Integrated Dell Remote Access Controller 9 (iDRAC9)

Guía del usuario, versión 3.00.00.00

DELL EMC

Notas, precauciones y avisos

NOTA: Una NOTA indica información importante que le ayuda a hacer un mejor uso de su producto.

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

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

2017 - 06

Rev. A0X

Tabla de contenido

1

Descripción general

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

La iDRAC con la tecnología 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 Dell desde cualquier ubicación y sin el uso de agentes. Esto lo hace independientemente del sistema operativo o de la presencia o del estado del hipervisor.

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

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

iDRAC está disponible en las variantes siguientes:

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

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

Temas:

- Acceso a documentos desde el sitio de asistencia de Dell

Ventajas de utilizar iDRAC con Lifecycle Controller

Entre las ventajas se incluyen las siguientes:

- Mayor disponibilidad: notificación temprana de fallas potenciales o reales que ayudan a evitar una falla de servidor o reducir el tiempo de recuperación después de una falla.
- Productividad mejorada y menor costo total de propiedad (TCO): la extensión del alcance que tienen los administradores a un mayor número de servidores remotos puede mejorar la productividad del personal de TI mientras se reducen los costos operativos, tales como los viajes.
- Entorno seguro: al proporciona acceso seguro a servidores remotos, los administradores pueden realizar funciones críticas de administración mientras conservan la seguridad del servidor y la red.
- Mejor administración incorporada a través de Lifecycle Controller: Lifecycle Controller proporciona capacidades de implementación y servicios simplificados a través de la GUI de Lifecycle Controller para la implementación local y las interfaces de servicios remotos (WSMan) para la implementación remota incorporada con Dell OpenManage Essentials y consolas de asociados.

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

Funciones clave

Entre las funciones clave del iDRAC se incluye lo siguiente:

NOTA: Algunas de las funciones solamente están disponibles con la licencia iDRAC Enterprise. Para obtener información sobre las funciones disponibles para una licencia, consulte Administración de licencias .

Inventario y supervisión

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

  NOTA: CMC proporciona acceso a iDRAC a través del panel LCD del chasis M1000E y conexiones de la consola local. Para obtener más información, consulte la *Guía de usuario de Chassis Management Controller* disponible en dell.com/support/manuals.
- Visualización de las interfaces de red disponibles en los sistemas operativos host
- La iDRAC9 proporciona una mejor supervisión y funcionalidad de administración con Quick Sync 2. Necesita la aplicación OpenManage Mobile configurada en su dispositivo móvil Android o iOS.

Implementación

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

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

Actualizar

- Administración de licencias del iDRAC
- Actualización del BIOS y firmware de dispositivos para dispositivos compatibles con Lifecycle Controller.
- Actualización o reversión del firmware de iDRAC y del firmware de Lifecycle Controller por medio de una única imagen de firmware
- Administración de actualizaciones preconfiguradas
- Creación de copia de seguridad y restauración del perfil del servidor.
- Acceder a la interfaz de iDRAC a través de una conexión USB directa.
- Configuración de iDRAC mediante perfiles de configuración del servidor en el dispositivo USB.

Mantenimiento y solución de problemas

- Operaciones relacionadas con la alimentación y supervisión del consumo de alimentación
- Optimización del rendimiento del sistema y del consumo de alimentación mediante la modificación de la configuración térmica
- Independencia de Server Administrator para la generación de alertas.
- Registro de datos de sucesos: registro de Lifecycle y de RAC
- Establecimiento de alertas por correo electrónico, alertas IPMI, registros del sistema remoto, registros de sucesos de WS, sucesos de Redfish y capturas SNMP (v1, v2c y v3) para sucesos y notificación mejorada de alertas por correo electrónico.

