando RACADM sobre una red. • El RACADM de firmware no es accesible al iniciar sesión en iDRAC7 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 iDRAC7. • No debe especificar la dirección IP, el nombre de usuario o la contraseña de iDRAC7 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 <code>racadm</code>.
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 iDRAC7, las cadenas programables del usuario • Configurar DHCP • Configurar la dirección IP de iDRAC7 <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 de 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

Interfaz o protocolo	Descripción
	<ul style="list-style-type: none"> • Actualizar el firmware de iDRAC7 • Establecer la configuración de red de iDRAC7 • Iniciar sesión en la interfaz web de iDRAC7 • Iniciar, detener o restablecer el sistema administrado • Actualizar el BIOS, PERC y otros adaptadores de red compatibles
Lifecycle Controller	<p>Utilice Lifecycle Controller para realizar las configuraciones de iDRAC7. Para acceder a Lifecycle Controller, presione <F10> durante el inicio y vaya a Configuración del sistema → Configuración de hardware avanzada → Configuración de iDRAC. Para obtener más información, consulte la <i>Lifecycle Controller User's Guide</i> (Guía del usuario de servicios remotos de Dell Lifecycle Controller) disponible en support.dell.com/manuals.</p>
Telnet	<p>Utilice Telnet para acceder a iDRAC7 donde puede ejecutar comandos RACADM y SMCLP. Para obtener información detallada acerca de RACADM, consulte la <i>RACADM Command Line Reference Guide for iDRAC7 and CMC</i> (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC) disponible en support.dell.com/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 iDRAC7, el servicio SSH está activado de manera predeterminada pero se puede desactivar. iDRAC7 solo admite SSH versión 2 con DSA y el algoritmo de clave de host RSA. Al iniciar iDRAC7 por primera vez, se genera una clave de host DSA y RDA de 1024.</p>
IPMITool	<p>Utilice IPMITool para acceder a las funciones de administración básicas del sistema remoto a través de iDRAC7. 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 la <i>Dell OpenManage Baseboard Management Controller Utilities User's Guide</i> (Guía del usuario de Dell OpenManage Baseboard Management Controller Utilities) disponible en support.dell.com/manuals.</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> <p>Web Services for Management (WS-Management) es un protocolo basado en SOAP que se utiliza para la administración de sistemas. iDRAC7 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 iDRAC7 asignada a los perfiles DMTF y de extensión.</p> <p>Para obtener más información, consulte lo siguiente:</p>

Interfaz o protocolo	Descripción
	<ul style="list-style-type: none"> • Lifecycle Controller-Remote Services User's Guide (Guía del usuario de servicios remotos de Dell Lifecycle Controller) disponible en support.dell.com/manuals. • Lifecycle Controller Integration Best Practices Guide (Guía de prácticas recomendadas para la integración de Lifecycle Controller) disponible en support.dell.com/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 DTMF: dmtf.org/standards/profiles/

Información de puertos iDRAC7

Se requieren los siguientes puertos de información para acceder a iDRAC7 de forma remota a través de servidores de seguridad. Se trata de los puertos iDRAC7 que detectan las conexiones.

Tabla 4. Puertos para los que iDRAC7 detecta las conexiones

Número de puerto	Función
22*	SSH
23*	Telnet
80*	HTTP
443*	HTTPS
623	RMCP/RMCP+
5900*	Teclado y redireccionamiento del mouse de la consola virtual, Medios virtuales, Carpetas virtuales y Uso compartido de archivos remotos

* Puerto configurable

En la tabla siguiente se enumeran los puertos que iDRAC7 utiliza como cliente.

Tabla 5. Puertos que iDRAC7 utiliza como cliente

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

Otros documentos que podrían ser de utilidad

Además de esta guía, los siguientes documentos están disponibles en el sitio web de Dell Support en support.dell.com/manuals y proporcionan información adicional acerca de la configuración y el funcionamiento de iDRAC7 en el sistema. En la página **Manuals** (Manuales), haga clic en **Software** → **Systems Management** (Administración de sistemas). Haga clic en el vínculo del producto correspondiente a la derecha para acceder a los documentos.


- En la *Ayuda en línea de iDRAC7* se proporciona información acerca de los campos disponibles en la interfaz web de iDRAC7 y las descripciones de los mismos. Puede acceder a la ayuda en línea después de instalar iDRAC7.
- En la *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC7 y CMC) se proporciona información acerca de los subcomandos de RACADM, las interfaces admitidas y los grupos de bases de datos de propiedades y las definiciones de objetos de iDRAC7.
- 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 la *Dell Lifecycle Controller User's Guide and Remote Services Ser Guide* (Guía del usuario de Dell Lifecycle Controller y la Guía del usuario de servicios remotos) se proporciona información acerca del uso de Lifecycle Controller y los servicios remotos, respectivamente.
- En la *Dell Remote Access Configurarlos Too User's Guide* (Guía del usuario de la herramienta de configuración de Dell Remote Access) se proporciona información sobre cómo utilizar la herramienta para descubrir las direcciones IP de iDRAC en la red y realizar actualizaciones de firmware de uno a varios y activar las configuraciones de directorio para las direcciones IP descubiertas.
- En la *Matriz de compatibilidad de software de sistemas Dell* se 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.
- 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 usuario de las utilidades de administración de OpenManage Baseboard Management Controller) se incluye información acerca de la interfaz IPMI.
- Es posible que se incluyan archivos Léame para proporcionar actualizaciones de última hora relativas al sistema o a la documentación, o material avanzado de consulta técnica destinado a técnicos o usuarios experimentados.
- En el *glosario* se proporciona información acerca de los términos utilizados en este documento.

Están disponibles los siguientes documentos para proporcionar más información:

- En la *iDRAC7 Overview and Feature Guide* (Guía de descripción general y funciones de iDRAC7) se incluye información acerca de iDRAC7, sus funciones con 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 las funciones del sistema.

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 **support.dell.com**.
2. Seleccione la categoría de soporte.
3. Si no es cliente de EE.UU., seleccione su código de país en la parte inferior de la página **support.dell.com** o seleccione **All** (Todos) para ver más opciones.
4. Seleccione el enlace de servicio o asistencia apropiado en función de sus necesidades.

Inicio de sesión en iDRAC7

Puede iniciar sesión en iDRAC7 como usuario de iDRAC7, como usuario de Microsoft Active Directory o como usuario LDAP. El nombre de usuario predeterminado y la contraseña correspondiente son root y calvin, respectivamente. También puede iniciar sesión mediante SSO o tarjeta inteligente.

 **NOTA:** Debe disponer del privilegio Iniciar sesión en iDRAC para poder iniciar sesión en iDRAC7.

Enlaces relacionados


[Inicio de sesión en iDRAC7 como usuario local de Active Directory o usuario LDAP](#)


[Inicio de sesión en el iDRAC7 mediante una tarjeta inteligente](#)

[Inicio de sesión en iDRAC7 mediante inicio de sesión único](#)

Inicio de sesión en iDRAC7 como usuario local de Active Directory o usuario LDAP


Antes de iniciar sesión en iDRAC7 mediante la interfaz web, asegúrese de haber configurado un explorador web compatible (Internet Explorer o Firefox) y que la cuenta de usuario se ha creado 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 openLDAP, openDS, Novell eDir y Fedora. Los caracteres "<" y ">" no se permiten en el nombre de usuario.

Para iniciar sesión en iDRAC7 como usuario local de Active Directory o usuario LDAP

1. Abra un explorador de web compatible.
2. En el campo **Dirección**, escriba `https://<dirección-IP-de-iDRAC7>` y presione **Intro**.

 **NOTA:** Si se ha cambiado el número de puerto HTTPS predeterminado (puerto 443), introduzca: `https://[dirección-IP-de-iDRAC7]:[número-puerto]` donde, `[dirección-IP-de-iDRAC7]` es la dirección IPv4 o IPv6 de iDRAC7 y `[número-puerto]` 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 iDRAC7.
 - 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**. Habrá iniciado sesión en iDRAC7 con los privilegios de usuario necesarios.

Enlaces relacionados

[Configuración de cuentas de usuario y privilegios](#)

[Configuración de exploradores web compatibles](#)

Inicio de sesión en el iDRAC7 mediante una tarjeta inteligente

Puede iniciar sesión en iDRAC7 mediante una tarjeta inteligente. Las tarjetas inteligentes proporciona una autenticación de factor doble (TFA) y ofrecen dos niveles de seguridad:

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

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

Enlaces relacionados

[Inicio de sesión en iDRAC7 como usuario local mediante una tarjeta inteligente](#)


[Inicio de sesión en iDRAC7 como usuario de Active Directory mediante una tarjeta inteligente](#)

Inicio de sesión en iDRAC7 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 iDRAC7
- Activar el inicio de sesión mediante tarjeta inteligente.


La interfaz web de iDRAC7 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 iDRAC7 como usuario local mediante una tarjeta inteligente:

1. Acceda a la interfaz web de iDRAC7 mediante el vínculo `https://[dirección IP]`.

Aparece la página **Inicio de sesión de iDRAC7** en la que se le solicita que inserte la tarjeta inteligente.


 **NOTA:** Si el número de puerto HTTPS predeterminado (puerto 443) se ha modificado, escriba: `https://[dirección IP]:[número de puerto]` donde, `[dirección IP]` es la dirección IP de DRAC7 y `[número de puerto]` 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 al iDRAC7.

 **NOTA:** Si es un usuario local para el que está activada la opción **Activar la revisión CRL para el inicio de sesión mediante tarjeta inteligente**, iDRAC7 intenta descargar la CRL y comprueba esta en búsqueda del certificado del usuario. El inicio de sesión falla si el certificado se indica como revocado en la CRL o si esta última no se puede descargar por el motivo que sea.

Enlaces relacionados

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

[Configuración del inicio de sesión mediante tarjeta inteligente de iDRAC7 para usuarios locales](#)

Inicio de sesión en iDRAC7 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 iDRAC7.
- Configurar el servidor DNS.
- Activar el inicio de sesión de Active Directory.
- Activar el inicio de sesión mediante tarjeta inteligente.

Para iniciar sesión en iDRAC7 como usuario de Active Directory mediante una tarjeta inteligente:

1. Inicie sesión en iDRAC7 mediante el enlace `https://[dirección IP]`.

Aparece la página **Inicio de sesión de iDRAC7** en la que se le solicita que inserte la tarjeta inteligente.

 **NOTA:** Si el número de puerto HTTPS predeterminado (puerto 443) se ha modificado, escriba: `https://[dirección IP]:[número de puerto]` donde, `[dirección IP]` es la dirección IP de DRAC7 y `[número de puerto]` 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**.

Habrá iniciado sesión en iDRAC7 mediante las 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 iDRAC7 para usuarios de Active Directory](#)

Inicio de sesión en iDRAC7 mediante inicio de sesión único

Cuando está activado el inicio de sesión único (SSO), puede iniciar sesión en iDRAC7 sin introducir las credenciales de autenticación de usuario del dominio, tal como el nombre de usuario y la contraseña.

Enlaces relacionados

[Configuración del inicio de sesión SSO de iDRAC7 para usuarios de Active Directory](#)


Inicio de sesión SSO de iDRAC7 mediante la interfaz web de iDRAC7


Antes de iniciar sesión en iDRAC7 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 iDRAC7 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://[dirección FQDN]`

 **NOTA:** Si el número de puerto HTTPS predeterminado (puerto 443) se ha modificado, escriba: `https://[dirección FQDN]:[número de puerto]` donde, `[dirección FQDN]` es el nombre FQDN de iDRAC7 (`iDRAC7dnsname.domain.`) y `[número de puerto]` es el número de puerto HTTPS.

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

iDRAC7 le inicia sesión con los privilegios adecuados de Microsoft Active Directory, utilizando las credenciales almacenadas en caché del sistema operativo en el momento de iniciar sesión mediante una cuenta de Active Directory válida.

Inicio de sesión SSO de iDRAC7 mediante la interfaz web de iDRAC7

Mediante la función SSO, puede iniciar la interfaz web de iDRAC7 desde la interfaz web de CMC. Un usuario de CMC tiene los privilegios de usuario de CMC al iniciar iDRAC7 desde CMC. Si la cuenta de usuario está presente en CMC y no en iDRAC, el usuario aún puede iniciar iDRAC7 desde CMC.

Si se desactiva la LAN de la red de iDRAC7 (LAN activada = No), SSO no estará disponible.

Si el servidor se quita del chasis, se cambia la dirección IP de iDRAC7 o hay un problema en la conexión de red, la opción para iniciar iDRAC7 estará desactivada en la interfaz web de CMC.


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

Acceso a iDRAC7 mediante RACADM remoto

Puede utilizar RACADM para acceder a iDRAC7 mediante la utilidad e configuración de RACADM.

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

Si la estación de trabajo no almacena el certificado SSL de iDRAC7 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 iDRAC7 es el que iDRAC7 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, RHEL5 64bits, 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: - cat testcacert.pem >> cert.pem`
4. Genere y cargue el certificado de servidor en iDRAC7.

Acceso a iDRAC7 mediante RACADM local

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

Acceso a iDRAC7 mediante RACADM de firmware

Puede utilizar las interfaces SSH o Telnet para acceder a iDRAC7 y ejecutar comandos RACADM. Para obtener más información, consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC) disponible en support.dell.com/manuals.

Acceso a iDRAC7 mediante SMCLP

SMCLP es el símbolo del sistema de línea de comandos predeterminado cuando inicia sesión en iDRAC7 mediante Telnet o SSH. Para obtener más información, consulte [Uso de SMCLP](#).

Inicio de sesión en iDRAC7 mediante la autenticación de clave pública

Puede iniciar sesión en iDRAC7 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:

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

```
o
```

```
SSO nombre de usuario@<dirección_IP_entrante>
```

donde `IP_address` es la dirección IP de iDRAC7.

Envío de comandos RACADM:

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

```
SSO nombre de usuario@<dominio> racadm getsensorinfo
```

Enlaces relacionados

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

Varias sesiones iDRAC7


En la tabla siguiente se proporciona la lista de varias sesiones iDRAC7 posibles mediante las distintas interfaces.

Tabla 6. Varias sesiones iDRAC7

Interfaz	Número de sesiones
Interfaz web de iDRAC7	4
RACADM remoto	4
Firmware RACADM / SMCLP	SSH - 2 Telnet - 2 Serie - 1

Configuración de Managed System y Management Station

Para realizar administración de sistemas fuera de banda mediante iDRAC7, debe configurar iDRAC7 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.


Enlaces relacionados

- [Configuración de la dirección IP de iDRAC7](#)
- [Configuración de Managed System](#)
- [Actualización del firmware de iDRAC7](#)
- [Reversión del firmware de iDRAC7](#)
- [Configuración de Management Station](#)
- [Configuración de exploradores web compatibles](#)

Configuración de la dirección IP de iDRAC7

Debe configurar los valores de red iniciales en función de la infraestructura de red para activar la comunicación entrante y saliente con iDRAC7. Puede configurar la dirección IP mediante una de las interfaces siguientes:

- 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 servidores Blade, puede configurar los valores de red mediante el panel LCD de chasis solo durante la configuración inicial de CMC. Una vez implementado el chasis, no es posible reconfigurar iDRAC7 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 servidores tipo bastidor y torre, puede configurar la dirección IP o utilizar la dirección IP predeterminada de iDRAC7 (192.168.0.120) para configurar los valores de red iniciales, incluida la configuración de DHCP o la dirección IP estática para iDRAC7.

En el caso de servidores Blade, la interfaz de red iDRAC7 está desactivada de manera predeterminada.

Después de configurar la dirección IP de iDRAC7:

- Asegúrese de *cambiar el nombre de usuario y la contraseña predeterminados después de configurar la dirección IP de iDRAC7.*
- Obtenga acceso a ella a través de cualquiera de las interfaces siguientes:
 - Interfaz web de iDRAC7 mediante un explorador compatible (Internet Explorer o Firefox).

- 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 está 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 support.dell.com).

Enlaces relacionados

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

[Configuración de la IP de iDRAC7 mediante la interfaz web de CMC](#)

[Activación del descubrimiento automático](#)

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

Para configurar la dirección IP de iDRAC7:

1. Encienda el sistema administrado.
2. Presione <F2> durante POST (autoprueba de encendido).
3. En la página **Menú principal de Configuración del sistema**, haga clic en **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
 - Valores comunes
 - Configuración de IPv4
 - Configuración de IPv6
 - Configuración de IPMI
 - Configuración de VLAN
6. Vuelva a la página **Menú principal de Configuración del sistema** y haga clic en **Terminar**. Se guarda la información de red y el sistema se reinicia.

Enlaces relacionados

[Configuración de red](#)

[Valores comunes](#)

[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 los sistemas tipo bastidor o torre con una licencia iDRAC7 Enterprise. Para servidores Blade, está disponible de manera predeterminada.

- 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 utiliza LOM para la comunicación iDRAC7.


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, la ruta al tráfico de red de iDRAC7 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. Bajo **Negociación automática**, seleccione **Activado** si iDRAC7 debe configurar automáticamente el modo dúplex y la velocidad de la red. Esta opción está disponible solamente para el modo dedicado. Si está activada, iDRAC7 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.

Valores comunes

Si la infraestructura de red tiene un servidor DNS, registre iDRAC7 en él. Estos son los requisitos de configuración inicial para las funciones avanzadas, tal como servicios de directorio: Active Directory o LDAP, Inicio de sesión único y tarjeta inteligente.

Para configurar registrar iDRAC7:

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** bajo **Activar IPv4**.
2. Seleccione **Activado** bajo **Activar DHCP** de modo que DHCP pueda asignar la automáticamente la dirección IP, la puerta de enlace y la máscara de subred a iDRAC7. De lo contrario, seleccione **Desactivado** e introduzca valores para las opciones siguientes:
 - Dirección IP
 - Puerta de enlace
 - Máscara de subred
3. De manera opcional, active **Usar DHCP para obtener direcciones de servidor DNS**, de modo que el servidor DHCP pueda asignar los valores de **Servidor DNS preferido** y **Servidor DNS alternativo**. De lo contrario, introduzca las direcciones IP en los cuadros **Servidor DNS preferido** y **Servidor DNS alternativo**.

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** bajo **Activar IPv6**.
2. Para que el servidor DHCPv6 asigne automáticamente la dirección IP, la puerta de enlace y la máscara de subred a iDRAC7, seleccione la opción **Activado** bajo **Activar autoconfiguración**. Si se activa, los valores estáticos se desactivan. De lo contrario, vaya al paso siguiente para realizar la configuración utilizando la dirección IP estática.
3. En el cuadro **Dirección IP 1**, introduzca la dirección IPv6 estática.
4. En el cuadro **Longitud de prefijo**, introduzca un valor entre 0 y 128.
5. En el cuadro **Puerta de enlace**, introduzca la dirección de la puerta de enlace.
6. Si utiliza DHCP, active la opción **DHCPv6 para obtener direcciones de servidor DNS** para obtener las direcciones de servidor DNS primaria y secundaria del servidor DHCPv6.
7. De manera opcional, active **Usar DHCP para obtener direcciones de servidor DNS**, de modo que el servidor DHCPv6 pueda asignar los valores de **Servidor DNS preferido** y **Servidor DNS alternativo**. De lo contrario, introduzca las direcciones IP en los cuadros **Servidor DNS preferido** y **Servidor DNS alternativo**. De lo contrario:
 - En el cuadro **Servidor DNS preferido**, introduzca la dirección IPv6 del servidor DNS.
 - En el cuadro **Servidor DNS alternativo**, 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 iDRAC7 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.

Configuración de la IP de iDRAC7 mediante la interfaz web de CMC

Para configurar la dirección IP de iDRAC7 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 iDRAC7 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 la *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
 - Valores comunes
 - Configuración de IPv4
 - Configuración de IPv6
 - Configuración de IPMI
 - Configuración de VLAN

 **NOTA:** Para obtener más información, consulte la Ayuda en línea de iDRAC7.

7. Para guardar la información de red, haga clic en **Aplicar**.
Para obtener más información, consulte la *Chassis Management Controller User's Guide* (Guía del usuario de Chassis Management Controller) disponible en support.dell.com/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 iDRAC7, de modo que pueda ser descubierto desde la consola de administración. Para obtener más información acerca del descubrimiento automático, consulte la *Lifecycle Controller Remote Services User's Guide* (Guía del usuario de servicios remotos de Dell Lifecycle Controller) disponible en support.dell.com/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.

Si la función de descubrimiento automático no se activa en el sistema enviado de fábrica, estará activada la cuenta de administrador predeterminada (root como nombre de usuario y calvin como contraseña). Antes de activar el descubrimiento automático, asegúrese de desactivar esta cuenta de administrador.

Puede activar el descubrimiento automático mediante la utilidad de configuración de iDRAC7 o Lifecycle Controller. Para obtener más información, consulte la *Dell Lifecycle Controller Remote Services User's Guide* (Guía del usuario de servicios remotos de Dell Lifecycle Controller) disponible en support.dell.com/manuals.

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 Management Station

Una estación de administración es un equipo que se utiliza para acceder a las interfaces de iDRAC7 para supervisar y administrar los 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 o Firefox).
3. Instale el Java Runtime Environment (JRE) más reciente (obligatorio si el tipo de complemento Java se utiliza para acceder a iDRAC7 mediante un explorador web).
4. Desde el *DVD de herramientas y documentación de Dell Systems Management*, instale RACADM remoto y VMCLI desde la carpeta SYSMGMT. De lo contrario, 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 la *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC) disponible en support.dell.com/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 iDRAC7 de manera remota

Para acceder a la interfaz web de iDRAC7 de manera remota desde una estación de administración, asegúrese de que esta última se encuentre en la misma red que iDRAC7. 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 la *Guía del usuario de Chassis Management Controller* disponible en support.dell.com/manuals.
- Servidores tipo bastidor y torre: establezca la NIC de iDRAC7 en LOM1 y asegúrese de que la estación de administración resida en la misma red que iDRAC7.

 **NOTA:** Si el sistema se actualiza a iDRAC7 Enterprise, puede establecer la NIC de iDRAC7 en **Dedicado**.

Para acceder a la consola del sistema administrado desde una estación de administración, utilice la consola virtual a través de la interfaz web de iDRAC7.

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 la *Guía del usuario de Server Administrator de Dell OpenManage* disponible en support.dell.com/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 iDRAC7, 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**, **Privilegios de usuario en la LAN**, **Privilegios 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 iDRAC7 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 iDRAC7, 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 iDRAC7*.
3. Haga clic en **Aplicar**. Los detalles de la ubicación del sistema se guardan en iDRAC7.