- Captura de la última imagen de bloqueo del sistema
- Visualización de vídeos de captura de inicio y bloqueo
- Supervisión y generación de alerta fuera de banda del índice de rendimiento de la CPU, la memoria y los módulos de E/S.
- Configuración del umbral de advertencia para la temperatura de entrada y el consumo de alimentación.
- Utilice el módulo de servicio de iDRAC para:
  - Ver información sobre el sistema operativo.
  - Replicar los registros de Lifecycle Controller en los registros del sistema operativo.
  - Opciones de recuperación automática del sistema.
  - Active o desactive la condición de ciclo de apagado y encendido completo para todos los componentes del sistema, excepto la unidad de fuente de alimentación (PSU).
  - Restablezca forzadamente de manera remota el iDRAC
  - Active las alertas de SNMP en banda del iDRAC
  - Acceda al iDRAC mediante el sistema operativo del host (función experimental)
  - Relleno de datos del instrumental de administración de Windows (WMI).
  - Integración con SupportAssist Collection. Esto se aplica únicamente si se ha instalado el módulo de servicio de iDRAC versión 2.0 o posterior.
  - Preparación para quitar una unidad SSD PCIe NVMe.
- Genere la recopilación de SupportAssist de las siguientes maneras:
  - Automática: el uso del módulo de servicio del iDRAC que automáticamente invoca la herramienta OS Collector.
  - Manual: mediante la herramienta OS Collector.

Prácticas recomendadas de Dell referidas al iDRAC

- Las iDRAC están diseñadas para estar en una red de administración independiente; no están diseñadas ni destinadas para introducirlas ni conectarlas a Internet. Si lo hace, se puede exponer el sistema conectado a problemas de seguridad y otros riesgos por los que Dell no es responsable.
- Además de colocar las iDRAC en una subred de administración separada, los usuarios deben aislar la subred de administración/vLAN con tecnologías tales como servidores de seguridad y limitar el acceso a la subred/vLAN a los administradores de servidor autorizados.

Conectividad segura

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

- Certificado de firma personalizado para el certificado de capa de sockets seguros (SSL)
- Actualizaciones de firmware firmadas
- Autenticación de usuarios a través de Microsoft Active Directory, servicio de directorio del protocolo ligero de acceso a directorios (LDAP) genérico o contraseñas e identificaciones de usuario administrados de manera local
- Autentificación de factor doble con la función de inicio de sesión mediante tarjeta inteligente. La autentificación de factor doble se basa en la tarjeta inteligente física y el PIN correspondiente.
- Inicio de sesión único y autentificación de clave pública
- Autorización basada en roles con el fin de configurar privilegios específicos para cada usuario
- Autenticación SNMPv3 para cuentas de usuario almacenadas de forma local en iDRAC. Se recomienda usar esta opción, pero está desactivada de forma predeterminada.
- Configuración de la identificación y contraseña del usuario
- Modificación de la contraseña de inicio de sesión predeterminada
- Configuración de las contraseñas de usuario y las contraseñas del BIOS mediante un formato de algoritmo hash unidireccional para una mayor seguridad.
- Capacidad de FIPS 140-2 nivel 1.
- Compatibilidad con TLS 1.2, 1.1 y 1.0. Para mejorar la seguridad, el valor predeterminado es TLS 1.1 y superior.
- Interfaces web y SMCLP que admiten cifrados de 128 bits y 40 bits (para países en los que no se aceptan 128 bits), utilizando el estándar TLS 1.2

NOTA: Para garantizar una conexión segura, Dell recomienda el uso de TLS 1.1 y posteriores.

- Configuración del tiempo de espera de la sesión (en segundos)
- Puertos IP configurables (para HTTP, HTTPS, SSH, Telnet, consola virtual y medios virtuales)

NOTA: Telnet no admite el cifrado SSL y está desactivado de manera predeterminada

- Shell seguro (SSH), que utiliza una capa cifrada de transporte para brindar una mayor seguridad
- Límites de falla de inicio de sesión por dirección IP, con bloqueo del inicio de sesión de la dirección IP cuando se ha superado el límite
- Rango limitado de direcciones IP para clientes que se conectan al iDRAC.
- Adaptador Gigabit Ethernet dedicado en servidores tipo bastidor y torre disponible (es posible que se necesite hardware adicional).

Novedades de esta versión

- Se ha agregado compatibilidad con Redfish 2016.R1 y .R2, una interfaz de programación de aplicaciones (API) RESTful, que es estandarizada por Distributed Management Task Force (DMTF). Proporciona una interfaz de administración de sistemas seguros y escalables.
- Compatibilidad de API RESTful de iDRAC mejorada con perfiles de configuración del servidor con acceso a través de la transmisión por secuencias de archivos local y la transferencia de archivos HTTP/S.
- Se ha agregado compatibilidad de perfiles de configuración del servidor con las actualizaciones basadas en repositorio de firmware y el formato de archivo JSON.
- Exportación e importación de perfiles de configuración del servidor desde la interfaz gráfica de usuario de iDRAC.
- Quick Sync 2 reemplaza a Quick Sync NFC (tecnología de comunicación de campo cercano) con Bluetooth de bajo consumo (BLE) y Wi-Fi para un alto rendimiento. Es compatible con la interfaz gráfica de usuario de iDRAC y el acceso a la consola virtual.
- Se ha agregado compatibilidad con transferencias de archivos de HTTP/HTTPS.
- Se ha agregado compatibilidad con la transmisión por secuencias WSMan para perfiles de configuración del servidor.
- Se ha agregado la nueva función Administrador de grupos. Todas las iDRAC en la misma subred se pueden agrupar y los sistemas se pueden agrupar y administrar mediante una iDRAC maestra del grupo.
- Se ha agregado un banner de seguridad para la página de inicio de sesión de la interfaz gráfica de usuario.
- Refrigeración de múltiples vectores para una mejor refrigeración de flujo de aire de tarjetas PCIe de otros fabricantes.
- DHCP es la dirección IP predeterminada de iDRAC (la dirección estática era el valor predeterminado en generaciones anteriores).
- La contraseña predeterminada se genera de forma aleatoria y está impresa en la etiqueta de información del sistema, a menos que los valores "root/calvin" heredados se hayan pedido de fábrica.
- La conexión USB directa de iDRAC en la parte delantera del servidor es ahora una ranura Micro B, y se conecta de forma permanente a la iDRAC solo para aumentar el nivel de seguridad.
- Se ha agregado una nueva función de bloqueo del sistema para restringir el uso de las herramientas de Dell para realizar cambios en el BIOS, la iDRAC, el firmware, etc.
- El Módulo de servicio de iDRAC (iSM) está previamente instalado en la iDRAC y puede aparecer en el sistema operativo; nada debe descargarse.
- SupportAssist se puede configurar a través de la iDRAC para el servicio de llamada a casa personalizado del soporte de Dell.
- SupportAssist Collector ahora incluye volcados de núcleo de la iDRAC, volcados de memoria de hardware y registros de ESXi.
- Visor de SupportAssist: es una opción para exportar un informe con formato HTML5 para que el cliente pueda verlo con navegadores web estándares.
- Interfaz web HTML5 completa para una carga más rápida de las páginas y la facilidad de uso.
- Configuración del BIOS en la interfaz gráfica de usuario de la iDRAC.
- Funciones de almacenamiento extendido a través de la iDRAC, como por ejemplo expansión de capacidad en línea (OCE) y migración de nivel RAID (RLM) sin el uso de agentes, a través de la interfaz gráfica de usuario o la CLI.
- Adición/Eliminación mejorada de los usuarios de iDRAC.
- Configuración eficiente de alertas.
- Se han agregado opciones de próximo inicio y control de alimentación en HTML5 vConsole.
- Se ha agregado la función Vista de conexión para proporcionar el switch y el puerto para iDRAC, LOM y tarjetas PCIe admitidas por Dell.
- Tarjeta interna vFlash de 16 GB (opcional).
- Bisel con panel LCD (opcional).

- Inicio seguro es una tecnología de UEFI que elimina las amenazas heredadas y proporciona verificación de identidad de software en cada paso del inicio (el firmware de la plataforma, las tarjetas opcionales y el cargador de inicio del sistema operativo) que elimina los principales vacíos de seguridad que pueden ocurrir durante la transferencia entre el firmware de UEFI y el sistema operativo (SO) de UEFI.