Configuración de la ubicación de Managed System mediante RACADM

Para especificar los detalles de utilización del sistema, utilice los objetos de grupo `System.Location`. Para obtener más información, consulte la *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC) disponible en support.dell.com/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

Puede optimizar el rendimiento, establecer la temperatura máxima de expulsión de aire y definir la velocidad del ventilador del sistema administrado mediante la utilidad de configuración de iDRAC. Para ello:

1. En la utilidad de configuración de iDRAC, vaya a **Térmico**. Aparece la pantalla **Térmico de la configuración de iDRAC**.
2. Especifique el térmico, la opción de usuario y la configuración del ventilador. Para obtener información, consulte la *Ayuda en línea de la utilidad de configuración iDRAC*.
3. Haga clic en **Atrás**, en **Terminar** y, a continuación, en **Sí**. Se habrán configurado los valores térmicos.

Configuración de exploradores web compatibles

Si se conecta a la interfaz web de iDRAC7 desde una estación de administración que se conecta a Internet mediante un servidor proxy, debe configurar el explorador web para que acceda a Internet desde este servidor.

Para configurar el explorador web Internet Explorer:

1. En el explorador web, vaya a **Herramientas** → **Opciones de Internet** → **Seguridad** → **Red local**.
2. 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.
3. 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

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

5. 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

Bajo Seguridad:

- Comprobar si se revocó el certificado del editor: desactivado
- Comprobar si existen firmas en los programas descargados: 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 iDRAC7 no funcione correctamente.

6. Haga clic en **Aplicar** y, después, en **Aceptar**.
7. Haga clic en la ficha **Conexiones**.
8. En **Configuración de red de área local (LAN)**, haga clic en **Configuración de LAN**.
9. Si la casilla **Usar servidor proxy** está seleccionada, seleccione la casilla **No usar servidor proxy para direcciones locales**.
10. Haga clic dos veces en **Aceptar**.
11. Cierre y reinicie el explorador para asegurarse de que todos los cambios tengan efecto.

Enlaces relacionados

[Visualización de las versiones traducidas de la interfaz web](#)


[Adición de iDRAC7 a la lista de dominios de confianza](#)

[Desactivación de la función de lista blanca en Firefox](#)

Adición de iDRAC7 a la lista de dominios de confianza

Cuando accede a la interfaz web de iDRAC7, se le solicitará que agregue la dirección IP de iDRAC7 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 iDRAC7.

Es posible que en algunos sistemas operativos, Internet Explorer (IE) 8 no le solicite que agregue la dirección IP de iDRAC7 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 iDRAC7 con un certificado en el que el explorador no confía, es posible que el aviso de error de certificado del explorador se muestre una segunda vez tras confirmar el primer aviso. Este comportamiento es esperado por motivos de seguridad.

Para agregar la dirección IP de iDRAC7 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 iDRAC7 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 para 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 iDRAC7 que visite, 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 iDRAC7 se admite en los idiomas siguientes:

- 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 iDRAC7 está diseñada para funcionar con teclados localizados para las variantes de idioma admitidas. Algunas funciones de la interfaz web de iDRAC7, tal 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 iDRAC7.

Actualización del firmware de iDRAC7

Puede actualizar el firmware mediante cualquiera de los métodos siguientes:

- Interfaz web de iDRAC7
- CLI de RACADM (iDRAC7 y CMC)
- Dell Update Package (DUP)
- Interfaz web de CMC
- Lifecycle Controller–Remote Services

- Lifecycle Controller

Durante la actualización del firmware:

- Una vez completada la actualización del firmware, iDRAC7 se restablecerá. Este proceso desconecta todas las conexiones y sesiones.
- Los ventiladores de los servidores tipo bastidor y torre protegen a los sistemas contra el sobrecalentamiento. Una vez completada la actualización, se reanuda el control normal de la velocidad de los ventiladores.
- iDRAC7 genera claves SHA1 y MD5 nuevas para el certificado SSL si la configuración no se conserva.



NOTA: Cierre todas las ventanas de explorador conectadas a iDRAC7 una vez completada la actualización del firmware. De lo contrario, se mostrará un mensaje de error de certificado no válido, ya que las claves serán distintas de las de la sesión de explorador antes de la actualización.

- Si se produce una interrupción por el motivo que sea, la función de activación del firmware quedará desactivada durante hasta 30 minutos.

Enlaces relacionados

[Descarga del firmware de iDRAC7](#)

[Actualización del firmware mediante la interfaz web de iDRAC7](#)

[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 iDRAC7

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

- Interfaz web de iDRAC7: descargue la 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 iDRAC7 mediante la interfaz web de CMC.

- Managed System: descargue el 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 la plataforma* en Lifecycle Controller para actualizar el iDRAC7. Para obtener más información acerca de la actualización de la plataforma, consulte la *Lifecycle Controller User's Guide* (Guía del usuario de Lifecycle Controller) disponible en support.dell.com/manuals.


Actualización del firmware mediante la interfaz web de iDRAC7

Para actualizar la interfaz web de iDRAC7:


1. Descargue la imagen más reciente del firmware de iDRAC7.
2. En la interfaz web de iDRAC7, vaya a **Información general** → **Configuración de iDRAC** → **Actualización del firmware de iDRAC**.
Se muestra la ventana **Actualización del firmware**.
3. En **Ruta de acceso de archivo**, haga clic en **Examinar** para seleccionar la imagen de firmware que se descarga y, a continuación, haga clic en **Cargar**.
Se muestra la página **Estado (paso 2 de 3)**. Una vez completada la carga, se muestran las versiones actuales y nuevas del firmware.

Si la imagen no carga y supera todas las comprobaciones de verificación, se muestra un mensaje de error y la actualización vuelve a la página Actualización de firmware. No obstante, puede reintentar actualizar iDRAC7 o hacer clic en **Cancelar** para restablecer iDRAC7 al modo de funcionamiento normal.

Durante la actualización del firmware, si la imagen no se carga debido a problemas de la red, seguirá mostrando que la actualización del firmware está en curso. Después de 30 minutos, vuelve a la página **Actualización de firmware**.

 **NOTA:** Durante estos 30 minutos, no puede realizar ninguna operación de actualización de firmware.

4. De manera predeterminada, la opción **Conservar configuración** está seleccionada y se guarda la configuración de iDRAC7 existente después de la actualización de firmware. Si se desactiva esta opción, todas las configuraciones de iDRAC7 se restablecen a sus valores predeterminados.

 **NOTA:** Si la configuración de iDRAC7 se restablece a los valores predeterminados, la dirección IP de iDRAC7 se restablece en 192.168.0.120. Puede acceder a iDRAC7 mediante esta IP o volver a configurar la dirección IP de iDRAC7 utilizando el RACADM local, el panel frontal (LCD) o la tecla F2 (RACADM remoto requiere acceso de red).

Para guardar la configuración actual, utilice RACADM local o RACADM remoto para exportar la configuración de iDRAC7 a un archivo y volver a importarla en iDRAC7 después de que el firmware se haya actualizado y las configuraciones se hayan restablecido a sus valores predeterminados. Esto no es necesario si conserva la configuración durante la actualización de firmware.

Para exportar la configuración de iDRAC7 de iDRAC7 a un archivo mediante la interfaz de RACADM:


- El comando de RACADM local es: `racadm getconfig -f iDRAC-config.txt`
- El comando RACADM remoto es: `racadm -r <dirección IP de iDRAC> -u <nombre de usuario de idrac> -p <contraseña> getconfig -f iDRAC-config.txt`, donde **iDRAC-config.txt** es el archivo que tiene la configuración.

Para importar la configuración de iDRAC desde el archivo a iDRAC7 a través de RACADM:

- El comando RACADM local es: `racadm config -f iDRAC-config.txt`
- El comando RACADM remoto es: `racadm -r <dirección IP de iDRAC> -u <nombre de usuario de idrac> -p <contraseña> config -f iDRAC-config.txt`, donde **iDRAC-config.txt** es el archivo que tiene la configuración.

5. Haga clic en **Siguiente**.

Se muestra la página **Actualización (paso 3 o 3)** y el progreso de la actualización (en porcentaje) en la columna **Progreso**.

 **NOTA:** Mientras se encuentra en modo actualización, el proceso de actualización sigue en segundo plano incluso si se aleja de esta página.

6. Una vez completada la actualización, para utilizar iDRAC7, utilice la ventana del explorador actual y vuelva a conectarse mediante una nueva ventana de explorador.
7. Para ver la versión de firmware de iDRAC7 en cualquiera de las páginas siguientes:
 - Vaya a **Información general** → **Servidor** → **Propiedades** → **Resumen** y consulte la versión de firmware bajo la sección **Información del servidor**.
 - Vaya a **Información general** → **Configuración de iDRAC** → **Propiedades** y consulte la versión de firmware bajo la sección **Integrated Dell Remote Access Controller 7**.

Enlaces relacionados

[Actualización del firmware de iDRAC7](#)

[Descarga del firmware de iDRAC7](#)

Actualización del firmware mediante la interfaz web de CMC

Puede actualizar el firmware de iDRAC7 para servidores Blade mediante la interfaz web de CMC.

Para actualizar el firmware de iDRAC7 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** para iniciar la interfaz web y seleccione **Actualización del firmware de iDRAC**.

Enlaces relacionados

[Actualización del firmware de iDRAC7](#)


[Descarga del firmware de iDRAC7](#)

[Actualización del firmware mediante la interfaz web de iDRAC7](#)

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 actualice el firmware de iDRAC7 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 iDRAC7 mediante DUP:

1. Descargue el DUP en función del sistema operativo y ejecútelo 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:

```
racadm -r <dirección IP de iDRAC7> -u <nombre de usuario> -p <contraseña>  
fwupdate -g -u -a <ruta de acceso>
```

donde *ruta de acceso* es la ubicación en el servidor TFTP en la que está almacenado **firmimg.d7**.

Servidor FTP:

```
racadm -r <dirección IP de iDRAC7> -u <nombredeusuario> -p <contraseña>  
fwupdate -f <dirección IP del servidor FTPIP> <nombre de usuario del  
servidor FTP> <contraseña del servidor FTP> -d <ruta de acceso>
```

donde *ruta de acceso* es la ubicación en el servidor FTP en la que está almacenado **firmimg.d7**.

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

Actualización del firmware mediante Lifecycle Controller Remote Services

Para obtener información sobre cómo actualizar el firmware mediante Lifecycle Controller–Remote Services, consulte la *Lifecycle Controller–Remote Services User's Guide* (Guía del usuario de Lifecycle Controller–Remote Services) disponible en support.dell.com/manuals.

Reversión del firmware de iDRAC7

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

- Interfaz web de iDRAC7
- Interfaz web de CMC
- CLI de RACADM (iDRAC7 y CMC)
- Lifecycle Controller
- Lifecycle Controller–Remote Services

Enlaces relacionados

[Reversión del firmware mediante la interfaz web de iDRAC7](#)

[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 iDRAC7

Para revertir mediante la interfaz web de iDRAC7:

1. En la interfaz web de iDRAC7, vaya a **Información general** → **Configuración de iDRAC** → **Actualización del firmware de iDRAC**.
Aparece la página **Firmware: carga / reversión (paso 1 de 3)**.
2. Haga clic en **Revertir**.
En la página **Estado (paso 2 de 3)** se muestran la versión de firmware actual y la de reversión.
3. De manera predeterminada, la casilla **Conservar configuración** está activada, de modo que se guardará la configuración de iDRAC7 existente después de una reversión de firmware. Para restablecer iDRAC7 a sus valores predeterminado, desactive esta casilla.

 **NOTA:** Si la configuración de iDRAC7 se restablece a los valores predeterminados, la dirección IP de iDRAC7 se restablece en 192.168.0.120. Puede acceder a iDRAC7 mediante esta IP o volver a configurar la dirección de iDRAC7 utilizando el RACADM local, el panel anterior (LCD) o la tecla F2 (RACADM remoto requiere acceso de red).

4. Haga clic en **Siguiente**.
Aparece la página **Actualización (paso 3 de 3)**.

 **NOTA:** Mientras se encuentra en modo reversión, el proceso de reversión sigue en segundo plano incluso si se aleja de esta página.

5. Una vez completada la reversión, iDRAC7 se restablece. Para utilizar iDRAC7, deberá cerrar la ventana del explorador actual y volver a conectarse mediante una nueva ventana de explorador.

6. Para ver la versión de firmware de iDRAC7, vaya a cualquiera de las páginas siguientes:
 - Vaya a **Información general** → **Servidor** → **Propiedades** → **Resumen** y consulte la versión de firmware bajo la sección **Información del servidor**.
 - Vaya a **Información general** → **Configuración de iDRAC** → **Propiedades** y consulte la versión de firmware bajo la sección **Integrated Dell Remote Access Controller 7**.

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** para iniciar la interfaz web y realice la reversión del firmware de iDRAC7.

Reversión del firmware mediante RACADM

Para revertir a una versión anterior del firmware, utilice el comando **fwupdate**. Para obtener más información, consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC) disponible en support.dell.com/manuals.

Reversión del firmware mediante Lifecycle Controller

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

Reversión del firmware mediante Lifecycle Controller Remote Services

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

Recuperación de iDRAC7

iDRAC7 admite dos imágenes de sistema operativo garantizar un iDRAC7 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 iDRAC7 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 iDRAC7 y luego reinicia iDRAC7.

Uso del servidor TFTP

Puede configurar el servidor Protocolo de transferencia de archivos trivial (TFTP) para actualizar o revertir el firmware de iDRAC7 o instalar certificados. Se utiliza en interfaces de línea de comandos SM-CLP y RACADM para transferir archivos desde y hasta iDRAC7. El servidor TFTP debe ser accesible mediante una dirección IP de iDRAC7 o un nombre de DNS.



NOTA: Si utiliza la interfaz web de iDRAC7 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.

Supervisión de iDRAC7 mediante otras herramientas de administración del sistema

Puede descubrir y supervisar iDRAC7 mediante IT Assistant, Dell Management Console y Dell OpenManage Essentials. También puede utilizar la herramienta de configuración Dell Remote Access (DRACT) para descubrir iDRAC, actualizar el firmware y configurar Active Directory. Para obtener más información, consulte las guías del usuario correspondientes.

Configuración de iDRAC7


iDRAC7 permite configurar las propiedades de iDRAC7, configurar usuarios y establecer alertas para realizar tareas de administración remotas.

Antes de configurar iDRAC7, asegúrese de haber establecido la configuración de red de iDRAC7 y configurado un explorador compatible. Asimismo, asegúrese de actualizar las licencias adecuadas. Para obtener más información acerca de la función con licencia en iDRAC7, consulte [Administración de licencias](#).

Puede configurar iDRAC7 mediante los elementos siguientes.

- Interfaz web de iDRAC7
- 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 iDRAC7:

1. Inicie sesión en iDRAC7.
2. Si fuera necesario, modifique la configuración de la red.
 **NOTA:** Si ha configurado los valores de red de iDRAC7 mediante la utilidad de configuración de iDRAC durante la configuración de la dirección IP de iDRAC7, puede omitir este paso.
3. Configure las interfaces para acceder a iDRAC7.
4. Configure la visualización del panel frontal.
5. Si fuera necesario, configure la ubicación del sistema.
6. Establezca cualquiera de los siguientes métodos de comunicación alternativos con el iDRAC7:
 - Comunicación en serie IPMI o RAC
 - Comunicación en serie IPMI en la LAN
 - IPMI en la LAN
 - Cliente SSH o Telnet
7. Obtenga los certificados necesarios.
8. Agregue y configure los usuarios con privilegios de iDRAC7.
9. Configure y active las alertas por correo electrónico, las capturas SNMP o las alertas IPMI.
10. Si fuera necesario, establezca la política de límite de alimentación.
11. Active la pantalla de último bloqueo.
12. Si fuera necesario, configure la consola virtual y los medios virtuales.
13. Si fuera necesario, configure la tarjeta vFlash SD.
14. Si fuera necesario, establezca el primer dispositivo de inicio.
15. Si fuera necesario, establezca la comunicación de administración interna.

Enlaces relacionados

[Inicio de sesión en iDRAC7](#)

[Modificación de la configuración de red](#)
[Configuración de servicios](#)
[Configuración del panel frontal](#)
[Configuración de la ubicación de Managed System](#)
[Configuración de la comunicación de iDRAC7](#)
[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 de la comunicación de la administración de sistemas internos](#)
[Configuración de iDRAC7 para enviar alertas](#)

Visualización de la información iDRAC7

Puede ver las propiedades básicas de iDRAC7.

Visualización de la información de iDRAC7 mediante la interfaz web

En la interfaz web de iDRAC7, vaya a **Información general** → **Configuración de iDRAC** → **Propiedades** para ver la información siguiente relacionada con iDRAC7. Para obtener información acerca de las propiedades, consulte la *Ayuda en línea de iDRAC7*.

- Tipo de dispositivo
- Versión de hardware y firmware
- Última actualización del firmware
- Hora del RAC
- Número posible de sesiones activas
- Número actual de sesiones activas
- LAN está activada o desactivada
- 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 iDRAC7 mediante RACADM


Para ver la información de iDRAC7 mediante RACADM, consulte los detalles del subcomando `getsysinfo` o `get` que se proporcionan en la *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC) disponible en support.dell.com/manuals.

Modificación de la configuración de red

Después de establecer la configuración de red de iDRAC7 mediante la utilidad de configuración de iDRAC, también puede modificarla mediante la interfaz web de iDRAC7, 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 red mediante la interfaz web de iDRAC7 o RACADM, deberá disponer de los privilegios **Configurar iDRAC**.

 **NOTA:** Si modifica la configuración de red, es posible que se anulen las conexiones de red actuales a iDRAC7.

Modificación de la configuración de red mediante la interfaz web

Para modificar la configuración de red de iDRAC7:

1. En la interfaz web de iDRAC7, vaya a **Información general** → **Configuración de iDRAC** → **Red**. Aparecerá la página **Red**.
2. Especifique la información necesaria y haga clic en **Aplicar**.
Para obtener información acerca de los distintos valores, consulte la *Ayuda en línea de iDRAC7*.

Modificación de la configuración de red mediante RACADM local

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


```
racadm getconfig -g cfgLanNetworking
```

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

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

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

```
racadm config -g cfgLanNetworking -o cfgNicEnable 1
racadm config -g cfgLanNetworking -o cfgNicIpAddress 192.168.0.120
racadm config -g cfgLanNetworking -o cfgNicNetmask 255.255.255.0
racadm config -g cfgLanNetworking -o cfgNicGateway 192.168.0.120
racadm config -g cfgLanNetworking -o cfgNicUseDHCP 0
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0
racadm config -g cfgLanNetworking -o cfgDNSServer1 192.168.0.5
racadm config -g cfgLanNetworking -o cfgDNSServer2 192.168.0.6
racadm config -g cfgLanNetworking -o cfgDNSRegisterRac 1
racadm config -g cfgLanNetworking -o cfgDNSRacName RAC-EK00002
racadm config -g cfgLanNetworking -o cfgDNSDomainNameFromDHCP 0
racadm config -g cfgLanNetworking -o cfgDNSDomainName MI_DOMINIO
```

 **NOTA:** Si **cfgNicEnable** se define en **0**, la LAN de iDRAC7 se desactiva aun cuando DHCP esté activado.

Configuración del filtrado de IP y bloqueo de IP


Además de la autenticación de usuario, utilice las opciones siguientes para proporcionar seguridad adicional mientras accede al iDRAC7:


- El filtrado IP limita el rango de direcciones IP de los clientes que acceden al iDRAC7. Compara la dirección IP de un inicio de sesión entrante con el rango especificado y solo permite el acceso a iDRAC7 desde una estación de

administración cuya dirección IP se encuentre dentro de dicho rango. Todas las demás solicitudes de inicio de sesión se deniegan.

- El bloqueo de IP detecta de forma dinámica cuando se presentan fallas de inicio de sesión provenientes de una dirección IP específica y bloquea (o impide) el inicio de sesión de dicha dirección en el iDRAC7 durante un lapso de tiempo predefinido. Incluye lo siguiente:
 - El número de fallas de inicio de sesión permitidas.
 - El periodo en segundos durante el cual se deben presentar estas fallas.
 - El marco de tiempo en segundos durante el que se impide que la dirección IP bloqueada establezca una sesión después de haber excedido el número de fallas permitidas.

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: *Identificación de intercambio de SSH: el host remoto cerró la conexión.*

 **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 y el bloqueo IP mediante la interfaz web de iDRAC7

Debe disponer del privilegio Configurar iDRAC7 para realizar estos pasos.

Para configurar el filtrado y el bloqueo IP

1. En la interfaz web de iDRAC7, 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 y bloqueo IP. Para obtener más información acerca de estas opciones, consulte la *Ayuda en línea de iDRAC7*.
4. Haga clic en **Aplicar** para guardar la configuración.

Configuración del filtrado y el bloqueo IP mediante RACADM

Debe disponer del privilegio Configurar iDRAC7 para realizar estos pasos.

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

- `cfgRacTuneIpRangeEnable`
- `cfgRacTuneIpRangeAddr`
- `cfgRacTuneIpRangeMask`
- `cfgRacTuneIpBlkEnable`
- `cfgRacTuneIpBlkFailCount`
- `cfgRacTuneIpBlkFailWindow`

La propiedad `cfgRacTuneIpRangeMask` se aplica a la dirección IP entrante y a la propiedad `cfgRacTuneIpRangeAddr`. Si los resultados son idénticos, a la solicitud de inicio de sesión entrante se le permite acceso a iDRAC7. 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:

```
cfgRacTuneIpRangeMask & (<dirección-IP-entrante> ^ cfgRacTuneIpRangeAddr)
```

donde `&` es el operador AND a nivel de bits de las cantidades y `^` es el operador OR 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:

```
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
```
- 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, según se muestra a continuación:

```
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeEnable 1
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeAddr 192.168.0.212
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeMask 255.255.255.252
```

El último byte de la máscara de rango está establecido en 252, el equivalente decimal de 1111100b.

Ejemplos bloqueo de IP

- El ejemplo siguiente impide que una dirección IP de la estación de administración establecer una sesión durante cinco minutos si ha fallado cinco intentos de inicio de sesión en el transcurso de un minuto.

```
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeEnable 1
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 5
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindow 60
```
- El ejemplo siguiente impide más de tres intentos con error dentro de un minuto e impide los intentos de inicio de sesión adicionales durante una hora.

```
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkEnable 1
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 3
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindow 60
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 3600
```

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

Configuración de servicios

Puede configurar y activar los servicios siguientes en iDRAC7:

- Configuración local: desactive el acceso a la configuración de iDRAC7 (desde el sistema host) mediante RACADM local y la utilidad de configuración de iDRAC.
- Servidor web: active el acceso a la interfaz web de iDRAC7. Si desactiva la opción, puede activarla mediante RACADM.
- SSH: acceda a iDRAC7 a través del firmware RACADM.
- Telnet: acceda a iDRAC7 a través del firmware RACADM.
- RACADM remoto: acceda a iDRAC7 de forma remota.
- Agente SNMP: active iDRAC7 para enviar capturas SNMP para los sucesos.
- Agente de recuperación automatizado del sistema: active la pantalla de último bloqueo del sistema.