Cómo usar esta guía del usuario

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

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

Exploradores web compatibles

iDRAC es compatible con los siguientes exploradores:

- Internet Explorer/Edge
- Mozilla Firefox
- Google Chrome
- Safari

Para ver la lista de versiones admitidas, consulte las *Notas de versión de iDRAC*, disponibles en **dell.com/idracmanuals**.

Hipervisores de SO compatibles

iDRAC es compatible con los siguientes hipervisores de SO:

- Microsoft
- VMware
- Citrix
- iOS

Administración de licencias

Las funciones de iDRAC se encuentran disponibles según iDRAC Express (predeterminado) o iDRAC Enterprise (se puede adquirir). Solo las funciones con licencia están disponibles en las interfaces que permiten configurar o usar iDRAC. Para obtener más información, consulte Funciones con licencia en iDRAC8 e iDRAC9.

Tipos de licencias

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

- Evaluación de 30 días: la licencia caduca después de 30 días y no puede ampliarse. Las licencias de evaluación se basan en períodos de tiempo y el tiempo transcurrirá mientras se aplique alimentación al sistema.

- Evaluación de 6 meses: la licencia caduca después de 6 meses y no puede extenderse. Las licencias de evaluación se basan en períodos de tiempo y el tiempo transcurrirá mientras se aplique alimentación al sistema.
- Perpetua: la licencia está enlazada a la etiqueta de servicio y es permanente.

Métodos para la 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 solicitarla desde el centro de asistencia técnica.
- Portal de autoservicio de licencias: hay un vínculo al portal de autoservicio disponible en iDRAC. Haga clic en este vínculo para abrir Dell Digital Locker. Dell Digital Locker le permite ver y administrar sus productos, software y la información de licencias en una sola ubicación.
- Punto de venta: la licencia se adquiere al realizar un pedido de un sistema.

Operaciones de licencia

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

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

Puede realizar las siguientes operaciones con licencia mediante iDRAC, RACADM, WSMan, Redfish y Lifecycle Controller-Remote Services para una administración de licencias de una a una, y Dell License Manager para la administración de licencias de una a varias:

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

  NOTA: Después de importar la licencia, se debe volver a iniciar sesión en iDRAC. Esto se aplica solamente a la interfaz web de iDRAC.
- Export (Exportar): exporta la licencia instalada para la copia de seguridad. Para obtener más información, consulte *iDRAC Online Help (Ayuda en línea de iDRAC)*.
- Delete (Eliminar): elimina la licencia. Para obtener más información, consulte *iDRAC Online Help (Ayuda en línea de iDRAC)*.
- Más información: obtenga más información acerca de la licencia instalada o las licencias disponibles para un componente instalado en el servidor. Puede visitar delltechcenter.com.

  NOTA: Para que la opción Learn More (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 una a varias, puede utilizar Dell License Manager. Para obtener más información, consulte *Dell License Manager User's Guide (Guía del usuario de Dell License Manager)*, disponible en **dell.com/support/manuals**.

Estado o condición del componente de licencia y operaciones disponibles

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

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

Para administrar licencias mediante la interfaz web de iDRAC, vaya a **Configuration (Configuración)** > **Licenses (Licencias)**.

En la página **Licenses (Licencias)**, se muestran las licencias que están asociadas a dispositivos o las licencias que están instaladas, pero para las que no hay dispositivos presentes en el sistema. Para obtener más información sobre la importación, la exportación o la eliminación de una licencia, consulte *iDRAC Online Help (Ayuda en línea de iDRAC)*.

Administración de licencias mediante RACADM

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

Funciones con licencia en iDRAC8 e iDRAC9

En la tabla siguiente se proporcionan las funciones de iDRAC8 e iDRAC9 activadas según la licencia adquirida.

Tabla 2. Funciones con licencia en iDRAC8 e iDRAC9

Función	iDRAC8 Basic	iDRAC9 Basic	iDRAC8 Express	iDRAC9 Express	iDRAC8 Express para servidores blade	iDRAC9 Express para servidores blade	iDRAC8 Enterprise	iDRAC9 Enterprise
Interfaces/estándares								
Redfish	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
IPMI 2.0	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
DCMI 1.5	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Interfaz gráfica web del usuario	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Función	iDRAC8 Basic	iDRAC9 Basic	iDRAC8 Express	iDRAC9 Express	iDRAC8 Express para servidores blade	iDRAC9 Express para servidores blade	iDRAC8 Enterprise	iDRAC9 Enterprise
Línea de comandos de RACADM (local/remota)	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
SMASH-CLP (solo SSH)	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Telnet	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
SSH	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Redirección serie	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
WSMan	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Protocolo de tiempo de la red	No	No	Sí	Sí	Sí	Sí	Sí	Sí
Conectividad								
NIC compartida (LOM)	Sí	Sí	Sí	Sí	N/A	N/A	Sí	Sí[1]
NIC dedicado[2]	Sí	Sí	Sí	Sí	Sí	Sí	Sí[2]	Sí[2]
Etiquetado VLAN	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
IPv4	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
IPv6	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
DHCP	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
DHCP sin intervención	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
DNS dinámico	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Paso a través del sistema operativo	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
iDRAC Direct: USB en panel frontal	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Vista de conexión	No	Sí	No	Sí	No	Sí	No	Sí
NFS v4	No	Sí	No	Sí	No	Sí	No	Sí
SMB3.0 con NTLMv1 y NTLMv2	No	Sí	No	Sí	No	Sí	No	Sí
Seguridad								
Autoridad basada en roles	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Usuarios locales	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Cifrado SSL	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Bloqueo de IP	No	No	Sí	Sí	Sí	Sí	Sí	Sí
Servicios de directorio (AD, LDAP)	No	No	No	No	No	No	Sí	Sí

Función	iDRAC8 Basic	iDRAC9 Basic	iDRAC8 Express	iDRAC9 Express	iDRAC8 Express para servidores blade	iDRAC9 Express para servidores blade	iDRAC8 Enterprise	iDRAC9 Enterprise
Autentificación de dos factores (tarjeta inteligente)	No	No	No	No	No	No	Sí	Sí
Inicio de sesión único	No	No	Sí	No	No	No	Sí	Sí
Autentificación de PK (para SSH)	No	No	Sí	Sí	Sí	Sí	Sí	Sí
FIPS 140-2	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Inicio seguro de UEFI: administración de certificados	No	Sí	No	Sí	No	Sí	No	Sí
Modo de bloqueo	No	No	No	No	No	No	No	Sí
Contraseña predeterminada exclusiva de iDRAC	No	Sí	No	Sí	No	Sí	No	Sí
Banner de política de seguridad personalizable: página de inicio de sesión	No	Sí	No	Sí	No	Sí	No	Sí
Quick Sync 2 de iDRAC: autorización opcional para operaciones de lectura	No	Sí	No	Sí	No	Sí	No	Sí
Quick Sync 2 de iDRAC: adición de número de dispositivo móvil a LCL	No	Sí	No	Sí	No	Sí	No	Sí
Presencia remota								
Control de alimentación	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Control de inicio	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Comunicación en serie en la LAN	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Soportes virtuales	No	No	No	No	Sí	Sí	Sí	Sí
Carpetas virtuales	No	No	No	No	No	No	Sí	Sí
Recurso compartido de archivos remotos	No	No	No	No	No	No	Sí	Sí
Acceso de HTML5 a consola virtual	No	No	No	No	Sí	Sí	Sí	Sí
Consola virtual	No	No	No	No	Sí	Sí	6 usuarios	Sí
Conexión VNC al sistema operativo	No	No	No	No	No	No	Sí	Sí