Configuración de servicios mediante la interfaz web

Para configurar los servicios mediante la interfaz web de iDRAC7:

1. En la interfaz web de iDRAC7, 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 iDRAC7*.

Configuración de los servicios mediante RACADM

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

- `cfgRacTuneLocalConfigDisable`
- `cfgRacTuneCtrlEConfigDisable`
- `cfgSerialSshEnable`
- `cfgRacTuneSshPort`
- `cfgSsnMgtSshIdleTimeout`
- `cfgSerialTelnetEnable`
- `cfgRacTuneTelnetPort`
- `cfgSsnMgtTelnetIdleTimeout`
- `cfgRacTuneWebserverEnable`
- `cfgSsnMgtWebserverTimeout`
- `cfgRacTuneHttpPort`
- `cfgRacTuneHttpsPort`
- `cfgRacTuneRemoteRacadmEnable`
- `cfgSsnMgtRacadmTimeout`
- `cfgOobSnmpAgentEnable`
- `cfgOobSnmpAgentCommunity`

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

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 del panel frontal del LCD del servidor:

1. En la interfaz web de iDRAC7, 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 (valor 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
 - Ninguna

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. Haga clic en **Aplicar**.

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

Configuración de los valores LCD mediante RACADM

Para configurar la visualización del panel anterior LCD del servidor, utilice los objetos del grupo `System.LCD`. Para obtener más información, consulte la *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC) disponible en support.dell.com/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 **LCD**.

Aparece la pantalla **LCD de configuración de iDRAC**.
2. Especifique las opciones obligatorias.

Para obtener 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**.

La configuración se guarda.

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 iDRAC7, vaya a **Información general** → **Hardware** → **Panel frontal**. Se abre 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 tiempo de espera de 1 día
 - Activar parpadeo tiempo de espera de 1 semana
 - Activar parpadeo tiempo de espera de 1 mes
3. Haga clic en **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 ID del sistema, utilice el comando **setled**. Para obtener más información, consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC) disponible en support.dell.com/manuals.

Configuración del primer dispositivo de inicio

Puede configurar el primer dispositivo de inicio para el siguiente inicio solamente 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 que se reinicie y todas las veces subsiguientes y permanece como el primer dispositivo de inicio hasta que se vuelva a cambiar en la interfaz web de iDRAC7 o en la secuencia de inicio del BIOS.

 **NOTA:** La configuración del primer dispositivo de inicio en la interfaz web de iDRAC7 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 iDRAC7:

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 iDRAC7*.

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

Activación de la comunicación de la administración de sistemas internos

En sistemas tipo bastidor o torre con dispositivos de tarjeta secundaria de red (NDC) o de LAN de la placa base (LOM), puede activar el canal de comunicación de la administración de sistemas internos que proporciona comunicación bidireccional de alta velocidad y dentro de banda entre iDRAC7 y el sistema operativo host a través de una LOM compartida. Puede activar este canal mediante los elementos siguientes:

- Utilidad de configuración de iDRAC (entorno anterior a la carga del sistema operativo)
- RACADM o WS-MAN (entorno posterior a la carga del sistema operativo)
- iDRAC7 se encuentra en modo compartido (es decir, la selección NIC se asigna a una de las LOM)
- El sistema operativo host e iDRAC7 se encuentran en la subred y la misma VLAN.

IMC admite direcciones IPv4 e IPv6.

Antes de activar la comunicación de la administración de sistemas internos, asegúrese de lo siguiente:

- iDRAC7 se encuentra en modo compartido (es decir, la selección NIC se asigna a una de las LOM).
- El sistema operativo host e iDRAC7 se encuentran en la subred y la misma VLAN.

Activación de IMC mediante la utilidad de configuración de iDRAC

Para activar IMC mediante la utilidad de configuración de iDRAC:

1. En la utilidad de configuración de iDRAC, vaya a **Paso a través de comunicación**. Se muestra la ventana **Paso a través de comunicación**.
2. Seleccione **Activado**.
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**.
Los detalles se guardan.

Activación de IMC mediante RACADM

Para establecer iDRAC7 en modo compartido (ejemplo LOM1):

```
racadm config -g cfglannetworking -o cfnicselection 2
```

Para activar IMC:

```
racadm set idrac.imc.AdministrativeState Enabled
```

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 iDRAC7.

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 la *Dell OpenManage Server Administrator Installation Guide* (Guía de instalación de Dell OpenManage Server Administrator) disponible en support.dell.com/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 la *Dell OpenManage Server Administrator Installation Guide* (Guía de instalación de Dell OpenManage Server Administrator) disponible en support.dell.com/manuals.

4. Active la opción **Apagado y recuperación automática** (ASR) mediante uno de los procedimientos siguientes:
 - Server Administrator: consulte la *Dell OpenManage Server Administrator User's Guide* (Guía del usuario de Server Administrator de Dell OpenManage) disponible en support.dell.com/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**.

Obtención de certificados

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

Tabla 7. 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	Generar una CSR y hacer que la firme una autoridad de certificados
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
Inicio de sesión de usuario de Active Directory	Certificado de CA de confianza	Este certificado lo emite una CA.
Inicio de sesión de usuario local	Certificado SSL	Generar una CSR y hacer que la firme una CA de confianza

 **NOTA:** iDRAC7 se entrega con un certificado de servidor SSL autofirmado predeterminado. El servidor web de iDRAC7, los medios virtuales y la consola virtual utilizan este certificado.

Enlaces relacionados

[Certificados de servidor SSL](#)

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

Certificados de servidor SSL

iDRAC7 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 para 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. iDRAC7 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, iDRAC7 Web Server dispone de un certificado digital SSL firmado por Dell. Para asegurarse de que las sesiones iDRAC7 son autenticadas e impedir que los administradores divulgan las credenciales de iDRAC7 a usuarios no autorizados, reemplace el certificado del servidor SSL con un certificado firmado por una autoridad de certificados (CA) conocida. Una CA es una entidad comercial reconocida en el sector de la tecnología de la información para cumplir los elevados estándares de filtrado e identificación de confianza, así como otros criterios de seguridad importantes. Entre los ejemplos de CA se incluyen Thawte y VeriSign.

Para iniciar el proceso de obtener un certificado firmado, utilice la interfaz web de iDRAC7 o una interfaz RACADM para generar una solicitud de firma de certificado (CSR) con la información de la compañía. A continuación, envíe la CSR generada a una CA, tal como VeriSign o Thawte.

Enlaces relacionados

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

[Carga del certificado del servidor](#)

[Visualización del certificado del servidor](#)

Generación de una nueva solicitud de firma de certificado

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, este puede cargarse en iDRAC7. La información que se utiliza para generar la CSR, almacenada en el firmware de iDRAC7, 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 iDRAC7.

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, iDRAC7 no aceptará el certificado.

1. En la interfaz web de iDRAC7, vaya a **Información general** → **Configuración de iDRAC** → **Red** → **SSL**, seleccione **Generar una nueva solicitud de firma de certificado (CSR)** y 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 iDRAC7*.
3. Haga clic en **Generar**.
Se genera una nueva CSR.
4. Haga clic en **Descargar** para guardar el archivo CSR en la estación de administración.

Generación de CSR mediante RACADM

Para generar una CSR, utilice los objetos del grupo `cfgRacSecurityData` para especifica los valores y utilice el comando `sslcsrigen` para generar la CSR. Para obtener más información, consulte la *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC7 y CMC) disponible en support.dell.com/manuals.

Carga del certificado del servidor

Después de generar una CSR, puede cargar el certificado del servidor SSL firmado al firmware de iDRAC7. iDRAC7 se restablece una vez cargado el certificado. iDRAC7 solo acepta certificados de servidor web codificado con X509, Base 64.

 **PRECAUCIÓN:** Durante el proceso de carga del certificado, iDRAC7 no está disponible.

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 iDRAC7, 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 **Aplicar**.
El certificado de servidor SSL se carga en el firmware de iDRAC7 y reemplaza el certificado existente.

Carga el certificado del servidor mediante RACADM

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

Visualización del certificado del servidor

Puede ver el certificado de servidor SSL que se utiliza actualmente en iDRAC7.

Enlaces relacionados

[Certificados de servidor SSL](#)

Visualización del certificado del servidor mediante la interfaz web


En la interfaz web de iDRAC7, vaya a **Información general** → **Configuración de iDRAC** → **Red** → **SSL**, seleccione **Ver certificado del servidor** y haga clic en **Siguiente**. Se mostrará la página **Ver certificado del servidor** con el certificado del servidor SSL en uso.

Visualización del certificado del servidor mediante RACADM

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

Configuración de varios iDRAC7s mediante RACADM


Puede configurar uno o más iDRAC7 con propiedades idénticas mediante RACADM. Al consultar un iDRAC7 específico utilizando este ID de grupo e ID de objeto, RACADM crea el archivo de configuración `.cfg` de la información recuperada. El nombre de archivo lo especifica el usuario. Importe el archivo a otros iDRAC7s para configurarlos de manera idéntica.


 **NOTA:** Pocos archivos de configuración contienen información de iDRAC7 única (tal como la dirección IP estática) que debe modificar antes de exportar el archivo a otros iDRAC7s.

Para configurar varios iDRAC7:

1. Consulte el iDRAC7 de destino que contiene la configuración necesaria mediante el comando: `racadm getconfig -f myfile.cfg`.


El comando solicita la configuración de iDRAC7 y genera el archivo **myfile.cfg**. Si fuera necesario, puede configurar el archivo con otro nombre.

 **NOTA:** La redirección de la configuración de iDRAC7 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 iDRAC7 de destino mediante el comando: `racadm config -f myfile.cfg`

De este modo, la información se carga en el otro iDRAC7. Puede utilizar el subcomando `config` para sincronizar la base de datos de usuarios y contraseñas mediante Server Administrator.

4. Restablezca el iDRAC7 de destino mediante: `racadm racreset`

Creación de un archivo de configuración de iDRAC7

El archivo de configuración `.cfg` se puede:

- crear
- obtener a partir de un comando `racadm getconfig -f <nombredearchivo>.cfg`.
- obtener a partir de un comando `acadm getconfig -f <nombredearchivo>.cfg` y luego editar.


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

El archivo `.cfg` primero se analiza para verificar que contiene nombres de grupo y objeto válidos y que las reglas de sintaxis básicas se cumplen. 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 que está correcto y se muestran todos los errores. Los comandos de escritura no se transmiten a iDRAC7 si se encuentra un error en el archivo `.cfg`. El usuario debe corregir todos los errores antes de utilizar el archivo para configurar iDRAC7. Utilice la opción `-c` en el subcomando `config`, que verifica la sintaxis y no realiza ninguna operación de escritura en iDRAC7.

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:

```
[cfgUserAdmin]
# cfgUserAdminIndex=11
cfgUserAdminUserName=
# cfgUserAdminPassword=***** (solo lectura)
cfgUserAdminEnable=0
cfgUserAdminPrivilege=0x00000000
cfgUserAdminIpmiLanPrivilege=15
cfgUserAdminIpmiSerialPrivilege=15
cfgUserAdminSolEnable=0
```
- 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.
- Hay disponible un conjunto predefinido de índices para cada grupo indexado. Para obtener más información, consulte la *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC) disponible en support.dell.com/manuals.
- Utilice el subcomando `racresetcfg` para restablecer iDRAC7 a sus valores predeterminados y luego ejecute el comando `racadm config -f <nombredearchivo>.cfg`. Asegúrese de que el archivo `.cfg` incluya todos los objetos, los usuarios, los índices y los parámetros necesarios.

 **PRECAUCIÓN:** Utilice el subcomando `racresetcfg` para restablecer la base de datos y la configuración de la NIC de iDRAC7 a sus valores predeterminados y quite todos los usuarios y configuraciones de usuario. Mientras el usuario raíz esté 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. Un carácter de escape no es necesario. Puede generar un archivo `.cfg` desde un comando `racadm getconfig -f <nombredearchivo>.cfg` y luego ejecutar un comando `racadm config -f <nombredearchivo>.cfg` a un iDRAC7 diferente, sin agregar caracteres de escape. Por ejemplo:

```
N.º
# Esto es un comentario
[cfgUserAdmin]
cfgUserAdminPageModemInitString=<Inicialización de módem # no es un comentario>
```

- 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 generan un error. Los datos de configuración se organizan en grupos, según se define en la *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC7 y CMC) disponible en support.dell.com/manuals. En el ejemplo siguiente se muestra un nombre de grupo, un objeto y el valor de la propiedad del objeto.

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

- 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 <nombredearchivo>.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 <Nombredegrupo> -i <índice de 1 a 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 <miejemplo>.cfg`, el comando genera un archivo **.cfg** para la configuración actual de iDRAC7. 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 iDRAC7

Cuando modifica la dirección IP de iDRAC7 en el archivo de configuración, quite 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:

```
N.º
# Grupo de objeto "cfgLanNetworking"
N.º
[cfgLanNetworking]
cfgNicIpAddress=10.35.10.110
cfgNicGateway=10.35.10.1
```


Este archivo se actualiza de la siguiente forma:

```
N.º
# Grupo de objeto "cfgLanNetworking"
N.º
[cfgLanNetworking]
cfgNicIpAddress=10.35.9.143
# comentario, el resto de esta línea se ignora
```

```
cfgNicGateway=10.35.9.1
```

El comando `racadm config -f myfile.cfg` analiza el archivo e identifica 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 iDRAC7 en el sistema host

Puede desactivar el acceso para modificar la configuración de iDRAC7 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 iDRAC7, 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 **Aplicar**.

 **NOTA:** Si se desactiva el acceso, no podrá utilizar Server Administrator ni IPMITool para realizar las configuraciones de iDRAC7. Sin embargo, podrá utilizar IPMI en la LAN.

Visualización de la información de iDRAC7 y Managed System

Puede ver la condición y las propiedades de iDRAC7 y el 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 podrá 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](#)
- [Inventario y supervisión de dispositivos de almacenamiento](#)
- [Inventario y supervisión de dispositivos de red](#)
- [Visualización de las conexiones de red Fabric de la tarjeta mezzanine FlexAddress](#)
- [Visualización o terminación de sesiones iDRAC7](#)

Visualización de la condición y las propiedades de Managed System

Cuando inicia sesión en la interfaz web de iDRAC7, la página **Resumen del sistema** permite ver la condición del sistema administrado, la información básica de iDRAC7 y una vista previa de la consola virtual. También permite agregar y ver notas de trabajo e iniciar tareas rápidamente, tal como apagado/encendido, ciclo de encendido, visualización de registros, actualización del firmware y restablecimiento de iDRAC7.


Para acceder a la página **Resumen del sistema**, vaya a **Información general** → **Servidor** → **Propiedades** → **Resumen**. Se muestra la página **Resumen del sistema**. Para obtener más información, consulte la *Ayuda en línea de iDRAC7*.

También puede ver información resumida del sistema básico 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 **Resumen del sistema de la configuración de iDRAC**. Para obtener más información, consulte la *Ayuda en línea de la utilidad de configuración de iDRAC*.

Visualización del inventario del sistema

Puede ver información acerca de los componentes de hardware y firmware instalados en el sistema administrado. Para ello, en la interfaz web de iDRAC7, vaya a **Información general** → **Servidor** → **Properties** → **Propiedades del sistema**. Para obtener más información acerca de las propiedades mostradas, consulte la *Ayuda en línea de iDRAC7*.


Si reemplaza componentes de hardware o actualiza versiones de firmware, asegúrese de activar y ejecutar la opción **Recopilar inventario del sistema al reiniciar**(CSR) para recopilar el inventario el sistema al reiniciar. Tras uno minutos, inicie sesión en iDRAC7 y vaya a la página **Inventario del sistema** para ver los detalles. Puede llevar hasta 5 minutos hasta que la información esté disponible, en función del hardware instalado en el servidor.

 **NOTA:** La opción CSR está activada de forma predeterminada.


Visualización de la información del sensor

Los sensores siguientes ayudan a supervisar la condición del sistema administrado:

- **Sensor de la batería:** proporciona información acerca de las baterías del CMOS de la placa base y el RAID de almacenamiento RAID 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.

- **Sensor de 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 muestran la velocidad de los ventiladores y los valores de umbral.
- **Sensor de CPU:** indica la condición de las CPU en el sistema administrado.
- **Sensor de intrusiones:** proporciona información acerca del chasis.
- **Sensor de 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**.

- **Sensor de soporte Flash extraíble:** 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.
 - 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.
- **Sensor de temperatura:** proporciona información acerca de la temperatura interna de la placa base y la temperatura de expulsión (solo se aplica a bastidores y torres). La sonda de temperatura indica si el estado de la sonda está dentro de los valores de umbral de aviso y críticos.
- **Sensor de 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 iDRAC7 y RACADM. Para obtener información acerca de las propiedades que se muestran en la interfaz web, consulte la *Ayuda en línea de iDRAC7* de las páginas correspondientes.

Tabla 8. Información del sensor mediante la interfaz web y RACADM

Visualización de la información del sensor	Mediante la interfaz web	Mediante RACADM
Batería	Información general → Hardware → Baterías	Utilice el comando getsensorinfo . Para suministros de energía, también puede usar el comando

Visualización de la información del sensor	Mediante la interfaz web	Mediante RACADM
		<p>System.Power.Supply con el subcomando <code>get</code>.</p> <p>Para obtener más información, consulte la <i>RACADM Command Line Reference Guide for iDRAC7 and CMC</i> (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC) disponible en support.dell.com/manuals.</p>
Ventilador	Información general → Hardware → Ventiladores	
CPU	Información general → Hardware → CPU	
Intrusión	Información general → Servidor → Intrusión	
Suministros de energía	Información general → Hardware → Suministros de energía	
Unidades Flash extraíbles	Información general → Hardware → Unidades Flash extraíbles	
Temperatura	Información general → Servidor → Alimentación/Térmico → Temperaturas	
Voltaje	Información general → Servidor → Alimentación/Térmico → Voltajes	

Inventario y supervisión de dispositivos de almacenamiento

Puede supervisar remotamente la condición y ver el inventario de los siguientes dispositivos de almacenamiento con capacidad CEM (administración incorporada completa) del sistema administrador mediante la interfaz web de iDRAC7 o RACADM:

- Controladoras RAID que incluyen una batería
- Gabinetes que incluyen módulos de administración de gabinetes (EMM), suministros de energía, sonda de ventilador y sonda de temperatura
- Discos físicos
- Discos virtuales

No obstante, WS-MAN muestra información para la mayoría de los dispositivos de almacenamiento del sistema.

iDRAC7 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) y SAS 6Gbps 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.

Para obtener información conceptual, consulte la *OpenManage Storage Management User's Guide* Guía del usuario de OpenManage Storage Management) disponible en support.dell.com/manuals.

Supervisión de dispositivos de almacenamiento mediante la interfaz web

Para ver la información del dispositivo de almacenamiento mediante la interfaz web:

- Vaya a **Información 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 **Información general** → **Almacenamiento** → **Topología** para ver la vista de contención física jerárquica de los componentes de almacenamiento clave.
- Vaya a **Información general** → **Almacenamiento** → **Discos físicos** para ver la información del disco físico. Se muestra la página **Discos físicos**.
- Vaya a **Información general** → **Almacenamiento** → **Discos virtuales** para ver la información del disco virtual. Se muestra la página **Discos virtuales**.
- Vaya a **Información general** → **Almacenamiento** → **Controladoras** para ver la información de la controladora RAID. Se muestra la página **Controladoras**.
- Vaya a **Información general** → **Almacenamiento** → **Gabinetes** para ver la información del gabinete. Se muestra la página **Gabinetes**.

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 iDRAC7*.

Supervisión de dispositivos de almacenamiento mediante RACADM

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

Inventario y supervisión de dispositivos de red

Puede supervisar de manera remota la condición de los siguientes dispositivos de red en el sistema administrado y ver el inventario de los mismos:


- 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)

Para cada dispositivo, puede ver la siguiente información sobre los puertos y las particiones admitidas:

- Estado del vínculo
- Propiedades
- Configuración y capacidades
- Estadísticas de recepción y transmisión

Supervisión de dispositivos de red mediante la interfaz web

Para ver la información del dispositivo de red mediante la interfaz de red, vaya a **Información 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 iDRAC7*.

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

Pueden mostrarse propiedades adicionales cuando se utiliza RACADM o WS-MAN, además de las propiedades que se muestran en la interfaz web de iDRAC7.


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 dirección Flex en iDRAC7, configure y active la función Dirección Flex en la controladora de administración de chasis (CMC). Para obtener más información, consulte la *Dell Chassis Management Controller User Guide* (Guía del usuario de Dell Chassis Management Controller) disponible en support.dell.com/manuals. Las sesiones de consola virtual o medios virtuales existentes se terminará si la configuración FlexAddress está activada o desactivada.


 **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 iDRAC7 junto con los LOM de Blade, las tarjetas mezzanine y los módulos de E/S. La función FlexAddress de iDRAC7 admite la conservación de una dirección MAC específica de ranura para iDRAC7s en un chasis. La dirección MAC asignada por el chasis se almacenan en memoria no volátil de CMC y se envía a iDRAC7 durante un inicio de iDRAC7 o cuando se activa CMC FlexAddress.

Si CMC activa direcciones MAC asignadas por el chasis, iDRAC7 muestra la **Dirección MAC** en cualquiera de las páginas siguientes:

- **Información general** → **Servidor** → **Propiedades Detalles** → **Información iDRAC**.
- **Información general** → **Servidor** → **Propiedades WWN/MAC**.
- **Información general** → **Configuración de iDRAC** → **Propiedades Información iDRAC** → **Configuración de red actual**.

- Información general → Configuración de iDRAC → Red Red → Configuración de red.

 **PRECAUCIÓN:** Con la función FlexAddress activada, si se pasa de una dirección MAC asignada por el servidor a una asignada por el chasis y viceversa, la dirección IP de iDRAC7 también cambia.

Visualización o terminación de sesiones iDRAC7

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

Terminación de las sesiones de iDRAC7 mediante la interfaz web

Los usuarios que no tienen privilegios administrativos deben tener privilegios de configuración de iDRAC7 para terminar sesiones iDRAC7 mediante la interfaz web de iDRAC7.

Para ver y terminar las sesiones iDRAC7:

1. En la interfaz web de iDRAC7, vaya a **Información 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 iDRAC7*.
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 iDRAC7 mediante RACADM

Debe disponer de privilegios de administrador para terminar las sesiones iDRAC7 mediante RACADM.

Para ver las sesiones de usuario actual, utilice la comando **getssninfo**.

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

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

Configuración de la comunicación de iDRAC7

Puede comunicarse con iDRAC7 mediante cualquiera de los modos siguientes:

- Interfaz web de iDRAC7
- 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 requisitos, consulte la tabla siguiente.

Tabla 9. Modos de comunicación: resumen

Modos de comunicación	Protocolo compatible	Comandos admitidos	Prerrequisito
Interfaz web de iDRAC7	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 iDRAC7 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 iDRAC7 se activa.
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 la *Lifecycle Controller Remote Services User's Guide* (Guía del usuario de servicios remotos de Dell Lifecycle Controller) disponible en support.dell.com/manuals.


Enlaces relacionados

- [Comunicación con iDRAC7 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 iDRAC7 mediante IPMI SOL](#)
- [Comunicación con iDRAC7 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 iDRAC7 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 la *Chassis Management Controller User's Guide* (Guía del usuario de Chassis Management Controller) disponible en support.dell.com/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 serie RAC o IPMI en iDRAC7.

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 iDRAC7 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 iDRAC7.



NOTA: Esto es aplicable solamente para iDRAC7 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 iDRAC7, vaya a **Información general** → **Configuración de iDRAC** → **Red** → **Comunicación en serie**.
Aparecerá la página **Comunicación en serie**.
2. En **Comunicación en serie RAC**, seleccione **Activado** y especifique los valores de los atributos.
3. Haga clic en **Aplicar**.
Se habrán configurado los valores de la comunicación en serie IPMI.

Activación de la conexión serie RAC mediante RACADM

Para activar la conexión serie RAC:

```
racadm config -g cfgSerial -o cfgSerialConsoleEnable 1
```

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 iDRAC7, configure la comunicación en serie IPMI en cualquiera de los modos siguientes en iDRAC7:



NOTA: Esto es aplicable solamente para iDRAC7 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. Permite ver las secuencias de inicio del sistema operativo hasta el BIOS, cuando inicia sesión en iDRAC7 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 iDRAC7, vaya a **Información 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 iDRAC7*.
3. Haga clic en **Aplicar**.

Activación del modo de comunicación en serie de IPMI mediante RACADM

Para configurar el modo IPMI:

1. Desactive la interfaz serie del RAC.


```
racadm config -g cfgSerial -o cfgSerialConsoleEnable 0
```
2. Active el modo IPMI adecuado.


```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialConnectionMode <0 01>
```

 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 comunicación en serie IPMI:

1. Cambie el modo de conexión serie IPMI al valor adecuado mediante el comando:


```
racadm config -g cfgSerial -o cfgSerialConsoleEnable 0
```
2. Establezca la velocidad en baudios de IPMI mediante el comando `racadm config -g cfgIpmiSerial -o cfgIpmiSerialBaudRate<velocidad_baudios>` donde `<velocidad_baudios>` es 9600, 19200, 57600 o 115200 bps.
3. Active el control de flujo de conexión serie IPMI mediante el comando: `racadm config -g cfgIpmiSerial -o cfgIpmiSerialFlowControl 1`
4. Establezca el nivel de privilegio mínimo del canal serie IPMI mediante el comando `racadm config -g cfgIpmiSerial -o cfgIpmiSerialChanPrivLimit <nivel>`, 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 iDRAC7, 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 iDRAC7*.

5. Haga clic en **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 siguiente: `racadm config cfgIpmiSerial`

Cambio entre la comunicación en serie RAC y la consola de comunicación en serie mediante el cable DB9

iDRAC7 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> +<Mayús> <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> +<Mayús> <q>`

En modo de terminal, para cambiar la conexión al modo de consola de comunicación en serie utilice:

`<Esc> +<Mayús> <q>`

Para volver al uso de modo de terminal, cuando esté conectado en el modo de consola de comunicación en serie:

`<Esc> +<Mayús> <9>`

Comunicación con iDRAC7 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 iDRAC7. 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 iDRAC7 para utilizar SOL.
3. Active un protocolo compatible (SSH, Telnet, IPMItool).

Enlaces relacionados


[Configuración del BIOS para la conexión serie](#)

[Configuración de iDRAC7 para utilizar 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 iDRAC7 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 en serie** en **Activado con redireccionamiento 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**.

Configuración de iDRAC7 para utilizar SOL

Puede especificar la configuración de SOL en iDRAC7 mediante la interfaz web, RACADM o la utilidad de configuración de iDRAC.



Configuración de iDRAC7 para usar SOL mediante la interfaz web iDRAC7

Para configurar la comunicación en serie IPMI en la LAN (SOL).

1. En la interfaz web de iDRAC7, 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 iDRAC7*.

Configuración de iDRAC7 para usar SOL mediante RACADM

Para configurar la comunicación en serie IPMI en la LAN (SOL).

1. Para activar la Comunicación en serie IPMI en la LAN, ejecute el comando `racadm config -g cfgIpmiSol -o cfgIpmiSolEnable 1`
 2. Actualice el nivel de privilegio mínimo IPMI SOL mediante el comando `racadm config -g cfgIpmiSol o cfgIpmiSolMinPrivilege <nivel>`, donde `<nivel>` 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 IPMI SOL mediante el comando `racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate <velocidad_baudios>` donde `<velocidad_baudios>` 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. Active SOL para cada usuario mediante el comando `racadm config -g cfgUserAdmin -o cfgUserAdminSolEnable -i <id> 2` donde `<id>` es el ID único del usuario.

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 **Información general** → **Configuración de iDRAC** → **Red** y seleccione **Activar IPMI en la LAN**. Asegúrese de que el valor **Clave de cifrado** es todos ceros o pulse la tecla de retroceso para borrar y cambiar el valor en caracteres NULOS.

Activación del protocolo admitido mediante RACADM

Para activar SSH o Telnet, ejecute el comando:

- Telnet: `racadm config -g cfgSerial -o cfgSerialTelnetEnable 1`

- SSH: `racadm config -g cfgSerial -o cfgSerialSshEnable 1`

 **NOTA:** Para cambiar el puerto SSH, ejecute el comando `racadm config -g cfgRacTuning -o cfgRacTuneSshPort <número de puerto>`

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 <--> iDRAC7

La utilidad SOL basada en IPMI y IPMItool utilizan RMCP+ entrega mediante datagramas UDP al puerto 623. RMCP+ proporciona opciones mejoradas de autenticación, 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 iDRAC7 debe cifrarse mediante la clave de cifrado (clave de generador de clave (KG)). Puede configurar la clave de cifrado mediante la interfaz web de iDRAC7 o la utilidad de Configuración iDRAC de iDRAC.

Para iniciar una sesión SOL mediante IPMItool desde una estación de administración:

 **NOTA:** Si fuera necesario, puede cambiar el tiempo de espera de la sesión SOL predeterminado en **Información 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 iDRAC7: `ipmitool -H <dirección IP de iDRAC7> -I lanplus -U <nombre de inicio de sesión> -P <contraseña de inicio de sesión> 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 iDRAC7 y deje que transcurran 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 realizar comunicaciones de línea de comandos a iDRAC7. Puede analizar comandos RACADM y SMCLP remotos a través de cualquiera de estas interfaces.

SSH es más seguro que Telnet. iDRAC7 solo admite SSH versión 2 con autenticación de contraseñas y está activado de manera predeterminada. iDRAC7 admite hasta dos sesiones SSH y dos sesiones Telnet a la vez. Es recomendable utilizar SSH, ya que Telnet no es un protocolo seguro. Debe utilizar Telnet solamente si no puede instalar un cliente SSH o si la infraestructura de la red es segura.

Para conectarse a iDRAC7, 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 iDRAC7, asegúrese de realizar lo siguiente:

1. Configurar el BIOS para activar la consola de comunicación en serie.
2. Configurar SOL en iDRAC7.
3. Activar SSH o Telnet mediante la interfaz web de iDRAC7 o RACADM.

Cliente Telnet (puerto 23)/SSH (puerto 22) <--> Conexión WAN <--> iDRAC7

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 iDRAC7. 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 iDRAC7: `putty.exe [-ssh | -telnet] <nombre de inicio de sesión>@<dirección IP de iDRAC7> <número de puerto>`

 **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 iDRAC7, 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 iDRAC7](#)

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 de la sesión SSH o Telnet predeterminado en **Información general** → **Configuración de iDRAC** → **Red** → **Servicios**.

1. Inicie una ventana de shell.
2. Conéctese a iDRAC7 mediante el comando siguiente:
 - Para SSH: `ssh <dirección IP de iDRAC7>-l <nombre de inicio de sesión>`
 - Para Telnet: `telnet <dirección IP de iDRAC7>`

 **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 iDRAC7 al puerto SOL del sistema administrado. Una vez establecida la sesión SOL, la consola de línea de comandos de iDRAC7 dejará de estar disponible. Siga la secuencia de escape correctamente para abrir la consola de línea de comandos de iDRAC7. 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.

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 <número>
```

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 iDRAC7](#)

Uso de la consola virtual de Telnet

Es posible que algunos clientes Telnet en el sistema operativo de Microsoft o muestren correctamente la pantalla de configuración del BIOS cuando la consola virtual del BIOS está configurada 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 iDRAC7 mediante el comando: `telnet <Dirección IP>:<Número de puerto>`, donde *Dirección IP* es la dirección IP de iDRAC7 y *Número de puerto* 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, pulse <Ctrl><J>.
3. En la petición, escriba `set bsasdel`.
Se muestra el mensaje `El retroceso se enviará como eliminación`.

Desconexión de la sesión SOL en la consola de línea de comandos de iDRAC7

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 iDRAC7.

- 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 iDRAC7 mediante IPMI en la LAN

Debe configurar IPMI en la LAN para iDRAC7 con el fin de activar o desactivar los comandos IPMI en los canales LAN a cualquier sistema externo. Si esta configuración no se establece, los sistemas externos no podrán comunicarse con el servidor iDRAC7 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 iDRAC7, 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 iDRAC7*.
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:

1. Para activar la comunicación en serie IPMI en la LAN, ejecute el comando `racadm config -g cfgIpmiSol -o cfgIpmiSolEnable 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 del canal IPMI mediante el comando: `racadm config -g cfgIpmiLan -o cfgIpmiLanPrivilegeLimit <nivel>` donde <nivel> es uno de los valores siguientes: 2 (Usuario), 3 (Operador) o 4 (Administrador)
3. Establezca la clave de cifrado del canal IPMI LAN (si fuera necesario) mediante el comando: `racadm config -g cfgIpmiLan -o cfgIpmiEncryptionKey <clave>` donde <clave> es una clave de cifrado de 20 caracteres en un formato hexadecimal válida.
-  **NOTA:** iDRAC7 IPMI admite el protocolo RMCP+. Para obtener más información, consulte las especificaciones de IPMI 2.0 en intel.com.

Activación o desactivación de RACADM remoto

Puede activar o desactivar RACADM remoto mediante la interfaz web de iDRAC7 o RACADM y puede 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 iDRAC7, vaya a **Información 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 **Aplicar**.
RACADM remoto se activa o desactiva según la opción seleccionada.

Activación o desactivación de RACADM remoto mediante RACADM

La capacidad de RACADM remoto está activada de manera predeterminada. Si está desactivada, ejecute el comando: `racadm config -g cfgRacTuning -o cfgRacTuneRemoteRacadmEnable 1` para activarla. Para desactivar la capacidad remota, ejecute el comando: `racadm config -g cfgRacTuning -o cfgRacTuneRemoteRacadmEnable 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 iDRAC7 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 la *Dell Open Manage Server Administrator's User Guide* (Guía del usuario de Dell Open Manage Server Administrator) disponible en support.dell.com/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/sdal #
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/sdal
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/sdal 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 Este archivo describe cómo el proceso INIT debe configurar #el sistema
en un nivel de ejecución determinado. #Autor:Miquel van Smoorenburg #Modificado
```

```

para RHS Linux por Marc Ewing y Donnie Barnes #Nivel de ejecución
predeterminada. Los niveles de ejecución que usa RHS son: #0 - halt (NO
establecer initdefault en este valor) #1 - Modo de un solo usuario #2 -
Multiusuario, sin NFS (Lo mismo que 3, si no tiene #conexiones a redes) #3 -
Modo multiusuario completo #4 - Sin usar #5 - X11 #6 - reboot (No establecer
initdefault en este valor) id:3:initdefault: #Inicialización del sistema.
si::sysinit:/etc/rc.d/rc.sysinit 10:0:wait:/etc/rc.d/rc 0 11:1:wait:/etc/
rc.d/rc 1 12:2:wait:/etc/rc.d/rc 2 13:3:wait:/etc/rc.d/rc 3 14:4:wait:/etc/
rc.d/rc 4 15:5:wait:/etc/rc.d/rc 5 16:6:wait:/etc/rc.d/rc 6 #Tareas a ejecutar
en cada nivel de ejecución. ud::once:/sbin/update ud::once:/sbin/update #Trap
CTRL-ALT-DELETE ca::ctrlaltdel:/sbin/shutdown -t3 -r now #Cuando la fuente UPS
indica una falla eléctrica, suponer que todavía quedan #minutos de carga
eléctrica. Planificar la desactivación por 2 minutos a partir de ahora. #Esto,
por lo general, supone la instalación eléctrica y que su #UPS está conectado y
funciona correctamente. pf::powerfail:/sbin/shutdown -f -h +2 "Falla eléctrica;
Apagado del sistema" #Si se restauró la carga eléctrica antes del apagado,
interrumpala. pr:12345:powerokwait:/sbin/shutdown -c "Carga eléctrica
restaurada; Apagado cancelado"

```

```


#Ejecutar gettys en niveles de ejecución estándar co:2345:respawn:/sbin/agetty -
-h -L 57600 ttyS1 ansi 1:2345:respawn:/sbin/mingetty tty1 2:2345:respawn:/sbin/
mingetty tty2 3:2345:respawn:/sbin/mingetty tty3 4:2345:respawn:/sbin/mingetty
tty4 5:2345:respawn:/sbin/mingetty tty5 6:2345:respawn:/sbin/mingetty tty6
#Ejecutar xdm en nivel de ejecución 5 #xdm ahora es un servicio independiente 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 iDRAC7 mediante el protocolo SSH, admite varios esquemas de criptografía que se enumeran en la tabla siguiente.

Tabla 10. 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

Tipo de esquema	Esquema
	<ul style="list-style-type: none"> • 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

iDRAC7 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 iDRAC7. 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 escenario, 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 iDRAC7 y la clave privada la utiliza el cliente SSH para establecer la relación de confianza entre la estación de administración e iDRAC7.

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 sean miembros del grupo de usuarios Administrador en iDRAC7. No obstante, los usuarios del grupo 'Personalizado' puede 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:** iDRAC7 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. iDRAC7 no realiza ninguna comprobación para asegurarse de que las claves anteriores se eliminen antes de agregarse 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 iDRAC7, vaya a **Información general** → **Configuración de iDRAC** → **Red** → **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.
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 iDRAC7.

5. Haga clic en **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 a 16> -k <1 a 4> -f <nombre de archivo>`
- Desde RACADM remoto mediante Telnet o SSH: `racadm sshpkauth -i <2 a 16> -k <1 a 4> -t <texto de clave>`

Por ejemplo, para cargar una clave válida al ID 2 de usuario de iDRAC7 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

Puede ver las claves cargadas en iDRAC7.

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**.
Aparece la página **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**.
Aparece la página **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 a 16> -d -k <1 a 4>`

- **Todas las claves:** `racadm sshpkauth -i <2 a 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 iDRAC7 y mantener la seguridad del sistema. De manera predeterminada, iDRAC7 está configurado con una cuenta de administrador local. Este nombre de usuario predeterminado es *rooty* y la contraseña es *calvin*. Como administrador, puede configurar cuentas de usuario para permitir a otros usuarios acceder a iDRAC7.

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.

iDRAC7 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 iDRAC7 con permisos de acceso específicos. Antes de crear un usuario de iDRAC7, compruebe si existen usuarios actuales. Puede establecer los nombres de usuario, las contraseñas y los roles con privilegios para estos usuarios. Los nombres de usuario y las contraseñas se pueden cambiar mediante cualquiera de las interfaces seguras de iDRAC7 (es decir, la interfaz web, RACADM o WS-MAN).

Configuración de usuarios locales mediante la interfaz web de iDRAC7

Para agregar y configurar usuarios de iDRAC7 locales:



NOTA: Debe tener el permiso Configurar usuarios para poder crear usuarios en iDRAC7.

1. En la interfaz web de iDRAC7, 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 el ID de usuario y especifique el nombre de usuario, la contraseña y los privilegios de acceso del usuario. Para obtener más información, consulte la *Ayuda en línea de iDRAC7*.

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 iDRAC7 mediante RACADM.

Para configurar varios usuarios de DRAC7 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.
- Crea el archivo de configuración de iDRAC7 y ejecute el subcomando **racadm config** en cada sistema administrado con el mismo archivo de configuración.

Si está configurando un iDRAC7 nuevo o ha utilizado el comando **racadm racresetcfg**, el único usuario actual es el usuario **root** con la contraseña **calvin**. El subcomando **racresetcfg** restablece iDRAC7 a los valores predeterminados.

 **NOTA:** Los usuarios se pueden activar o desactivar con el tiempo. Como resultado, un usuario puede tener un número de índice diferente en cada iDRAC7.


Para verificar si el usuario existe, escriba el comando siguiente en el símbolo del sistema:

```
racadm getconfig -u <nombredeusuario>
```

O bien

Escriba el siguiente comando una vez para cada índice (de 1 a 16):

```
racadm getconfig -g cfgUserAdmin -i <índice>
```

 **NOTA:** También puede escribir **racadm getconfig -f <miarchivo.cfg>** y ver o editar el archivo **miarchivo.cfg**, que incluye todos los parámetros de configuración de iDRAC7.

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

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

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

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

Tenga en cuenta que el objeto **cfgUserAdminIndex** del objeto 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 escribir, no se puede especificar el índice. Un usuario nuevo se agrega al primer índice disponible. Este comportamiento permite una mayor flexibilidad a la hora de configurar varios iDRAC7 con los mismos valores.

Adición de un usuario iDRAC7 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:

- iDRAC7
- LAN
- Puerto serie
- 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 la *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC7 y CMC) disponible en support.dell.com/manuals.

Eliminación de un usuario iDRAC7

Al usar RACADM, los usuarios se debe desactivar manualmente y de manera individual. Los usuarios no se pueden eliminar mediante un archivo de configuración.

Para eliminar un usuario de iDRAC7, la sintaxis de comando es la siguiente:

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i <índice> ""
```

Una cadena nula de dos caracteres de comillas ("") indica al iDRAC7 que debe eliminar la configuración del usuario en el índice especificado y volver a establecer los valores predeterminados originales de fábrica en la configuración del usuario.


Activación del usuario iDRAC7 mediante permisos

Para activar un usuario con permisos administrativos específicos (autoridad basada en roles):

1. Busque un índice de usuario disponible mediante la sintaxis de comando siguiente:



```
racadm getconfig -g cfgUserAdmin -i <índice>
```
2. Escriba los comandos siguientes con el nombre de usuario y la contraseñas nuevos.


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

 **NOTA:** Para obtener una lista de valores de máscara de bits válidos para privilegios de usuario específicos, consulte la *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC y CMC) disponible en support.dell.com/manuals. El valor predeterminado del privilegio es 0, 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 iDRAC7, lo que permite agregar y controlar los privilegios de usuario iDRAC7 para los usuarios existentes en el servicio de directorio. Esta función requiere una licencia.

 **NOTA:** El uso de Active Directory para reconocer usuarios de iDRAC7 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 iDRAC7. 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 iDRAC7 han cambiado de la generación anterior de servidores. Los nombres de rol son los siguientes:

Tabla 11. Roles de iDRAC7

Generación anterior	Generación actual	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
Usuario avanzado	Operador	Inicio de sesión, Configurar, Control del sistema, Acceder a la consola virtual, Acceder a medios virtuales, Operaciones del sistema, Depuración
Usuario invitado	Solo lectura	Inicio de sesión
Ninguna	Ninguna	Ninguna

Tabla 12. Privilegios de usuario iDRAC7

Generación anterior	Generación actual	Descripción
Inicio de sesión en iDRAC	Inicio de sesión	Permite al usuario iniciar sesión en el iDRAC.
Configurar iDRAC	Configurar	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.
Borrar registros	Registros	Permite al usuario solo borrar el registro de sucesos del sistema (SEL).
Ejecutar comandos de control del servidor	Control del sistema	Permite al usuario ejecutar comandos de RACADM.
Redirección de acceso a la consola virtual (para servidores Blade)	Acceder a la consola virtual	Permite al usuario ejecutar la consola virtual.
Acceder a la consola virtual (para servidores tipo bastidor y torre)		
Acceder a los medios virtuales	Acceder a los medios virtuales	Permite al usuario ejecutar y usar los medios virtuales.

Generación anterior	Generación actual	Descripción
Probar alertas	Operaciones del sistema	Permite al usuario enviar alertas de prueba a un usuario específico.
Ejecutar comandos de diagnóstico	Depuración	Permite al usuario ejecutar comandos de diagnóstico.

Enlaces relacionados

[Prerrequisitos del uso de la autenticación de Active Directory para iDRAC7](#)

[Mecanismos de autenticación compatibles de Active Directory](#)

Prerrequisitos del uso de la autenticación de Active Directory para iDRAC7

Para utilizar la función de autenticación de Active Directory de iDRAC7, 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. iDRAC7 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 la Capa de sockets seguros (SSL) en todas las controladoras de dominio a las que se conecta iDRAC7 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 iDRAC7 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 iDRAC7. Para que iDRAC7 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 iDRAC7.
3. Importar el certificado SSL del firmware de iDRAC7.

Enlaces relacionados

[Instalación de un certificado SSL para cada controladora de dominio](#)

[Exportación del certificado de CA raíz de la controladora de dominio a iDRAC7.](#)

[Importación del certificado SSL de firmware de iDRAC7](#)


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 del certificado de CA raíz de la controladora de dominio a iDRAC7.

 **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 iDRAC7.


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 en él con el botón derecho del mouse, 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 iDRAC7.

Importación del certificado SSL de firmware de iDRAC7

El certificado SSL de iDRAC7 es el certificado idéntico que se utiliza para el servidor web iDRAC7. Todas las controladoras iDRAC7 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 iDRAC7 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 iDRAC7 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 iDRAC7 en todas las listas de certificado seguras de la controladora de dominio:

1. Descargue el certificado SSL de iDRAC7 mediante el comando RACADM siguiente:
`racadm sslcertdownload -t 0x1 -f <certificado SSL del RAC>`
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 iDRAC7 en la lista de **Entidades emisoras 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 iDRAC7 se importa a todas las listas de certificado de confianza de controladoras de dominio.

Mecanismos de autenticación compatibles de Active Directory

Puede utilizar Active Directory para definir el acceso de usuario a iDRAC7 mediante dos métodos:

- La solución del *esquema estándar*, que solo utiliza objetos de grupo de Active Directory.
- La solución de *esquema extendido*, que tiene objetos de Active Directory personalizados. Todos los objetos de control de acceso se mantienen en Active Directory. Proporciona una flexibilidad máxima a la hora de configurar el acceso de usuario en distintos iDRAC7 con niveles de privilegios variados.