Función	iDRAC8 Basic	iDRAC9 Basic	iDRAC8 Express	iDRAC9 Express	iDRAC8 Express para servidores blade	iDRAC9 Express para servidores blade	iDRAC8 Enterprise	iDRAC9 Enterprise
Control de calidad/ancho de banda	No	No	No	No	No	No	Sí	Sí
Colaboración de consola virtual (hasta seis usuarios en simultáneo)	No	No	No	No	No	No	Sí	Sí
Chat de consola virtual	No	No	No	No	No	No	Sí	Sí [2,3]
Particiones de flash virtual	No	No	No	No	No	No	Sí [1,2]	Sí
Group Manager	No	No	No	No	No	No	No	Sí
Compatibilidad de HTTP/HTTPS junto con NFS/CIFS	No	Sí	No	Sí	No	Sí	No	Sí
Alimentación y elementos térmicos								
Medidor de alimentación en tiempo real	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Umbrales y alertas de alimentación	No	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Gráficos de alimentación en tiempo real	No	No	Sí	Sí	Sí	Sí	Sí	Sí
Contadores de datos históricos de alimentación	No	No	Sí	Sí	Sí	Sí	Sí	Sí
Límites de alimentación	No	No	No	No	No	No	Sí	Sí
Integración de Power Center	No	No	No	No	No	No	Sí	Sí
Supervisión de la temperatura	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Gráficos de temperatura	No	No	Sí	Sí	Sí	Sí	Sí	Sí
Supervisión de la condición								
Supervisión completa sin agentes	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Supervisión predictiva de fallas	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
SNMPv1 y v2 y v3 (capturas y obtenciones)	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Función	iDRAC8 Basic	iDRAC9 Basic	iDRAC8 Express	iDRAC9 Express	iDRAC8 Express para servidores blade	iDRAC9 Express para servidores blade	iDRAC8 Enterprise	iDRAC9 Enterprise
Alertas de correo electrónico	No	No	Sí	Sí	Sí	Sí	Sí	Sí
Umbrales configurables	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Supervisión de ventiladores	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Supervisión de suministros de energía	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Supervisión de memoria	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Supervisión de CPU	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Supervisión de RAID	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Supervisión de NIC	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Supervisión de discos duros (gabinete)	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Supervisión de rendimiento fuera de banda	No	No	No	No	No	No	Sí	Sí
Alertas de desgaste excesivo de SSD	No	Sí	No	Sí	No	Sí	No	Sí
Configuración personalizable para temperatura de salida	No	Sí	No	Sí	No	Sí	No	Sí
Actualizar								
Actualización remota sin agentes	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Herramientas de actualización incorporadas	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Sincronización con un repositorio (actualizaciones programadas)	No	No	No	No	No	No	Sí	Sí
Actualización automática	No	No	No	No	No	No	Sí	Sí
Actualizaciones mejoradas del firmware de PSU	No	Sí	No	Sí	No	Sí		Sí

Función	iDRAC8 Basic	iDRAC9 Basic	iDRAC8 Express	iDRAC9 Express	iDRAC8 Express para servidores blade	iDRAC9 Express para servidores blade	iDRAC8 Enterprise	iDRAC9 Enterprise
Implementación y configuración								
Configuración local a través de F10	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Herramientas incorporadas de implementación del sistema operativo	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Herramientas de configuración incorporadas	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Descubrimiento automático	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí
Implementación remota del sistema operativo	No	No	Sí	Sí	Sí	Sí	Sí	Sí
Paquete incorporado de controladores	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Configuración completa del inventario	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Exportación de inventario	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Configuración remota	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Configuración sin intervención	No	No	No	No	No	No	Sí	Sí
Retiro/reasignación del sistema	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Perfil de configuración del servidor en la GUI	No	Sí	No	Sí	No	Sí	No	Sí
Diagnóstico, servicio y registro								
Herramientas de diagnóstico incorporadas	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Reemplazo de piezas	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí

Función	iDRAC8 Basic	iDRAC9 Basic	iDRAC8 Express	iDRAC9 Express	iDRAC8 Express para servidores blade	iDRAC9 Express para servidores blade	iDRAC8 Enterprise	iDRAC9 Enterprise
NOTA: Después de la realización de un reemplazo de piezas en el hardware RAID, una vez que se haya completado el proceso para el reemplazo del firmware y la configuración, los registros de Lifecycle informan entradas dobles de reemplazo de piezas, lo cual es un comportamiento esperado.								
Copia de seguridad de la configuración del servidor	No	No	No	No	No	No	Sí	Sí
Easy Restore (configuración del sistema)	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Restauración de la configuración del servidor	No	Sí	No	Sí	Sí	Sí	Sí	Sí
Restauración fácil del tiempo de espera automático	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí
Indicadores LED de estado de la condición	Sí	Sí [5]	Sí	Sí [5]	No	N/A	Sí	Sí [5]
Pantalla LCD (iDRAC9 requiere opcional).	Sí	Sí [5]	Sí	Sí [5]	N/A	N/A	Sí	Sí [5]
Quick Sync (requiere bisel de NFC, bisel de 13 G únicamente).	Sí	N/A	Sí	N/A	No	N/A	Sí	N/A
Quick Sync 2 de iDRAC (hardware de Wi-Fi/ BLE)	N/A	Sí	N/A	Sí	No	Sí	N/A	Sí
iDRAC directo (puerto de administración de USB frontal)	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Función	iDRAC8 Basic	iDRAC9 Basic	iDRAC8 Express	iDRAC9 Express	iDRAC8 Express para servidores blade	iDRAC9 Express para servidores blade	iDRAC8 Enterprise	iDRAC9 Enterprise
Módulo de servicio de iDRAC (iSM) integrado	N/A	Sí	N/A	Sí	No	Sí	N/A	Sí
Transferencia de alertas de iSM en banda a consolas	No	Sí	No	Sí	No	Sí	No	Sí
Informe de SupportAssist (integrado)	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Captura de pantalla de bloqueo	No	No	Sí	Sí	Sí	Sí	Sí	Sí
Captura de video de bloqueo[4]	N/A	No	N/A	No	No	No	Sí	Sí
Captura de inicio	No	No	No	No	No	No	Sí	Sí
Restablecimiento manual de iDRAC (botón de Id. de LCD)	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Restablecimiento remoto de iDRAC (requiere iSM).	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
NMI virtual	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Vigilancia del sistema operativo[4]	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Registro de sucesos del sistema	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Registro de Lifecycle	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Inicio de sesión mejorado en el registro de Lifecycle Controller	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Notas de trabajo	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Syslog remoto	No	No	No	No	No	No	Sí	Sí
Administración de licencias	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

[1] Requiere medios de la tarjeta SD vFlash.

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

[3] La función de actualización sin agente remoto está disponible sólo mediante IPMI.

[4] Disponible sólo mediante IPMI.

[5] Requiere el agente OMSA en el servidor de destino.

Interfaces y protocolos para acceder a iDRAC

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

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

Tabla 3. Interfaces y protocolos para acceder a iDRAC

Interfaz o protocolo	Descripción
Utilidad de configuración de iDRAC (F2)	Utilice la utilidad de configuración de iDRAC para realizar operaciones previas al sistema operativo. Posee un subconjunto de funciones disponibles en la interfaz web de iDRAC, además de otras funciones. Para acceder a la utilidad de configuración de iDRAC, presione <F2> durante el inicio y luego haga clic en **iDRAC Settings (Configuración de iDRAC)** en la página **System Setup Main Menu (Menú principal de configuración del sistema)**.
Lifecycle Controller (F10)	Utilice Lifecycle Controller para realizar las configuraciones de iDRAC. Para acceder a Lifecycle Controller, presione <F10> durante el inicio y vaya a **System Setup (Configuración del sistema)** > **Advanced Hardware Configuration (Configuración avanzada de hardware)** > **iDRAC Settings (Configuración de iDRAC)**. Para obtener más información, consulte *Lifecycle Controller User's Guide (Guía del usuario de Lifecycle Controller)*, disponible en **dell.com/idracmanuals**.
Interfaz web de iDRAC	Utilice la interfaz web de iDRAC para administrar iDRAC y controlar el sistema administrado. El explorador se conecta al servidor web a través del puerto HTTPS. Los flujos de datos se cifran mediante SSL de 128 bits para proporcionar privacidad e integridad. Todas las conexiones al puerto HTTP se redireccionan a HTTPS. Los administradores pueden cargar su propio certificado SSL a través de un proceso de generación de SSL CSR para proteger el servidor web. Se puede modificar el valor predeterminado de los puertos HTTP y HTTPS. El acceso del usuario se basa en los privilegios del usuario.
Interfaz web de la CMC	Además de supervisar y administrar el chasis, utilice la interfaz web de la CMC para realizar lo siguiente: • Ver el estado de un sistema administrado • Actualizar el firmware del iDRAC • Establecer la configuración de red de iDRAC • Iniciar sesión en la interfaz web de iDRAC • Iniciar, detener o restablecer el sistema administrado • Actualizar el BIOS, PERC y otros adaptadores de red compatibles
Panel LCD de servidor/ panel LCD de chasis	Utilice la pantalla LCD en el panel frontal del servidor para realizar lo siguiente: • Ver alertas, la dirección IP o MAC de iDRAC, las cadenas programables del usuario • Configurar DHCP • Configurar la dirección IP de iDRAC Para servidores Blade, la pantalla LCD se encuentra en el panel anterior del chasis y se comparte entre todos los servidores Blade. Para restablecer iDRAC sin reiniciar el servidor, mantenga presionado el botón System Identification (Identificación del sistema) durante 16 segundos.
RACADM	Use esta utilidad de línea de comandos para realizar la administración de iDRAC y del servidor. Puede utilizar RACADM de manera local y remota.