Enlaces relacionados

[Generalidades del esquema estándar de Active Directory](#)

[Información general sobre el esquema extendido de Active Directory](#)

Generalidades 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 iDRAC7.

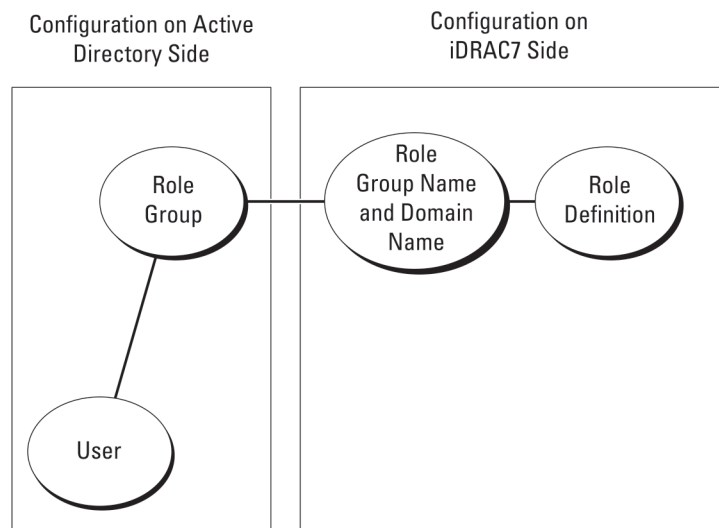



Ilustración 1. Configuración de iDRAC7 con el esquema estándar de Active Directory

En Active Directory, un objeto de grupo estándar se utiliza como grupo de roles. Un usuario con acceso a iDRAC7 es miembro del grupo de roles. Para conceder a este usuario acceso a un iDRAC7 específico, el nombre del grupo de roles y su nombre de dominio deben configurarse en el iDRAC7 específico. El rol y el nivel de privilegios se definen en cada iDRAC7 y no en Active Directory. Puede configurar hasta cinco roles de grupo en cada iDRAC7. En la tabla de referencia se muestran los privilegios predeterminados del grupo de roles.

Tabla 13. Privilegios predeterminados del grupo de roles

Grupos de roles	Nivel predeterminado de privilegios	Permisos otorgados	Máscara de bits
Grupo de roles 1	Ninguna	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	Ninguna	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
Grupo de roles 3	Ninguna	Inicio de sesión en iDRAC	0x00000001
Grupo de roles 4	Ninguna	Sin permisos asignados	0x00000000
Grupo de roles 5	Ninguna	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 iDRAC7. 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 iDRAC7. 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

Para configurar iDRAC7 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 iDRAC7.
3. Configure el nombre del grupo, el nombre del dominio y los privilegios de rol en iDRAC7 mediante la interfaz web de iDRAC7 Web o RACADM.

Enlaces relacionados

[Configuración de Active Directory con el esquema estándar mediante la interfaz web de iDRAC7](#)

[Configuración de Active Directory con esquema estándar vía RACADM](#)

Configuración de Active Directory con el esquema estándar mediante la interfaz web de iDRAC7

 **NOTA:** Para obtener información acerca de los distintos campos, consulte la *Ayuda en línea de iDRAC7*.

1. En la interfaz web de iDRAC7, 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 (AD). Asimismo, especifique el tiempo que iDRAC7 debe esperar para las respuestas de Active Directory durante el proceso de inicio de sesión de iDRAC7.

 **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 iDRAC7 Active Directory con esquema estándar a través de RACADM:


1. En el símbolo del sistema racadm, ejecute los comandos siguientes:

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1
racadm config -g cfgActiveDirectory -o cfgADType 2
racadm config -g cfgStandardSchema -i <índice> -o cfgSSADRoleGroupName
<nombre común del grupo de roles>
racadm config -g cfgStandardSchema -i <índice> -o cfgSSADRoleGroupDomain
<nombre de dominio completamente expresado>
racadm config -g cfgStandardSchema -i <índice> -o cfgSSADRoleGroupPrivilege
<número de la máscara de bits para los permisos del usuario específico>
```


 **NOTA:** Para valores de máscara de bit para permisos de grupo de roles específicos, consulte [Privilegios predeterminados del grupo de roles](#).


```
racadm config -g cfgActiveDirectory -o cfgADDomainController1 <nombre de dominio completo o dirección IP de la controladora de dominio>
racadm config -g cfgActiveDirectory -o cfgADDomainController2 <nombre de dominio completo o dirección IP de la controladora de dominio>
racadm config -g cfgActiveDirectory -o cfgADDomainController3 <nombre de dominio completo o dirección IP de la controladora de dominio>
```

 **NOTA:** Introduzca el FQDN de la controladora de dominio, no el FQDN del dominio. Por ejemplo, introduzca `nombreservidor.dell.com` en lugar de `dell.com`.

 **NOTA:** Al menos una de las tres direcciones se debe configurar. iDRAC7 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.

```
racadm config -g cfgActiveDirectory -o cfgGlobal Catalog1 <nombre de dominio completo o dirección IP de la controladora de dominio>
racadm config -g cfgActiveDirectory -o cfgGlobal Catalog2 <nombre de dominio completo o dirección IP de la controladora de dominio>
racadm config -g cfgActiveDirectory -o cfgGlobal Catalog3 <nombre de dominio completo o dirección IP de la controladora de dominio>
```

 **NOTA:** El servidor de catálogo global solo se requiere para el esquema estándar cuando las cuentas de usuario y los grupos de roles se encuentran en dominios distintos. En el caso de dominio múltiple, solamente se puede usar el grupo universal.

 **NOTA:** La dirección IP o el FQDN que especifique en este campo debe concordar con el campo Sujeto o Nombre alternativo de sujeto del certificado de controladora de dominio si tiene activada la validación de certificados.

Si desea desactivar la validación del certificado durante el protocolo de enlace con SSL, ingrese el siguiente comando de RACADM:

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0
```


En este caso, no es necesario cargar ningún certificado de CA.

Para aplicar la validación de certificado durante el protocolo de enlace SSL (opcional):

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1
```

En este caso, también debe cargar el certificado de CA con el siguiente comando de RACADM:

```
racadm sslcertupload -t 0x2 -f <certificado de CA raíz de ADS>
```

 **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**.

El siguiente comando de RACADM es opcional.

```
racadm sslcertdownload -t 0x1 -f <certificado SSL del RAC>
```

2. Si DHCP está activado en el iDRAC7 y desea utilizar el DNS proporcionado por el servidor DHCP, introduzca los siguientes comandos de RACADM:

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

3. Si el DHCP está desactivado en el iDRAC7 o si desea introducir manualmente la dirección IP de DNS, introduzca los siguientes comandos de RACADM:

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

```
racadm config -g cfgLanNetworking -o cfgDNSServer1 <dirección IP principal de DNS>
```

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

4. Si desea configurar una lista de dominios de usuario para que solamente tenga que introducir el nombre de usuario cuando se inicia sesión en la interfaz web, introduzca el siguiente comando:

```
racadm config -g cfgUserDomain -o cfgUserDomainName <nombre de dominio completo o dirección IP de controladora de dominio> -i <índice>
```

Puede configurar hasta 40 dominios de usuario con números de índice entre 1 y 40.

Información general sobre el 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 son una base de datos distribuidas 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 incluyen el nombre del usuario, sus apellidos, su número de teléfono. etc. Puede extender la base de datos de Active Directory al agregar *atributos* y *clases* únicos propios para satisfacer requisitos específicos. Dell ha extendido el esquema para incluir los cambios necesarios para admitir la autenticación y 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

Información general sobre las extensiones de esquema de iDRAC7

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 más dispositivos iDRAC7. Este modelo proporciona a un administrador la flexibilidad máxima sobre las distintas combinaciones de usuarios, privilegios de iDRAC7 y dispositivos iDRAC7 en la red sin mucha complejidad.

Para cada dispositivo iDRAC7 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 iDRAC7. Puede crear varios objetos de asociación y cada uno de ellos se puede vincular a varios usuarios, grupos de usuarios u objetos de dispositivo iDRAC7, según sea necesario. Los usuarios y los grupos de usuarios de iDRAC7 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 iDRAC7) a un solo objeto de privilegio. Este ejemplo permite al administrador controlar los privilegios de cada usuario sobre dispositivos iDRAC7 específicos.

El objeto del dispositivo iDRAC7 es el vínculo al firmware de iDRAC7 para consultar Active Directory para la autenticación y autorización. Cuando iDRAC7 se agrega a la red, el administrador debe configurar iDRAC7 y su objeto de dispositivo con su nombre de Active Directory de modo que los usuarios pueda realizar la autenticación y autorización con Active Directory. Asimismo, el administrador debe agregar iDRAC7 a al menos 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.

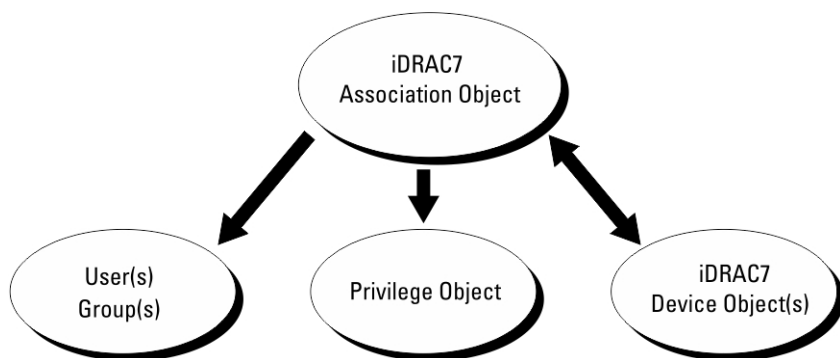


Ilustración 2. Configuración típica de los objetos de Active Directory

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 iDRAC7 para cada dispositivo de iDRAC7 en la red que desee integrar con Active Directory para la autenticación y autorización con iDRAC7.

El objeto de asociación permite el número de usuario o grupos necesario, así como objetos de dispositivo de iDRAC7. 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 iDRAC7.

La extensión de Dell al complemento ADUC MMC solo permite asociar el objeto de privilegio y objetos iDRAC7 desde el mismo dominio con el objeto de asociación. La extensión de Dell no permite que un grupo o un objeto iDRAC7 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 puede 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.

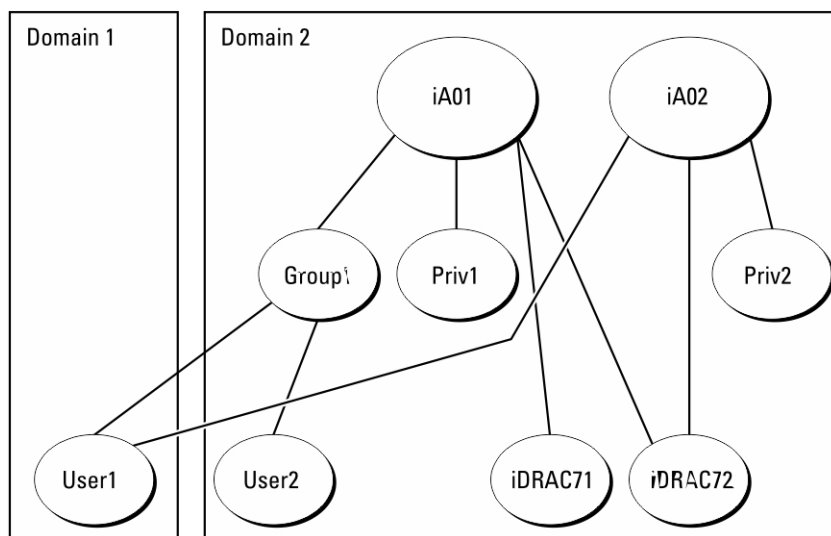


Ilustración 3. Acumulación de privilegios para un usuario

En la figura se muestran dos objetos de asociación (A01 y A02). User1 está asociado a iDRAC72 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 iDRAC72. User1 dispone de privilegios Priv1 en solo iDRAC71. User2 dispone de los privilegios en iDRAC71 y en iDRAC72. 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

Para configurar Active Directory para acceder a iDRAC7:

1. Extienda el esquema de Active Directory.
2. Extienda el complemento Usuarios y equipos de Active Directory.
3. Agregue usuarios iDRAC7 y sus privilegios en Active Directory.
4. Configure las propiedades de Active Directory de iDRAC7 mediante la interfaz web de iDRAC7 o RACADM.

Enlaces relacionados

[Información general sobre el esquema extendido de Active Directory](#)

[Instalación de Dell Extension para el complemento Usuarios y equipos de Active Directory](#)


[Adición de usuarios y privilegios de iDRAC7 a Active Directory](#)


[Configuración de Active Directory con esquema extendido mediante la interfaz web de iDRAC7](#)

[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\OActiveDirectory_Tools\Remote_Management_Advanced\LDIF_Files
- <Unidad DVD >:\SYSMGMT\ManagementStation\support\OActiveDirectory_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 **Terminar**.

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 14. Definiciones de las clases agregadas al esquema de Active Directory

Nombre de la clase	Número de identificación de objeto asignado (OID)
dellDRACDevice	1.2.840.113556.1.8000.1280.1.7.1.1
dellDRACAssociation	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 15. Clase dellRacDevice

OID	1.2.840.113556.1.8000.1280.1.7.1.1
Descripción	Representa el dispositivo Dell iDRAC7. iDRAC7 debe configurarse como dellIDRACDevice en Active Directory. Esta configuración permite a iDRAC enviar solicitudes LDAP a Active Directory.
Tipo de clase	Clase estructural
Superclases	dellProduct
Atributos	dellSchemaVersion dellRacType

Tabla 16. Clase dellIDRACAssociationObject

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

Tabla 17. Clase dellRAC4Privileges

OID	1.2.840.113556.1.8000.1280.1.1.1.3
Descripción	Define los privilegios (Derechos de autorización) para iDRAC7
Tipo de clase	Clase auxiliar
Superclases	Ninguna
Atributos	dellIsLoginUser dellIsCardConfigAdmin dellIsUserConfigAdmin dellIsLogClearAdmin dellIsServerResetUser dellIsConsoleRedirectUser dellIsVirtualMediaUser dellIsTestAlertUser dellIsDebugCommandAdmin

Tabla 18. Clase dellPrivileges

OID	1.2.840.113556.1.8000.1280.1.1.1.4
Descripción	Esta clase se usa como una clase de contenedor para los privilegios de Dell (derechos de autorización).
Tipo de clase	Clase estructural
Superclases	Usuario

OID	1.2.840.113556.1.8000.1280.1.1.1.4
Atributos	dellRAC4Privileges

Tabla 19. Clase dellProduct

OID	1.2.840.113556.1.8000.1280.1.1.1.5
Descripción	La clase principal de la que se derivan todos los productos Dell.
Tipo de clase	Clase estructural
Superclases	Computadora
Atributos	dellAssociationMembers

Tabla 20. Lista de atributos agregados al esquema de Active Directory

Nombre del atributo/Descripción	OID asignado/Identificador de objeto de sintaxis	Con un solo valor
dellPrivilegeMember Lista de los objetos dellPrivilege que pertenecen a este atributo.	1.2.840.113556.1.8000.1280.1.1.2.1 Nombre distintivo (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellProductMembers Lista de objetos dellRacDevice y DelliDRACDevice que pertenecen a este rol. Este atributo es el vínculo de avance al vínculo de retroceso de dellAssociationMembers. Identificación de vínculo: 12070	1.2.840.113556.1.8000.1280.1.1.2.2 Nombre distintivo (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellsLoginUser TRUE si el usuario tiene derechos de inicio de sesión en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.3 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellsCardConfigAdmin TRUE si el usuario tiene derechos de configuración de tarjeta en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.4 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellsUserConfigAdmin TRUE si el usuario tiene derechos de configuración de usuario en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.5 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellsLogClearAdmin TRUE si el usuario tiene derechos de borrado de registro en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.6 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellsServerResetUser TRUE si el usuario tiene derechos de restablecimiento de servidor en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.7 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellsConsoleRedirectUser	1.2.840.113556.1.8000.1280.1.1.2.8	TRUE

Nombre del atributo/Descripción	OID asignado/Identificador de objeto de sintaxis	Con un solo valor
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)	
dellVirtualMediaUser	1.2.840.113556.1.8000.1280.1.1.2.9	TRUE
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)	
dellTestAlertUser	1.2.840.113556.1.8000.1280.1.1.2.10	TRUE
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)	
dellDebugCommandAdmin	1.2.840.113556.1.8000.1280.1.1.2.11	TRUE
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)	
dellSchemaVersion	1.2.840.113556.1.8000.1280.1.1.2.12	TRUE
La versión del esquema actual se usa para actualizar el esquema.	Cadena de no distinguir mayúsculas de minúsculas (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	
dellRacType	1.2.840.113556.1.8000.1280.1.1.2.13	TRUE
Este atributo es el tipo de RAC actual para el objeto dellIDRACDevice y el vínculo de retroceso al vínculo de avance de dellAssociationObjectMembers.	Cadena de no distinguir mayúsculas de minúsculas (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	
dellAssociationMembers	1.2.840.113556.1.8000.1280.1.1.2.14	FALSE
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	Nombre distintivo (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	

Instalación de Dell Extension para el complemento Usuarios y equipos de Active Directory

Cuando se extiende el esquema en Active Directory, también debe extenderse el complemento Usuarios y equipos de Active Directory para que el administrador pueda administrar los dispositivos iDRAC7, los usuarios y los grupos de usuarios, y las asociaciones y privilegios de iDRAC7.

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.

Adición de usuarios y privilegios de iDRAC7 a Active Directory

Mediante el Complemento Usuarios y equipos de Active Directory extendido de Dell, puede agregar usuarios y privilegios de iDRAC7 creando objetos de dispositivo, asociación y privilegios. Para agregar cada objeto, realice los pasos siguientes:

- Cree un objeto de dispositivo iDRAC7
- 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 iDRAC7](#)

[Creación de un objeto de privilegio](#)

[Creación de un objeto de asociación](#)


Creación de un objeto de dispositivo de iDRAC7

Para crear un objeto de dispositivo de iDRAC7:

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 iDRAC7 que introduce al configurar las propiedades de Active Directory mediante la interfaz web de iDRAC7.
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 iDRAC7 se deriva de un grupo y su alcance está establecido en Local de dominio.

1. En la ventana **Raíz de consola** (MMC), haga clic con el botón derecho del mouse en un contenedor.
2. Seleccione **Nuevo** → **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 **Usuarios autenticados**, 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 iDRAC7 o grupos de dispositivos iDRAC7.

Puede agregar grupos de usuarios y dispositivos de iDRAC7.

Enlaces relacionados

[Adición de usuarios o grupos de usuarios](#)

[Adición de privilegios](#)

[Adición de dispositivos iDRAC7 o grupos de dispositivos iDRAC7](#)

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 de usuario y grupo de usuarios al autenticar un dispositivo iDRAC7. A un objeto de asociación solo se puede agregar un objeto de privilegio.

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 de usuario y grupo de usuarios al autenticar un dispositivo iDRAC7. A un objeto de asociación solo se puede agregar un objeto de privilegio.

Adición de dispositivos iDRAC7 o grupos de dispositivos iDRAC7


Para agregar dispositivos iDRAC7 o grupos de dispositivos iDRAC7

1. Seleccione la ficha **Productos** y haga clic en **Agregar**.
2. Introduzca el nombre de los dispositivos iDRAC7 o de los grupos de dispositivos iDRAC7 y haga clic en **Aceptar**.


3. En la ventana **Propiedades**, haga clic en **Aplicar** y en **Aceptar**.
4. Haga clic en la ficha **Productos** para agregar un dispositivo iDRAC7 conectado a la red que está disponible para los usuarios o los grupos de usuarios definidos. Puede agregar varios dispositivos iDRAC7 a un objeto de asociación.

Configuración de Active Directory con esquema extendido mediante la interfaz web de iDRAC7

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 iDRAC7*.

1. En la interfaz web de iDRAC7, 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 utilizó durante la iniciación de las conexiones SSL al comunicarse con el servidor de Active Directory (AD).
4. Haga clic en **Siguiente**.
Aparece la página **Paso 2 de 4 de Configuración y administración de Active Directory**.
5. Especifique la información de ubicación acerca de los servidores y las cuentas de usuario de Active Directory (AD). Asimismo, especifique el tiempo que iDRAC7 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 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 extendido** y haga clic en **Siguiente**.
Aparece la página **Paso 4 de 4 de Configuración y administración de Active Directory**.
8. Introduzca el nombre y la ubicación del objeto de dispositivo de iDRAC7 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:


1. Abra un símbolo del sistema e introduzca los siguientes comandos de RACADM:


```
racadm config -g cfgActiveDirectory -o cfgADEnable 1
racadm config -g cfgActiveDirectory -o cfgADType 1
racadm config -g cfgActiveDirectory -o cfgADRacName <nombre común de RAC>
racadm config -g cfgActiveDirectory -o cfgADRacDomain <nombre completo del dominio del RAC>
racadm config -g cfgActiveDirectory -o cfgADDomainController1 <nombre de dominio completo o dirección IP de la controladora de dominio>
racadm config -g cfgActiveDirectory -o cfgADDomainController2 <nombre de dominio completo o dirección IP de la controladora de dominio>
racadm config -g cfgActiveDirectory -o cfgADDomainController3 <nombre de dominio completo o dirección IP de la controladora de dominio>
```

 **NOTA:** Debe configurar al menos una de las tres direcciones. iDRAC7 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 iDRAC7.

Para desactivar la validación de certificado durante el protocolo de enlace SSL (opcional):

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0
```


 **NOTA:** En este caso, no tiene que cargar un certificado de CA.

Para aplicar la validación de certificado durante el protocolo de enlace SSL (opcional):

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1
```

En este caso, debe cargar un certificado de CA.

```
racadm sslcertupload -t 0x2 -f <certificado CA raíz de ADS>
```

 **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 bajo **Información general** → **Configuración de iDRAC** → **Red**.

El siguiente comando de RACADM es opcional:

```
racadm sslcertdownload -t 0x1 -f <certificado SSL del RAC>
```

2. Si DHCP está activado en el iDRAC7 y desea utilizar el DNS proporcionado por el servidor DHCP, introduzca el siguiente comando de RACADM:
3. Si DHCP está desactivado en iDRAC7 o si desea introducir manualmente la dirección IP de DNS, introduzca los siguientes comandos de RACADM:

```
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0
racadm config -g cfgLanNetworking -o cfgDNSServer1 <dirección IP principal de DNS>
racadm config -g cfgLanNetworking -o cfgDNSServer2 <dirección IP secundaria del DNS>
```
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 iDRAC7, introduzca el siguiente comando:

```
racadm config -g cfgUserDomain -o cfgUserDomainName <nombre de dominio completo o dirección IP de la controladora de dominio> -i <índice>
```

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 iDRAC7

Para probar la configuración de Active Directory:

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

Configuración de los usuarios LDAP genéricos

iDRAC7 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 iDRAC7 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 iDRAC7.

 **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 web de iDRAC7](#)

[Configuración del servicio de directorio LDAP genérico mediante RACADM](#)

Configuración del servicio de directorio de LDAP genérico mediante la interfaz web de iDRAC7


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 iDRAC7*.


1. En la interfaz web de iDRAC7, 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 en los grupos RACADM **cfgLdap** y **cfgLdapRoleGroup**. Para obtener más información, consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC) disponible en support.dell.com/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 iDRAC7


Para probar la configuración del servicio de directorio LDAP:


1. En la interfaz web de iDRAC7, 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 **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, iDRAC7 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 iDRAC7 no puede comunicarse con el servidor LDAP.

 **NOTA:** Cuando está habilitado LDAP genérico, iDRAC7 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 *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC) disponible en support.dell.com/manuals.

Configuración de iDRAC7 para inicio de sesión único o inicio de sesión mediante tarjeta inteligente

En esta sección se proporciona información para configurar iDRAC7 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.

iDRAC7 admite la autenticación de Active Directory basado 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 iDRAC7 para usuarios de Active Directory](#)

[Configuración del inicio de sesión mediante tarjeta inteligente de iDRAC7 para usuarios locales](#)

[Configuración del inicio de sesión mediante tarjeta inteligente de iDRAC7 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 iDRAC7 con la hora de la controladora de dominio de Active Directory. De lo contrario, fallará la autenticación kerberos en iDRAC7. El valor de desvío es en minutos desde la hora de iDRAC time (UTC) hasta la hora de la controladora de dominio (por ejemplo, -360 para la zona horaria Hora central). Se permite una diferencia de hora máxima de cinco minutos. Después de sincronizar la hora del servidor con la hora de la controladora de dominio, **restablezca (reinicie)** iDRAC7.

También puede utilizar el siguiente comando de diferencia de zona horaria de RACADM para sincronizar la hora:


```
racadm config -g cfgRacTuning -o
cfgRacTuneTimeZoneOffset <valor de desvío>
```

Si la hora de verano está vigente, utilice el comando siguiente:

```
cfgRacTuneDaylightOffset <valor de desvío>
```

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

- Registre el iDRAC7 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 iDRAC7.

 **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 iDRAC7 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 iDRAC7 como equipo en el dominio raíz de Active Directory

Para registrar iDRAC7 en el dominio raíz de Active Directory:

- Haga clic en **Información general** → **Configuración de iDRAC** → **Red** → **Red**. Aparecerá la página **Red**.
- Proporcione 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.
- Seleccione **Registrar el iDRAC en DNS**.
- Indique un **nombre de dominio DNS** válido.
- 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 iDRAC7*.

Generación del archivo Keytab de Kerberos

Para compatibilidad con la autenticación de inicio de sesión mediante SSO y tarjeta inteligente, iDRAC7 permite que la configuración se active como un servicio Kerberos en una red de Windows Kerberos. La configuración de Kerberos en iDRAC7 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 iDRAC7 DNS al que cargará el archivo keytab generado.

Para generar un archivo keytab mediante la herramienta *ktpass*:

- Ejecute la utilidad *ktpass* en la controladora de dominio (servidor de Active Directory) donde desee asignar el iDRAC7 a una cuenta de usuario en Active Directory.
- 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 DES-CBC-MD5 -ptype  
KRB5_NT_PRINCIPAL -pass [password] +DesOnly -out c:\krbkeytab
```


El tipo de cifrado es DES-CBC-MD5. El tipo de elemento 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 opción Utilizar tipos de cifrado DES para esta propiedad de cuenta.

 **NOTA:** Utilice letras en minúsculas para **iDRAC7name** 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/iDRAC7name.domainname.com username
```

Se genera un nuevo archivo keytab.

 **NOTA:** Si encuentra problemas con el usuario de iDRAC7 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

[Adición de usuarios y privilegios de iDRAC7 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.

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 iDRAC7 y que forman parte de la configuración del SSO (por ejemplo: **mihost.ejemplo.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 iDRAC7 a `network.negotiate-auth.trusted-uris` (usando lista de valores separados por coma).

4. Agregue el nombre de iDRAC7 a network.negotiate-auth.delegation-uris (usando lista de valores separados por coma).

Configuración del inicio de sesión SSO de iDRAC7 para usuarios de Active Directory

Antes de configurar iDRAC7 para el inicio de sesión SSO de Active Directory, asegúrese de satisfacer todos los requisitos.


Puede configurar iDRAC7 para SSO de Active Directory cuando configura una cuenta de usuario basada en Active Directory.

Enlaces relacionados

- [Prerrequisitos 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 iDRAC7](#)
- [Configuración de Active Directory con esquema estándar vía RACADM](#)
- [Configuración de Active Directory con esquema extendido mediante la interfaz web de iDRAC7](#)
- [Configuración de Active Directory con esquema extendido mediante RACADM](#)

Configuración del inicio de sesión SSO de iDRAC7 para usuarios de Active Directory mediante la interfaz web

Para configurar iDRAC7 para un inicio de sesión SSO de Active Directory:

 **NOTA:** Para obtener más información acerca de estas opciones, consulte la *Ayuda en línea de iDRAC7*.

1. Verifique si el nombre DNS de iDRAC7 coincide con el nombre de dominio completo de iDRAC7. Para ello, en la interfaz web de iDRAC7, 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 iDRAC7 para usuarios de Active Directory mediante RACADM

Además de los pasos que se realizan durante la configuración de Active Directory, para activar SSO debe ejecutar el comando siguiente:

```
racadm -g cfgActiveDirectory -o cfgADSSOEnable 1
```

Configuración del inicio de sesión mediante tarjeta inteligente de iDRAC7 para usuarios locales

Para configurar el usuario local de iDRAC7 para inicio de sesión mediante tarjeta inteligente:

1. Cargue el certificado de usuario de tarjeta inteligente y el certificado de CA de confianza en iDRAC7.
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.

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 iDRAC7, vaya a **Información general** → **Configuración de iDRAC** → **Red** → **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.
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 del servidor de tarjeta inteligente, utilice el comando `usercertupload`. Para obtener más información, consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC) disponible en support.dell.com/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 iDRAC7, vaya a **Información general** → **Configuración de iDRAC** → **Red** → **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.
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 la *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC) disponible en support.dell.com/manuals.

Configuración del inicio de sesión mediante tarjeta inteligente de iDRAC7 para usuarios de Active Directory

Antes de configurar el inicio de sesión mediante tarjeta inteligente de iDRAC7 para los usuarios de Active Directory, asegúrese de haber cumplido los prerequisites necesarios.

Para configurar el inicio de sesión mediante tarjeta inteligente de iDRAC7:

1. En la interfaz web de iDRAC7, 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 iDRAC7*.

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 iDRAC7](#)

[Configuración de Active Directory con esquema estándar vía RACADM](#)

[Configuración de Active Directory con esquema extendido mediante la interfaz web de iDRAC7](#)

[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 iDRAC7, asegúrese de haber realizado lo siguiente:

- Configurar los permisos iDRAC7.
- Completar la configuración de usuario local de iDRAC7 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 iDRAC7 para usuarios de Active Directory](#)

[Configuración del inicio de sesión mediante tarjeta inteligente de iDRAC7 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 iDRAC7, vaya a **Información 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 iDRAC7*.

3. Haga clic en **Aplicar** para aplicar los cambios.

Se le solicitará un inicio de sesión mediante tarjeta inteligente durante todos los intentos de inicio de sesión subsiguientes mediante la interfaz web de iDRAC7.

Activación o desactivación del inicio de sesión mediante tarjeta inteligente utilizando RACADM

Para activar el inicio de sesión mediante tarjeta inteligente, utilice los objetos **cfgSmartCardLogonEnable** y **cfgSmartCardCRLEnable**. Para obtener más información, consulte la *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC) disponible en support.dell.com/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 iDRAC7 para enviar alertas

Puede establecer alertas y acciones para determinados sucesos que se produce 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 ha configurado este último para generar una alerta (por correo electrónico, captura SNMP o alerta IPMI), se envía una alerta a uno o más destinos configurados. Si el mismo filtro de suceso también está configurado para realizar una acción (tal como un reinicio, un ciclo de encendido o un apagado del sistema), la acción se llevará a cabo. Puede configurar una sola acción para cada suceso.

Para configurar de iDRAC7 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 la alerta por correo electrónico, la alerta IPMI o la captura SNMP.
4. Active las alertas y las acciones de suceso, como por ejemplo:
 - Enviar una alerta por correo electrónico, una alerta IPMI o capturas SNMP a los destinos configurados.
 - Realizar 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 la captura SNMP o IPMI para alertas por correo electrónico](#)

[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 la captura SNMP o IPMI para alertas por correo electrónico](#)

Activación o desactivación de alertas mediante la interfaz web

Para activar o desactivar la generación de alertas:

1. En la interfaz web de iDRAC7, vaya a **Información 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 suceso:

```
racadm config -g cfgIpmiLan -o cfgIpmiLanAlertEnable 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 la captura SNMP o IPMI para alertas por correo electrónico](#)

Filtrado de alertas mediante la interfaz web de iDRAC7

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 iDRAC7, vaya a **Información 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
 - En almacenamiento
 - Configuración
 - Auditorías
 - Actualizaciones
 - Notas de trabajo
3. Seleccione uno o más de los niveles de gravedad siguientes:
 - Información
 - Aviso
 - Crítico
4. Haga clic en **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 *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC) disponible en support.dell.com/manuals.

Configuración de alertas de suceso

Puede establecer alertas de suceso, tales como alertas por correo electrónico, alertas IPMI y alertas SNMP para su envío a destinos configurados.

Enlaces relacionados

[Activación o desactivación de alertas](#)

[Configuración de la captura SNMP o IPMI para alertas por correo electrónico](#)

[Filtrado de alertas](#)

Configuración de alertas de suceso mediante la interfaz web

Para establecer una alerta de suceso mediante la interfaz web:

1. Asegúrese de haber configurado los valores de alerta por correo electrónico, alerta IPMI y captura SNMP.
2. Vaya a **Información general** → **Servidor** → **Alertas**.
Aparecerá la página **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
4. Haga clic en **Aplicar**.
La configuración se guarda.
5. Bajo la sección **Alertas**, seleccione la opción **Activar** para enviar alertas a los destinos configurados.

Configuración de alertas de suceso mediante RACADM

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

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 iDRAC7, vaya a **Información general** → **Servidor** → **Alertas** . Aparecerá la página **Alertas**.
2. Bajo **Resultados de alertas**, en el menú desplegable **Acciones**, seleccione una acción para cada suceso:
 - Reiniciar
 - Ciclo de encendido
 - Apagado
 - Sin acción
3. Haga clic en **Aplicar**.
La configuración se guarda.

Configuración de acciones del suceso mediante RACADM

Para configurar una acción de suceso, utilice el objeto `cfgIpmiPefAction` o el comando `eventfilters`. Para obtener más información, consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC) disponible en support.dell.com/manuals.

Configuración de la captura SNMP o IPMI para alertas por correo electrónico

La estación de administración utiliza capturas de protocolo simple de administración de red (SNMP) e interfaz de administración de plataforma inteligente (IPMI) para recibir datos de iDRAC7. Para los sistemas con un gran número de nodos, es posible que no sea suficiente que una estación de administración sondee cada iDRAC7 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.

Puede configurar los destinos de alerta IPv4 e IPv6, valores de correo electrónico y valores del servidor SMTP y luego probar la configuración.

Antes de configurar los valores de correo electrónico, SNMP o capturas 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 alerta por correo electrónico](#)


Configuración de destinos de alerta IP

Puede configurar las direcciones IPv6 o IPv4 para recibir las alertas IPMI o las capturas SNMP.

Configuración de destinos de alerta IP mediante la interfaz web

Para configurar los valores de destino de alerta IPv4 o IPv6 mediante la interfaz web:

1. Vaya a **Información general** → **Servidor** → **Alertas** → **Configuración SNMP y de correo electrónico**.
2. Seleccione la opción **Estado** para activar la dirección IP y recibir las capturas e introduzca las direcciones IPv4 e IPv6. Puede especificar hasta cuatro direcciones de destino IPv4 y cuatro direcciones de destino IPv6. Para obtener más información acerca de las opciones, consulte la *Ayuda en línea de iDRAC7*.
3. Introduzca la cadena de comunidad SNMP de iDRAC7. Para obtener más información acerca de las opciones, consulte la *Ayuda en línea de iDRAC7*.

 **NOTA:** El valor de cadena de comunidad indica la cadena de comunidad que se debe utilizar como una captura de alerta SNMP enviada desde iDRAC7. Asegúrese de que la cadena de comunidad de destino sea igual a la de iDRAC7. el valor predeterminado es Público.

4. 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.
5. Haga clic en **Aplicar**. Se configuran los destinos de alerta.

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 (índice) (0|1)
```

- Dirección IPv6:

```
racadm config -g cfgIpmiPetIpv6 -o cfgIpmiPetIpv6AlertEnable -i (índice) (0|1)
```

donde, (índice) 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 [índice] [dirección IP]
```

donde [índice] es el índice del destino de la captura de y [dirección_IP] 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 [nombre]
```

donde [nombre] es el nombre de comunidad SNMP.

4. Para probar la captura, si fuera necesario:

```
racadm testtrap -i [índice]
```

donde [índice] es el índice del destino de captura que se debe probar.

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

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

Puede configurar solamente los destinos de alerta IPv4 mediante la utilidad de configuración de iDRAC. Para ello, realice lo siguiente:



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 IPv4 de destino. Puede especificar hasta cuatro direcciones IPv4.
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 configuran los destinos de alerta IPv4.

Configuración de los valores de alerta por correo electrónico

Puede configurar la dirección de correo electrónico para recibir alertas por correo electrónico. También deberá configurar los valores de dirección del servidor SMTP.

-  **NOTA:** Si el servidor de correo es Microsoft Exchange Server 2007, compruebe que el nombre de dominio de iDRAC7 está configurado para que el servidor de correo reciba alertas por correo electrónico desde iDRAC7.
-  **NOTA:** Las alertas por correo electrónico admiten direcciones IPv4 e IPv6. El nombre de dominio DNS de DRAC se debe especificar mediante IPv6.

Enlaces relacionados

[Configuración de los valores de dirección de 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 **Información general** → **Servidor** → **Alertas** → **Configuración SNMP y de correo electrónico**.
2. Seleccione la opción **Estado** para activar la dirección de correo electrónico para recibir las alertas y escriba una dirección de correo electrónico válida. Para obtener más información sobre las opciones disponibles, consulte la *Ayuda en línea de iDRAC7*.
3. Haga clic en **Enviar** bajo **Correo electrónico de prueba** para probar la configuración de alerta por correo electrónico.
4. Haga clic en **Aplicar**.

Configuración de los valores de alerta por correo electrónico mediante RACADM

Para configurar los valores de alerta por correo electrónico, siga los pasos siguientes:

1. Para activar una alerta por correo electrónico:

```
racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i [índice] [0|1]
```

donde [índice] es el índice del destino de correo electrónico y 0 desactiva la alerta por correo electrónico o 1 activa la alerta.

El índice de destino de correo electrónico puede ser un valor de 1 a 4. Por ejemplo, para activar el correo electrónico con índice 4, ejecute el comando siguiente:

```
racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 4 1
```

2. Para configurar los valores de correo electrónico:

```
racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 [dirección_de_correo_electrónico]
```

donde 1 es el índice del destino de correo electrónico y [dirección_de_correo_electrónico] es la dirección de correo electrónico de destino que recibe las alertas de sucesos de plataforma.

3. Para configurar un mensaje personalizado:

```
racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i [índice]
[mensaje_personalizado]
```

donde [índice] es el índice del destino de correo electrónico y [mensaje_personalizado] es el mensaje personalizado.

4. Para probar la alerta por correo electrónico, si fuera necesario:

```
racadm testemail -i [índice]
```

donde [índice] es el índice del destino de correo electrónico que se debe probar.

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

Configuración de los valores de dirección de servidor de correo electrónico SMTP

Debe configurar la dirección de servidor SMTP para las alertas por correo electrónico de modo que se envíen a destinos específicos.

Configuración de los valores de dirección de servidor de correo electrónico SMTP mediante la interfaz web de iDRAC7

Para configurar la dirección del servidor SMTP:

1. En la interfaz web de iDRAC7, vaya a **Información general** → **Servidor** → **Alertas** → **Configuración SNMP y de correo electrónico**.
2. Seleccione la opción **Activar autenticación**, especifique el nombre de usuario y la contraseña (del usuario que tiene acceso al servidor SMTP) e introduzca una dirección IP válida o un nombre de dominio calificado (FQDN) del servidor SMTP que se debe utilizar en la configuración.

Para obtener más información acerca de estas opciones, consulte la *Ayuda en línea de iDRAC7*.

3. Haga clic en **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 SMTP de correo electrónico, ejecute el comando siguiente:

```
racadm config -g cfgRemoteHosts -o cfgRhostsSmtServerIpAddr <dirección IP del
servidor SMTP de correo electrónico>
```

ID de mensaje de alertas

En la tabla siguiente se proporciona la lista de ID de mensaje que se muestran para las alertas.

Tabla 21. ID de mensaje de alertas

ID de mensaje	Descripción
AMP	Amperaje
ASR	Restablecimiento automático del sistema
BAR	Copia de seguridad/restauración
BAT	Suceso de la batería
BIOS	Administración del BIOS
BOOT	Control BOOT
CBL	Cable

ID de mensaje	Descripción
CPU	Procesador
CPUA	Procesador ausente
CTL	Controladora de almacenamiento
DH	Administración de certificados
DIS	Descubrimiento automático
ENC	Gabinete de almacenamiento
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 del vínculo
LOG	Suceso del registro
MEM	Memoria
NDR	Controlador de SO de NIC
NIC	Configuración de NIC
OSD	Implementación de sistema operativo
OSE	Suceso del sistema operativo
PCI	Dispositivo PCI
PDR	Disco físico
PR	Intercambio de piezas
PST	POST del BIOS
PSU	Fuente de alimentación
PSUA	PSU ausente
PWR	Uso de alimentación
RAC	Suceso RAC
RDU	Redundancia
RED	Descarga de firmware
RFL	Medios IDSDM
RFLA	IDSDM ausente
RFM	SD de dirección flexible
RRDU	Redundancia IDSDM
RSI	Servicio remoto
SEC	Suceso de seguridad

ID de mensaje	Descripción
SEL	Registro de sucesos del sistema
SRD	RAID de software
SSD	SSD PCIe
STOR	En 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	Voltaje
VME	Medios virtuales
VRM	Consola virtual
WRK	Nota de trabajo

Administración de registros

iDRAC7 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 iDRAC7, 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](#)

[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 iDRAC7 vaya a la ficha **Información 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 iDRAC7*.

Haga clic en **Guardar como** para guardar el **registro de sucesos del sistema** en el directorio de su elección.



NOTA: Si al usar Internet Explorer tiene un problema para guardar, asegúrese de descargar la actualización de seguridad acumulada para Internet Explorer que se encuentra en el sitio web de asistencia de Microsoft en support.microsoft.com.

Visualización del registro de sucesos del sistema mediante RACADM

Para ver el SEL:

```
racadm getsel <opciones>
```

Si no se especifican argumentos, se muestra todo el registro.

Para mostrar el número de entradas de SEL:

```
racadm getsel -i
```

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

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

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 resultados del registro de Lifecycle](#)

[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 **Información 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 iDRAC7*.

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 **Nivel de estado**.
 - Introduzca una palabra clave.
 - Especifique el intervalo de fechas.

2. Haga clic en **Aplicar**.

Las entradas filtradas del registro se muestran en **Resultados del registro**.

Exportación de los resultados del registro de Lifecycle

Para exportar los resultados del **Registro de Lifecycle**, en la sección **Resultados del registro**, haga clic en **Exportar**. Aparecerá un cuadro de diálogo que permite guardar las entradas del registro en formato XML en la ubicación deseada.

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

Adición de notas de trabajo

Todos los usuarios que inician sesión en iDRAC7 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 iDRAC7 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 iDRAC7, vaya a **Información 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 iDRAC7*.

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 iDRAC7 y el sistema remoto.
- El sistema remoto e iDRAC7 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 iDRAC7, vaya a **Información 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 iDRAC7*.
3. Haga clic en **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 de servidor de syslog remoto, utilice los objetos RACADM siguientes:

- `cfgRhostsSyslogEnable`
- `cfgRhostsSyslogPort`
- `cfgRhostsSyslogServer1`
- `cfgRhostsSyslogServer2`
- `cfgRhostsSyslogServer3`

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

Supervisión y administración de la alimentación

Puede utilizar iDRAC7 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, repuesto dinámico y 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](#)

Supervisión de la alimentación

iDRAC7 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 iDRAC7 vaya a **Información general** → **Servidor** → **Alimentación/Térmico** → **Supervisión de alimentación**. Se muestra la página **Supervisión de alimentación**. Para obtener más información, consulte la *Ayuda en línea de iDRAC7*.

Supervisión de la alimentación mediante RACADM

Para ver la información de supervisión de la alimentación, utilice los objetos del grupo **System.Power** con el comando **get** o el objeto **cfgServerPower** con el comando **getConfig**. Para obtener más información, consulte la *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC) disponible en support.dell.com/manuals.

Ejecución de las operaciones de control de alimentación

iDRAC7 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 la *Lifecycle Controller Remote Services User's Guide* (Guía del usuario de Dell Lifecycle Controller Remote Services) disponible en support.dell.com/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 iDRAC7, vaya a **Información general** → **Servidor** → **Alimentación/Térmico** → **Configuración de la alimentación** → **Control de alimentación**. Aparece 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 iDRAC7*.

Ejecución de las operaciones de control de alimentación mediante RACADM

Para realizar acciones de control de alimentación, utilice el comando **serveraction**. Para obtener más información, consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC) disponible en support.dell.com/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, iDRAC7 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 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 iDRAC7 solicite un aumento del consumo de alimentación potencial máximo, por lo que aumentará el intervalo de alimentación. iDRAC7 solo aumenta su solicitud de consumo de alimentación potencial máximo a CMC. No solicita una alimentación potencial menor si el consumo disminuye. iDRAC7 sigue solicitando más alimentación y el consumo de alimentación supera la alimentación que asigne CMC.

Una vez que el sistema esté encendido e inicializado, iDRAC7 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 hay suficiente alimentación asignada, el servidor Blade no se enciende. Si al servidor Blade se le ha asignado alimentación suficiente, iDRAC7 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 cercado al umbral especificado.

El consumo de alimentación real puede ser inferior para cargas de trabajo ligeros 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 iDRAC7 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 cercado. 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 iDRAC7, vaya a **Información general** → **Servidor** → **Alimentación/Térmico** → **Configuración de la alimentación** → **Configuración de la alimentación**. Aparece 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 la *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC) disponible en support.dell.com/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 alimentación**.
Se muestra la página **Configuración de alimentación de la configuración de iDRAC**.
2. Seleccione **Activado** para activar la opción **Política de límite de alimentación de iDRAC**. De lo contrario, seleccione **Desactivado**.
3. Utilice los valores recomendados o, bajo **Límites definidos 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, deberá establecer la PSU principal (que debe estar encendido). En un sistema de cuatro PSU, deberá establecer un par de PSU (1+1 o 2+2) que deben estar encendidos.

Después de que se active el repuesto dinámico, las PSU pueden activarse o permanecer inactivas según la carga.

El factor de alimentación es la relación de alimentación real consumida y la alimentación aparente. Si se desactiva la corrección del factor de alimentación, el consumo de alimentación se reduce cuando se apague el servidor. De manera predeterminada, la corrección de factor de alimentación se activa cuando se encienda el sistema.

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 iDRAC7, vaya a **Información general** → **Servidor** → **Alimentación/Térmico** → **Configuración de la alimentación** → **Configuración de la alimentación**. Aparece la página **Control de alimentación**.
2. En **Opciones de suministro de energía**, seleccione las opciones necesarias. Para obtener más información, consulte la *Ayuda en línea de iDRAC7*.
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 la *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC) disponible en support.dell.com/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**. Se muestra la página **Configuración de la alimentación de la configuración de iDRAC**.
2. Bajo 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 **Configuración de seguridad**. Se muestra la página **Configuración de seguridad de la configuración de iDRAC**.
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

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 cuatro 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 utilizar 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 22. 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 Linux, es posible que una consola X11 no pueda visualizarse en el monitor local. Presione <Ctrl><Alt><F1> en la consola virtual de iDRAC7 para cambiar Linux a una consola de texto.

Configuración de exploradores web para utilizar la consola virtual


Para utilizar la consola virtual en la estación de administración:

1. Asegúrese de que esté instalada una versión compatible de Internet Explorer (Windows) o Mozilla Firefox (Windows o Linux).
Para obtener más información acerca de las versiones de explorador compatibles para Windows y Linux, consulte el archivo Léame.
2. 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.
3. Si la consola virtual y los medios virtuales están configurados para utilizar el complemento Java, deberá desactivar la opción *Modo de seguridad mejorado* en Internet Explorer. Si esto no es posible, en iDRAC7, configure la consola virtual para utilizar el complemento ActiveX. Debe activar el control ActiveX en IE, agregar el URL web de iDRAC7 a la zona de seguridad de Intranet y establezca el nivel de seguridad para esta zona en *Medio-bajo* para que la consola virtual y los medios virtuales funcionen correctamente.

 **NOTA:** En sistemas operativos Windows Server, puede acceder a la configuración de seguridad mejorada de IE en la ventana **Panel de control** → **Herramientas administrativas Administrador de servidores** → **Configuración de seguridad mejorada de Internet Explorer**. También puede establecer los privilegios necesarios en esta ventana.

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.

Enlaces relacionados


[Configuración de exploradores web para utilizar el complemento Java](#)

[Configuración de IE para utilizar el complemento ActiveX](#)

[Importación de certificados de CA a Management Station](#)

Configuración de exploradores web para utilizar 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 utilizar el complemento ActiveX


El complemento ActiveX solo se puede utilizar con Internet Explorer.

Para configurar IE para utilizar el complemento ActiveX:

1. Borre la memoria caché del explorador.
2. Agregue la dirección IP o el nombre de host de iDRAC7 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 active las extensiones de explorador de terceros. Para ello, vaya a **Herramientas** → **Opciones de Internet** → **Opciones avanzadas**, desactive la opción **No guardar páginas cifradas en disco** y seleccione la opción **Habilitar las 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 **Activar** 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:** 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 iDRAC7 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 iDRAC7 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 muestra 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 muestra la ventana **Administrar complementos**.
3. Seleccione **Todos los complementos** del 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 iDRAC7*.

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 cierra 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.

Puede configurar la consola virtual mediante la interfaz web de iDRAC7 o la interfaz de línea de comandos RACADM.

Enlaces relacionados

[Configuración de exploradores web para utilizar 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 iDRAC7:

1. Vaya a **Información general** → **Servidor** → **Consola**. 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 iDRAC7*.
3. Haga clic en **Aplicar**. Se configura la consola virtual.

Configuración de la consola virtual mediante RACADM

Para configurar la consola virtual, utilice los objetos siguientes:

- `cfgRACTuneConRedirEnable`

- cfgRACTuneConRedirPort
- cfgRACTuneConRedirEncryptEnable
- cfgRacTunePluginType
- cfgRacTuneVirtualConsoleAuthorizeMultipleSessions

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

Puede iniciar la consola virtual mediante la interfaz web de iDRAC7 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.

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 "Error de certificado: navegación bloqueada". 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 utilizar el complemento Java](#)

[Configuración de IE para utilizar el complemento ActiveX](#)

[Inicio de la consola virtual mediante la interfaz web](#)

[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 **Información general** → **Servidor** → **Consola**. Aparece la página **Consola virtual**. Haga clic en **Iniciar la consola virtual**. Se inicia el **Visor de la consola virtual**.
- Vaya a **Información 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 en la ventana del visor aparezcan dos punteros del mouse, uno para el servidor administrado y el otro para la estación de administración. Si los cursores no se sincronizan, seleccione **Cursor sencillo** del menú **Herramientas** del visor de la consola virtual.


Si se inicia la consola virtual desde una estación de administración con Windows Vista, es posible que se reinicien los mensajes de la consola virtual. Para evitarlo, 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 el siguiente URL en minúsculas: **https://iDRAC7_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.

Uso del visor de la consola virtual

El visor de la consola virtual proporciona distintos controles, tal como la sincronización del mouse, opciones de chat, macros de teclado, acciones de alimentación y acceso a los medios virtuales. Para obtener más información, consulte la *Ayuda en línea de iDRAC7*.

 **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 del iDRAC7 al que está conectado desde la estación de administración. Si iDRAC7 no tiene nombre DNS, se mostrará la dirección IP. El formato es el siguiente:

- **Servidores tipo bastidor y torre:**
<Nombre DNS / Dirección IPv6 / Dirección IPv4>, <Modelo>, User: <nombre de usuario>, <fps>
- **Servidores Blade:**
<Nombre DNS / Dirección IPv6 / Dirección IPv4>, <Modelo>, <Nombre de ranura>, User: <nombre de usuario>, <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 muestran dos cursores del mouse en el visor de la consola virtual, significa que el sistema operativo del servidor admite el posicionamiento relativo. Esto es típico en Linux o Lifecycle Controller y hace que aparezcan dos cursores del mouse si la configuración de aceleración del mouse del servidor es distinta de la del cliente de consola virtual. Para solucionar esto, cambie al cursor sencillo seleccionando **Cursor sencillo** en el menú **Herramientas** del visor de la consola virtual. O bien, puede hacer coincidir la aceleración del mouse entre el sistema administrado y la estación de administración. Para salir del modo de cursor sencillo, presione <F9>.

 **NOTA:** Esto no se aplica a los sistemas administrados que ejecutan Windows, ya que estos admiten el posicionamiento absoluto.

Si 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 del mouse. Esto puede deberse a la función de aceleración del puntero previsible del escritorio GNOME. Para conseguir una sincronización adecuada del mouse en la consola virtual de iDRAC7, debe desactivar esta función. Para ello, en la sección del mouse del 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 toda las pulsaciones de tecla al servidor y enviar todas las pulsaciones y las combinaciones de teclas desde la estación de administración al sistema administrado a través del visor de la consola virtual. Si se desactiva, todas las combinaciones de teclas se dirigirán a la estación de administración en la que se ejecuta la sesión de la consola virtual.

El comportamiento de esta opción depende de los elementos siguientes:

- Tipo de complemento (Java o ActiveX) según la sesión de consola virtual que se inicia.
- 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, la estación de administración y el sistema administrado ejecuta 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 abre 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 abre 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.

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:
Haga clic en Ayuda en la página de la consola virtual para ver la ayuda en línea
- 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.
- Los medios de disco flexible virtuales de iDRAC7 no son accesibles 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.

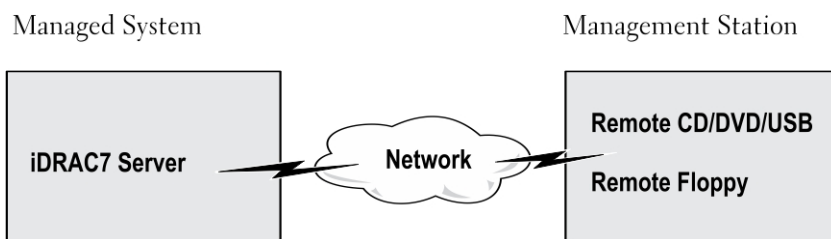


Ilustración 4. Configuración de medios virtuales

Unidades y dispositivos compatibles

En la tabla siguiente se enumeran las unidades compatibles a través de los medios virtuales.

Tabla 23. 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 utilizar la consola virtual](#)

Configuración de medios virtuales mediante la interfaz web de iDRAC7

Para configurar los valores de medios virtuales:

⚠ PRECAUCIÓN: No restablezca iDRAC7 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 iDRAC7, vaya a **Información general** → **Servidor** → **Medios conectados**.
2. Especifique los valores necesarios. Para obtener más información, consulte la *Ayuda en línea de iDRAC7*.
3. Haga clic en **Aplicar** para guardar la configuración.

Configuración de medios virtuales mediante RACADM

Para configurar los medios virtuales, utilice los objetos del grupo **cfgRacVirtual**. Para obtener más información, consulte la *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC) disponible en support.dell.com/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 **Medios virtuales**.
Se muestra la página **Medios virtuales de configuración de iDRAC**.
2. 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 habrán configurado los valores de alerta.

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 24. 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 .

Acceso a medios virtuales

Puede acceder a los medios virtuales con o sin la consola virtual. Antes de poder acceder a ellos, asegúrese de haber configurado los exploradores web.

Enlaces relacionados

[Configuración de exploradores web para utilizar 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 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 acceder a los medios virtuales mediante la consola virtual:

1. En la interfaz web de iDRAC7, vaya a **Información general** → **Servidor** → **ConsolaAdministrar**.
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, para acceder a la consola virtual mediante JAVA, abra el archivo **.jnlp** para iniciar la consola.

3. Haga clic en **Medios virtuales** → **Iniciar medios virtuales**.
Aparece la ventana **Vista de cliente** de los medios virtuales con los 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 utilizar la consola virtual](#)

[Configuración de medios virtuales](#)

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 iDRAC7, vaya a **Información general** → **Servidor** → **ConsolaAdministrar**.
Se muestra la ventana **Consola virtual**.

2. Haga clic en **Iniciar Consola virtual**.
Aparece el mensaje siguiente:

La consola virtual se ha desactivado. ¿Desea seguir utilizando el redireccionamiento de medios virtuales?

3. Haga clic en **Aceptar** para conectarse a los medios virtuales.
Aparece la ventana **Vista de cliente** de los medios virtuales con los dispositivos disponibles para la asignación.

 **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](#)

Adición de imágenes de medios virtuales

Para agregar imágenes de medios virtuales, en la ventana **Vista de cliente** de los medios virtuales:

- Haga clic en **Agregar imagen** y seleccione el archivo de imagen de la estación de administración o la unidad C: del sistema administrado.
La imagen ISO o de disco flexible se agrega a la lista de dispositivos disponibles.
- Para agregar una carpeta como una imagen ISO o de disco flexible, haga clic en **Agregar carpeta como imagen**. Esta función crea una imagen de medios de la carpeta remota y la monta como un dispositivo USB conectado al sistema operativo del servidor.
Los medios se conectan y la información se actualiza en la ventana **Vista de cliente**.
Cuando una carpeta se agrega como imagen, se crea un archivo **.iso** en el escritorio de la estación de administración desde la que se utiliza la función. Si este archivo **.iso** se mueve o se elimina, la entrada correspondiente en la ventana **Vista de cliente** de los medios virtuales no funcionarán. Por tanto, es recomendable no mover ni eliminar el archivo **.iso** mientras la *carpeta agregada* esté en uso. No obstante, el archivo **.iso** se puede quitar después de que se desactive la entrada pertinente y esta se quite mediante la opción **Quitar imagen**.

Eliminación de imágenes de medios virtuales

Para quitar la imagen, en la ventana **Vista de cliente** de los medios virtuales, seleccione la imagen asignada necesaria y haga clic en **Quitar imagen**.

La imagen seleccionada se quita de la lista de dispositivos en la ventana **Vista del cliente**.


Visualización de los detalles del dispositivo virtual

Para ver los detalles de los dispositivos virtuales, en la ventana **Vista de cliente** de los medios virtuales, haga clic en **Detalles**. Aparece la sección **Detalles** en la que se muestran los dispositivos virtuales disponibles y la actividad de lectura y escritura para cada uno de ellos.

Restablecimiento de USB


Para restablecer el dispositivo USB:

1. En la ventana **Vista del cliente** de los medios virtuales, haga clic en **Detalles** y, a continuación, 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.
2. Haga clic en **Sí**.
Se restablece el USB.

 **NOTA:** Los medios virtuales de iDRAC7 no se terminan, incluso después de cerrar la sesión de la interfaz web de iDRAC7.

Asignación de la unidad virtual

Para asignar la unidad virtual:

 **NOTA:** Mientras utiliza los medios virtuales basados en ActiveX, debe disponer de privilegios administrativos para asignar un DVD de sistema operativo o unidad Flash USB (conectada a la estación de administración). Para asignar las unidades, inicie IE como administrador o agregue la dirección IP de iDRAC7 a la lista de sitios de confianza.

1. Desconecte las unidades asignadas existentes antes de asignar otro origen de medios
2. En la ventana **Vista de cliente** de los medios virtuales, agregue la imagen o la carpeta que contiene la imagen.
3. En la columna **Asignado**, seleccione la casilla relacionada con la unidad que contiene la imagen necesaria. Para asignar dispositivos grabables en modo de solo lectura, active la opción **Solo lectura** para el dispositivo antes de asignarlo.

El dispositivo se asigna al sistema administrado.

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 también puede mostrar discos extraíbles y discos flexibles que no forman parte de ella. Para asegurarse de que las unidades virtuales correctas estén disponibles para su asignación, debe activar la configuración de puertos para el disco duro SATA conectada. Para ello:

1. Reinicie el sistema operativo de la estación de administración. Durante la POST, presione <F2> o <F12> para entrar en la 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 **Cliente** 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. En la ventana **Vista de cliente** de los medios virtuales, en la columna **Asignado**, desactive la casilla de la unidad.
Se anula la asignación de la unidad virtual en el sistema administrado.
2. Haga clic en **Salir** para terminar la sesión **Medios virtuales**.
Se cierra la ventana **Vista de cliente** de los medios virtuales.

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 iDRAC7, 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> para entrar en la **Configuración de iDRAC**.
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 iDRAC7 en el sistema administrado. Mediante 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:** La utilidad VMCLI solo se puede ejecutar en la estación de administración.

La utilidad VMCLI proporciona las siguientes funciones:

- Administración de dispositivos extraíbles o imágenes accesibles a través de medios virtuales.
- Terminación automática de la sesión cuando se activa la opción **Inicio único** en el firmware de iDRAC7.
- Comunicaciones seguras con iDRAC7 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\trac5** 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, para acceder a iDRAC7, ejecute la utilidad VMCLI y los comandos de inicio de sesión de usuario. Los usuarios que no sean administradores deben anexar el prefijo `sudo` en los comandos 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 [parámetro] [opciones_de_shell_de_sistema_operativo]

Por ejemplo, `vmcli -r iDRAC7-IP-address:iDRAC7-SSL-port`

El valor *parámetro* permite a la interfaz VMCLI conectarse al servidor especificado, acceder a iDRAC7 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 <dirección IP de iDRAC7[:iDRAC7-SSL-port]> -S -u <nombre de usuario de iDRAC7> -p <contraseña de usuario de iDRAC7> -c {<nombre de dispositivo> | <archivo de imagen>}`: indica si el certificado de CA de iDRAC7 es válido. Si no lo es, aparecerá un mensaje de advertencia al ejecutar el comando. Sin embargo, el comando se ejecuta correctamente y se establece una sesión VMCLI. Para obtener más información sobre los parámetros de VMCLI, consulte la *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 25. Comandos VMCLI

Medios virtuales	Comando
Unidad de disco flexible	<code>vmcli -r [IP o nombre de host de RAC] -u [nombre de usuario de iDRAC7] -p [contraseña de usuario de iDRAC7] -f [nombre del dispositivo]</code>
Disco flexible o imagen de memoria de USB de inicio	<code>vmcli -r [dirección IP de iDRAC7] [nombre de usuario de iDRAC7] -p [contraseña de iDRAC7] -f [disco flexible.img]</code>
Unidad CD mediante la opción -f	<code>vmcli -r [dirección IP de iDRAC7] -u [nombre de usuario de iDRAC7] -p [contraseña de iDRAC7] -f [nombre de dispositivo] [archivo de imagen]-f [cdrom - dev]</code>
Imagen CD/DVD de inicio	<code>vmcli -r [dirección IP de iDRAC7] -u [nombre de usuario de iDRAC7] -p [contraseña de iDRAC7] -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 iDRAC7 bajo **Información general** → **Servidor** → **vFlash**:

Tarjeta SD no detectada. Inserte una tarjeta SD de 256 MB o superior.

 **NOTA:** Asegúrese de solo insertar 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 el *Manual del propietario de hardware* del sistema disponible en support.dell.com/manuals.

 **NOTA:** Debe tener permiso para configurar iDRAC para activar o desactivar la funcionalidad de 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, puede ver las propiedades de la tarjeta SD mediante la interfaz web de iDRAC7 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 iDRAC7, vaya a **Información general** → **Servidor** → **vFlash**. Aparecerá la página **Propiedades de la tarjeta SD**. Para obtener información acerca de las propiedades que se muestran, consulte la *Ayuda en línea de iDRAC7*.

Visualización de las propiedades de la tarjeta vFlash SD mediante RACADM

Para ver las propiedades de la tarjeta vFlash SD mediante RACADM:

1. Abra una consola Telnet, SSH o de comunicación en serie al sistema e inicie sesión.
2. Introduzca el comando: `racadm getconfig -g cfgvFlashSD`

Aparecen las siguientes propiedades de solo lectura:

- `cfgVFlashSDSize`
- `cfgVFlashSDLicensed`
- `cfgVFlashSDAvailableSize`
- `cfgVFlashSDHealth`
- `cfgVFlashSDEnable`
- `cfgVFlashSDWriteProtect`
- `cfgVFlashSDInitialized`

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 **Medios vFlash**. En la página **Medios vFlash de configuración de iDRAC** se muestran las propiedades. Para obtener más 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 iDRAC7, 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:

1. Abra una consola Telnet, SSH o de comunicación en serie al sistema e inicie sesión.
2. Introduzca los comandos siguientes:
 - Para activar vFlash, escriba:
`racadm config -g cfgvFlashsd -o cfgvflashSDEnable 1`

- Para desactivar vFlash, escriba:
`racadm config -g cfgvFlashsd -o cfgvflashSDEnable 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 **Medios vFlash**.
Se muestra la página **Medios vFlash de configuración de iDRAC**.
2. Seleccione **Activado** para activar la funcionalidad vFlash o seleccione **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.

Inicialización de la tarjeta vFlash SD mediante la interfaz web

Para iniciar la tarjeta vFlash SD:

1. En la interfaz web de iDRAC7, 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:

1. Abra una consola Telnet, SSH o de comunicación en serie al sistema e inicie sesión.
2. Introduzca el comando: `racadm vflashsd initialize`
Se eliminan todas las particiones existentes y la tarjeta se reformatea.

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 **Medios vFlash**.
Se muestra la página **Medios vFlash de configuración de iDRAC**.
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 **Medios vFlash de configuración de de iDRAC** para ver el mensaje de que la operación se ha realizado correctamente.
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 (índice)`


 **NOTA:** Si se restablece iDRAC7, se pierde el estado de la última operación de partición.

Administración de las particiones vFlash

Puede realizar lo siguiente mediante la interfaz web de iDRAC7 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, tal como WS-MAN, la utilidad de configuración de iDRAC o RACADM, utiliza vFlash, o si desea desplazarse a otra página de la GUI, es posible que iDRAC7 muestre el mensaje siguiente: Otro proceso está utilizando vFlash. Vuelva a intentar más tarde.

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 iDRAC7, 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 iDRAC7*.

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 **.iso**) 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 iDRAC7 emula un dispositivo con un tipo de imagen incorrecto. Por ejemplo, si la partición se utiliza mediante una imagen ISO y el tipo de emulación se especifica como Disco duro, el BIOS no puede 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.

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 iDRAC7, vaya a **Información general** → **Servidor** → **vFlash** → **Crear a partir de 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 iDRAC7*.
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 de la imagen es mayor de 4 GB o excede el espacio disponible en la tarjeta.
 - El archivo de imagen no existe o la extensión del archivo de imagen no es .img ni .iso.
 - Ya se está realizando una operación de inicialización en la tarjeta.


Creación de una partición a partir de 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 //miservidor/carpetacompartida/foo.iso -u root -p micontraseña
```

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, F00.ISO en lugar F00.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 iDRAC7, 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 iDRAC7*.
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 iDRAC7 vaya a **Información 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 la *Ayuda en línea de iDRAC7*.

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 iDRAC7, vaya a **Información 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. Introduzca los comandos siguientes:

- 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
```

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 iDRAC7.

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 iDRAC7, vaya a **Información 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. Introduzca los comandos siguientes:

- 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
```

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, no cambia el nombre de la etiqueta de partición almacenado en iDRAC7.

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 iDRAC7, vaya a **Información 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 iDRAC7)
- 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 iDRAC7, 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 iniciar 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 ha actualizado a la versión más reciente.

Inicio de una partición mediante RACADM


Para establecer una partición vFlash como el primer dispositivo de inicio, utilice el objeto `cfgServerInfo`. Para obtener más información, consulte la *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC) disponible en support.dell.com/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 SMWG SMCLP.

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 alija desde el firmware de la controladora de iDRAC7 y admite interfaces Telnet, SSH y de conexión en serie. La interfaz SMCLP de iDRAC7 se basa en la especificación SMCLP versión 1.0 que proporciona la organización DMTF.

 **NOTA:** Encontrará información acerca de los perfiles, las extensiones y los MOF en delltechcenter.com y toda la información sobre DMTF en dmf.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 iDRAC7 permite realizar lo siguiente:

- 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
- Administrar la cuenta de usuario de iDRAC7
- 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 iDRAC7 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 `-s` 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 iDRAC7

SMCLP de iDRAC7 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:

```
<verbo> [<opciones>] [<destino>] [<propiedades>]
```

En la tabla siguiente se proporcionan los verbos y sus definiciones.

Tabla 26. Verbos de SMCLP

Verbo	Definición
<code>cd</code>	Navega en el MAP mediante el shell
<code>set</code>	Establece una propiedad para un valor específico
<code>help</code>	Muestra la ayuda de un destino específico
<code>reset</code>	Restablece el destino
<code>show</code>	Muestra las propiedades del destino, los verbos y los destinos secundarios
<code>start</code>	Activa un destino
<code>stop</code>	Desactiva un destino
<code>exit</code>	Cierra la sesión del shell de SMCLP
<code>version</code>	Muestra los atributos de versión de un destino
<code>load</code>	Lleva una imagen binaria de una URL a una dirección de destino especificada

En la tabla siguiente se proporciona una lista de destinos.

Tabla 27. Destinos de SMCLP

Destino	Definiciones
<code>admin1</code>	Dominio de admin
<code>admin1/profiles1</code>	Perfiles registrados en iDRAC7
<code>admin1/hdwr1</code>	Hardware
<code>admin1/system1</code>	Destino del sistema administrado
<code>admin1/system1/capabilities1</code>	Capacidades de recopilación del sistema administrado SMASH

Destino	Definiciones
admin1/system1/capabilities1/pwrcap1	Capacidades de utilización de la alimentación del sistema administrado
admin1/system1/capabilities1/electcap1	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
admin1/system1/sp1/capabilities1/pwrmgmtcap1	Capacidades del servicio de administración del estado de la alimentación en el sistema
admin1/system1/sp1/capabilities1/acctmgmtcap*	Capacidades del servicio de administración de cuentas
admin1/system1/sp1/capabilities1/rolemgmtcap*	Capacidades de administración basada en funciones locales
admin1/system1/sp1/capabilities1/PwrutilmgmtCap1	Capacidades de administración de utilización de la alimentación
admin1/system1/sp1/capabilities1/electcap1	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

Destino	Definiciones
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
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 iDRAC7. Desplácese 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 del 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 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 y 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 están disponibles en el sitio web de DMTF en dmf.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 se ha detenido correctamente
```
- Para activar el servidor:

```
start /system1
```

Aparece el mensaje siguiente:

```
system1 se ha iniciado correctamente
```
- Para reiniciar el servidor:

```
reset /system1
```

Aparece el mensaje siguiente:

```
system1 se ha restablecido correctamente
```

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
```

Destinos:
Anotación1
Anotación2
Anotación3
Anotación4
Anotación5

Propiedades:
InstanceID = IPMI:BMC1 registro SEL
MaxNumberOfRecords = 512
CurrentNumberOfRecords = 5
Name = IPMI SEL
EnabledState = 2
OperationalState = 2
HealthState = 2

```
Caption = IPMI SEL
Description = IPMI SEL
ElementName = IPMI SEL
Comandos:
cd
show
help
exit
version
```

- **Para ver la anotación SEL:**

```
show/system1/logs1/log1
```

Aparece la siguiente información :

```
/system1/logs1/log1/record4
```

Propiedades:

```
LogCreationClassName= CIM_RecordLog
```

```
CreationClassName= CIM_LogRecord
```

```
LogName= IPMI SEL
```

```
RecordID= 1
```

```
MessageTimeStamp= 20050620100512.000000-000
```

```
Description= FAN 7 RPM: sensor de ventilador, fallo detectado
```

```
ElementName= anotación de IPMI SEL
```

Comandos:

```
cd
```

```
show
```

```
help
```

```
exit
```

```
version
```

- **Para borrar el SEL:**

```
delete /system1/logs1/log1/record*
```

Aparece la siguiente información :

```
Todos los registros se borraron satisfactoriamente
```

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`

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.
- El usuario tiene disponible los privilegios **Configurar Usuario** y **Acceder a los medios virtuales** para iDRAC7.
- 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.

- iDRAC7 está configurado en los sistemas remotos de destino.
- El sistema puede iniciar desde el archivo de imagen.
- IPMI en la LAN está activado en iDRAC7.
- El recurso compartido de red contiene controladores y el archivo de imagen de sistema operativo en 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 iDRAC7 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 <iDRAC7-IPAddress or file> -u <iDRAC7-user> -p <iDRAC7-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 a la opción `-r` es el nombre de un archivo existente, la secuencia de comandos lee las direcciones IPv4 o IPv6 de iDRAC7 desde el archivo especificado y ejecuta la utilidad una vez para cada línea. Si el argumento a la opción `-r` no es un nombre de archivo, debería ser una única dirección de iDRAC7. 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 28. Parámetros de comando de vmdeploy

Parámetro	Descripción
<code><iDRAC7-user></code>	Nombre de usuario de iDRAC7. Debe tener los atributos siguientes: <ul style="list-style-type: none"> – Nombre de usuario válido – Permiso de usuario de medios virtuales de iDRAC7 <p>Si la autenticación de iDRAC7 falla, aparece un mensaje de error y el comando termina.</p>
<code><iDRAC7-ip file></code>	Dirección IP de iDRAC7 o el archivo que contiene la dirección IP de iDRAC7.
<code><iDRAC7-user-password> o <iDRAC7- -passwd></code>	Contraseña del usuario de iDRAC7. Si la autenticación de iDRAC7 falla, aparece un mensaje de error y el comando termina.
<code>-c {<device-name> <image-file>}</code>	Ruta de acceso a una imagen ISO9660 del CD o DVD de instalación del sistema operativo.
<code><floppy-device></code>	Ruta de acceso al dispositivo que contiene el CD, DVD o disco flexible de instalación del sistema operativo.
<code><floppy-image></code>	Ruta de acceso a una imagen de disco flexible válido.
<code><Device ID></code>	ID del dispositivo de inicio único.

Enlaces relacionados

[Configuración de medios virtuales](#)


[Configuración de iDRAC7](#)

Implementación del sistema operativo mediante recurso compartido de archivos remotos

Antes de implementar el sistema operativo mediante el recurso compartido de archivos remotos, asegúrese de lo siguiente:

- Los medios virtuales deben estar en el estado **Conectado** para que las unidades virtuales aparezcan en la secuencia de inicio.
- El usuario tiene disponible los privilegios **Configurar Usuario** y **Acceder a los medios virtuales** para iDRAC7.
- El recurso compartido de archivos remotos está activado.

- El recurso compartido de red contiene controladores y el archivo de imagen de sistema operativo en 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 el sistema operativo mediante recurso compartido de archivos remotos:

1. Monte el archivo de imagen ISO o IMG en el sistema administrado mediante NFS o CIFS.
2. Vaya a **Información 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 **Aplicar**.
6. 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](#)

[Administración de recursos compartidos de archivos remotos](#)


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 situado en un recurso compartido y ponerlo a la disposición del sistema operativo del servidor administrado en forma de unidad virtual. Para ello, móntelo como CD o DVD mediante NFS o CIFS. Esta función requiere una 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 se ejecuta ESXi en el sistema administrado y si monta una imagen de disco virtual (**.img**) mediante recursos compartidos de archivos remotos, la imagen de disco flexible conectada no estará disponible para el sistema operativo ESXi.

El estado de conexión de RFS está disponible en el registro de iDRAC7. Una vez conectado, una unidad virtual montada mediante RFS no se desconecta, incluso si cierra la sesión de iDRAC7. La conexión RFS se cierra si iDRAC7 se restablece o si se interrumpe la conexión de red. Las opciones de la interfaz web y la línea de comandos también están disponibles en CMC e iDRAC7 para cerrar la conexión RFS. La conexión RFS de CMC siempre invalida una unidad montada mediante RFS en iDRAC7.

 **NOTA:** La función vFlash de iDRAC7 y RFS no están relacionados.

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 iDRAC7, vaya a **Información general** → **Servidor** → **Medios conectados**.

Aparece la página **Medios conectados**.

2. Bajo **Recurso compartido de archivos remotos**, seleccione conectar o conectar automáticamente y especifique el nombre de usuario, la contraseña y la ruta de acceso al archivo de imagen. Para obtener más información, consulte la *Ayuda en línea de iDRAC7*.
3. Haga clic en **Aplicar** y, después, en **Conectar**.
Se establece la conexión y la opción **Estado de conexión** muestra que está 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 <opciones>
```

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. Indique la ubicación entre comillas

-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 de sistema operativo en 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 en Inicio único desde **Disco flexible virtual** o **CD/DVD/ISO virtual** mediante la interfaz web de iDRAC7.
 - 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 iDRAC7](#)

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. Establezca la opción **Puerto USB interno** en **Activado**. Si se establece en **Desactivado**, el IDSDM no estará disponible como dispositivo de inicio.
4. Si no se necesita redundancia (una sola tarjeta SD), establezca la opción **Puerto de tarjeta SD interno** en **Activado** y la opción **Redundancia de la tarjeta SD interna** en **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).

Puede ver el estado, la condición y la disponibilidad de IDSDM mediante la interfaz web de iDRAC7 o RACADM. El estado de redundancia de la tarjeta SD y sus sucesos de falla se registran en el SEL, que se muestra en el panel anterior, y las alertas PET se general si están activadas.

Enlaces relacionados

[Visualización de la información del sensor](#)

Solución de problemas de Managed System mediante iDRAC7

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](#)

[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](#)

Uso de la consola de diagnósticos

iDRAC7 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 iDRAC7 puede acceder a las herramientas de depuración de la red.

Para acceder a la consola de diagnósticos:

1. En la interfaz web de iDRAC7, vaya a **Información 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 la *Ayuda en línea de iDRAC7*.
Los resultados se muestran en la misma página.

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.

iDRAC7 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 iDRAC7, 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 **Información de inicio** → **Servidor** → **Solución de problemas** → **Captura de video**.

Se muestra la pantalla **Captura de video**. Para obtener más información, consulte la *Ayuda en línea de iDRAC7*.

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 iDRAC7. 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 iDRAC7, vaya a **Información 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
- Suministros de energía
- Unidades 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 del panel frontal LCD para los servidores tipo bastidor y torre aplicables, en la interfaz web de iDRAC7 vaya a **Información general** → **Hardware** → **Panel frontal**. Se muestra la página **Panel frontal**.

En la sección **Fuente en directo del panel frontal** se muestran las fuentes en directo de los mensajes que se están mostrando 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 del panel frontal LCD del servidor mediante RACADM, utilice los objetos del grupo `System.LCD`. Para obtener más información, consulte la *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC) disponible en support.dell.com/manuals.

Enlaces relacionados

[Configuración de los valores de LCD](#)

Visualización del estado del LED del panel anterior del sistema

Para ver el estado actual del LED de ID del sistema, en la interfaz web de iDRAC7 vaya a **Información general** → **Hardware** → **Panel frontal**. En la sección **Fuente en directo del panel frontal** 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 condición azul en el panel frontal del LED), 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 del LED de ID del sistema mediante RACADM, utilice el comando **getled**. Para obtener más información, consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC) disponible en support.dell.com/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 iDRAC7 y CMC (para servidores Blade) muestran el estado de los elementos siguientes:




- Baterías
- Ventiladores
- Intrusión
- Suministros de energía
- Unidades Flash extraíbles
- Temperaturas
- Voltajes
- CPU

En la interfaz web de iDRAC7, vaya a la sección **Información 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.

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 iDRAC7

Puede realizar un reinicio por hardware o por software de iDRAC7 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 iDRAC7 o RACADM.

Reinicio de iDRAC7 mediante la interfaz web de iDRAC7

Para reiniciar iDRAC7, realice una de las acciones siguientes en la interfaz web de iDRAC7:

- 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**.

Restablecimiento de iDRAC7 mediante RACADM

Para reiniciar iDRAC7, utilice el comando **racreset**. Para obtener más información, consulte *RACADM Reference Guide for iDRAC7 and CMC* (Guía de referencia de RACADM para iDRAC7 y CMC) disponible en support.dell.com/manuals.

Restablecimiento de iDRAC7 a la configuración predeterminada de fábrica

Puede restablecer iDRAC7 a los valores predeterminados de fábrica mediante la utilidad de configuración de iDRAC. De lo contrario, asegúrese de desactivar la opción **Conservar configuración** durante la actualización del firmware.

Para restablecer iDRAC7 a los valores predeterminados de fábrica mediante la utilidad de configuración de iDRAC:

1. En la utilidad de configuración de iDRAC, vaya a **Restablecer valores predeterminados de iDRAC**. 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 más 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](#)
- [RACADM](#)
- [Varios](#)

Registro de sucesos del sistema

Al utilizar la interfaz web de iDRAC7 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 iDRAC7 está en la Intranet local, seleccione **Intranet local** y haga clic en **Nivel personalizado....**
2. En la ventana **Configuración de seguridad**, en **Descargas** compruebe que las siguientes opciones están activadas:
 - Preguntar automáticamente si se debe descargar un archivo: (si está disponible)
 - Descarga de archivos

 **PRECAUCIÓN:** Para garantizar la seguridad del equipo que se utiliza para acceder a iDRAC7, bajo **Varios**, desactive la opción **Inicio de aplicaciones y archivos no seguros**.

Seguridad de la red

Al acceder a la interfaz web de iDRAC7, aparece una advertencia de seguridad que indica que el certificado emitido por la autoridad de certificados (CA) no es de confianza.

iDRAC7 incluye un certificado de servidor 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 iDRAC7 emitido por una CA de confianza (por ejemplo Microsoft Certificate Authority, Thawte o Verisign).

¿Por qué el servidor DNS no registra iDRAC7?

Algunos servidores DNS registran nombres de iDRAC7 que contienen solo hasta 31 caracteres.

Al acceder a la interfaz web de iDRAC7, se muestra una advertencia de seguridad que indica que el nombre de host del certificado SSL no coincide con el nombre de host de iDRAC7.

iDRAC7 incluye un certificado de servidor de iDRAC7 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 iDRAC7 no coincide con el nombre de host de iDRAC7 (por ejemplo, la dirección IP).

Para solucionar esto, cargue un certificado de servidor de iDRAC7 a la dirección IP o el nombre de host de iDRAC7. 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 iDRAC7 (si el certificado se ha emitido a la IP) o con el nombre DNS registrado de iDRAC7 (si el certificado se ha emitido al nombre registrado de iDRAC7).

Para asegurarse de que la CSR coincida con el nombre DNS de iDRAC7:

1. En la interfaz web de iDRAC7, vaya a **Información general** → **Configuración de iDRAC** → **Red**. Aparecerá 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 iDRAC7.
3. Haga clic en **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 iDRAC7 local, inicie sesión en iDRAC7 mediante las credenciales locales. Tras iniciar sesión, compruebe lo siguiente:
 - La opción **Activar Active Directory** 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 iDRAC7**.
 - Se ha cargado el certificado CA raíz de Active Directory correcto en iDRAC7 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.
- Verifique los certificados SSL de la controladora de dominio para asegurarse de que la hora del iDRAC7 está dentro del 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: No se puede establecer la conexión con el servidor LDAP, Error:
14090086:Rutinas SSL:SSL3_GET_SERVER_CERTIFICATE:error de verificación de
```

certificado: compruebe que se ha cargado el certificado de CA correcto en iDRAC7. Compruebe también si la fecha de iDRAC7 está dentro del período válido de los certificados y que la dirección de la controladora de dominios configurada en iDRAC7 coincide con el asunto del certificado del servidor de directorios.

Si está activada la validación de certificados, cuando iDRAC7 establece la conexión SSL con el servidor de directorios, iDRAC7 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 iDRAC7 no se encuentra dentro de período de validación del certificado de servidor o de CA. Compruebe la hora de iDRAC7 y el período de validación del certificado.
- Las direcciones de controladora de dominio configuradas en iDRAC7 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 iDRAC7 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 iDRAC7.
- 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 iDRAC7.

¿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?

iDRAC7 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 hay direcciones de controladora global configuradas, iDRAC7 sigue consultando el catálogo global. Si se recuperan privilegios adicionales desde el catálogo global, estos privilegios se acumulan.

¿iDRAC7 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, iDRAC7 realiza una conexión LDAP para aislar el problema, pero no realiza un enlace LDAP en una conexión no segura.

¿Por qué iDRAC7 activa la validación de certificados de manera predeterminada?

iDRAC7 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 iDRAC7 el nombre NetBIOS?

No en esta versión.

¿Por qué tarda hasta cuatro minutos iniciar sesión en iDRAC7 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. iDRAC7 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 iDRAC7 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 `klint purge`.
5. Una vez actualizado el GPO, cree el nuevo archivo keytab.
6. Cargue el archivo keytab en iDRAC7.

Ahora puede iniciar sesión en iDRAC mediante SSO.

¿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 el **Editor del Registro**. Ahora puede iniciar sesión en iDRAC7 mediante SSO.

Si ha activado el inicio de sesión único para iDRAC7 y está utilizando Internet Explorer para iniciar sesión en iDRAC7, 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 iDRAC7 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 iDRAC7 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. iDRAC7 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 está activa incluso si se ha cerrado la sesión de la interfaz web de iDRAC7. ¿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 video local del servidor está apagado?

Sí

¿Por qué tarda 15 segundos apagar el vídeo local del servidor después de solicitar la desactivación del video local?

Para que el usuario local tenga la oportunidad de realizar alguna acción antes de que el video se apague.

¿Hay algún retraso al encender el video local?

No. Después de que iDRAC7 recibe la solicitud de encendido de video local, el video se enciende instantáneamente.

¿El usuario local puede desactivar el video?

Cuando la consola local está desactivada, el usuario local no puede apagar el video.

¿La desactivación del video local también desactiva el teclado y el mouse locales?

No

¿La desactivación de la consola local desactivará el video en la sesión de consola remota?

No, la activación o desactivación del video local es independiente de la sesión de consola remota.

¿Cuáles son los privilegios necesarios para que un usuario de iDRAC7 active o desactive el video del servidor local?

Cualquier usuario con privilegios de configuración de iDRAC7 puede activar o desactivar la consola local.

¿Cómo se puede ver el estado actual del video 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 -p getconfig -g cfgRacTuning
```

El estado también se puede ver en la pantalla OSCAR de la consola virtual. Cuando la consola local está activada, se muestra un estado verde junto al nombre del servidor. Cuando está desactivada, un punto amarillo indica que iDRAC7 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 iDRAC7 del cliente de la consola virtual de iDRAC7. 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 iDRAC7, 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 iDRAC7 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 iDRAC7. 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 iDRAC7, ¿por qué aparece una ventana emergente sobre la seguridad de ActiveX?

Es posible que iDRAC7 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 iDRAC7 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 iDRAC7.
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. iDRAC7 tiene un controlador de mouse USB, lo que permite la posición absoluta y un seguimiento más cercano del puntero del mouse. Incluso si iDRAC7 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 del mouse** se establece en **USC/Cuadros de diálogo**. Presione 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 iDRAC7 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 iDRAC7 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 iDRAC7 en una estación de administración, se agota el tiempo de espera de la GUI de iDRAC7 si la GUI se inicia antes de que se cierre la ventana emergente. Si la GUI de iDRAC7 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, presione 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 iDRAC7, 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 iDRAC7 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 iDRAC7 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 iDRAC7 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?

iDRAC7 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?

Consulte support.dell.com para obtener Dell Boot Utility.

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 iDRAC7?

Las actualizaciones del firmware restablecen el iDRAC7 y hacen que este interrumpa la conexión remota y desmonte las unidades virtuales. Las unidades vuelven a aparecer una vez finalizada el restablecimiento de iDRAC7.

¿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 iDRAC7 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 iDRAC7 es public. Cuando IT Assistant envía una solicitud set, el agente iDRAC7 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 iDRAC7 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 iDRAC7. ¿Por qué?

iDRAC7 muestra información solamente para los dispositivos capacidad CEM (administración incorporada completa).

RACADM

Después de realizar un restablecimiento de iDRAC7 (mediante el comando `racreset` de RACADM), si se emite algún comando, aparece el mensaje siguiente. ¿Qué significa esto?

```
ERROR: no se puede conectar con el RAC en la dirección IP especificada
```

El mensaje indica que antes de emitir otro comando, debe esperar hasta que iDRAC7 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 iDRAC7, 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 remota 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 <nombredearchivo>
```

donde `nombredearchivo` 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 libopenssl10_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 iDRAC7.

El servidor web iDRAC7 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 iDRAC7.
- Cuando la propiedad `cfgRacTuneHttpsPort` cambia (incluso cuando un comando `config -f` (archivo de configuración) la cambia).
- Cuando se utiliza el comando `racresetcfg`.
- Cuando se restablece iDRAC7.
- Cuando se carga un nuevo certificado de servidor SSL.

¿Por qué se muestra un mensaje de error si se intenta eliminar una partición después de crearla mediante RACADM local?

Esto sucede porque la operación de creación de partición está en curso. Sin embargo, la partición se elimina después de cierto tiempo y se mostrará un mensaje que 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 aparece, consulte la dirección IP del servidor.

Con la consola virtual: reinicie el servidor para consultar la dirección IP de iDRAC durante la 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 la *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC) 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 iDRAC7: haga clic en **Información general** → **Configuración de iDRAC** → **CMC**. Aparecerá 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 la *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC) 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?

En la interfaz web de iDRAC7: vaya a **Información general** → **Servidor** → **Propiedades** → **Resumen**. Aparece la página **Resumen del sistema** con la dirección IP de iDRAC7.

Desde RACADM local: utilice el comando `racadm getsysinfo`.

En la pantalla LCD: en el servidor físico, utilice los botones de navegación del panel para ver la dirección IP de iDRAC7. 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 iDRAC7 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.

- iDRAC7 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 iDRAC7?

El iDRAC7 se debe restaurar a sus valores predeterminados. Para obtener más información, consulte [Restablecimiento de iDRAC7 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**.

iDRAC7 en el servidor Blade no responde durante el inicio.

Retire el servidor e insértelo nuevamente.

Compruebe la interfaz web de CMC para ver si iDRAC7 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 iDRAC7 mediante la interfaz web de iDRAC7 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 iDRAC7.

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 iDRAC7

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, apunte la dirección IP o el nombre de host y luego realice las operaciones siguientes mediante la interfaz web de iDRAC desde la 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.

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 iDRAC7, vaya a **Información 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.

Configuración de alertas y alertas por correo electrónico


Para configurar alertas y 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 iDRAC7, vaya a **Información general** → **Servidor** → **Registros** para ver el SEL e **Información general** → **Servidor** → **Registros** → **Registro de Lifecycle** para ver el registro de ciclos de vida.

 **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.

Interfaces para actualizar el firmware de iDRAC

Utilice las interfaces siguientes para actualizar el firmware de iDRAC:

- Interfaz web de iDRAC7
- CLI de RACADM (iDRAC7 y CMC)
- Dell Update Package (DUP)
- Interfaz web de 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, en la interfaz web de iDRAC7 vaya a una de las ubicaciones siguientes:

- **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**.
- **Información 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 iDRAC7*.

Creación de una 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 iDRAC7:
 - Vaya a **Información general** → **Servidor** → **Consola** 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

Actualmente, hay dos servidores instalados 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](#).