Interfaz o protocolo	Descripción
	• La interfaz de línea de comandos RACADM local se ejecuta en los sistemas administrados que tengan instalado Server Administrator. RACADM local se comunica con iDRAC a través de su interfaz de host IPMI dentro de banda. Dado que está instalado en el sistema administrado local, los usuarios deben iniciar sesión en el sistema operativo para ejecutar esta utilidad. Un usuario debe disponer de privilegios de administrador completo para utilizar esta utilidad. • El RACADM remoto es una utilidad cliente que se ejecuta en una estación de administración. Utiliza la interfaz de red fuera de banda para ejecutar los comandos de RACADM en los sistemas administrados y el canal HTTPS. La opción **–r** ejecuta el comando RACADM sobre una red. • El RACADM de firmware no es accesible al iniciar sesión en iDRAC mediante SSH o Telnet. Puede ejecutar los comandos de RACADM de firmware sin especificar la dirección IP, el nombre de usuario o la contraseña de iDRAC. • No debe especificar la dirección IP, el nombre de usuario o la contraseña de iDRAC para ejecutar los comandos de RACADM de firmware. Después de entrar en el símbolo del sistema de RACADM, puede ejecutar directamente los comandos sin el prefijo racadm.
Redfish	La API de Redfish Scalable Platforms Management es un estándar definido por Distributed Management Task Force (DMTF). Redfish es un estándar de interfaz de administración de sistemas de última generación, que permite que una administración de servidores escalable, segura y abierta. Se trata de una nueva interfaz que utiliza semántica de interfaz RESTful para acceder a los datos que se ha definido en el formato de modelo para realizar la administración de sistemas fuera de banda. Es adecuado para un amplio rango de servidores que van de servidores independientes a montados en rack y entornos blade y entornos de nube de gran escala. Redfish proporciona las siguientes ventajas sobre los métodos de administración de servidores existentes: • Mayor simplicidad y facilidad • Alta seguridad de datos • Interfaz programable que puede usar fácilmente con secuencias de comandos • Adhesión a estándares de uso muy difundido Para obtener más información, consulte lo siguiente: • Redfish API Reference Guide (Guía de referencia de la API de Redfish), disponible en **dell.com/support/manuals**.
WSMan	La funcionalidad LC-Remote Services (Servicios remotos LC) se basa en el protocolo WSMan para realizar tareas de administración de uno a varios sistemas. Debe utilizar el cliente WSMan como cliente WinRM (Windows) o cliente OpenWSMan (Linux) para utilizar la funcionalidad LC-Remote Services (Servicios remotos LC). También puede utilizar PowerShell y Python para crear secuencias de comandos para la interfaz de WSMan. Web Services for Management (WSMan) es un protocolo basado en el protocolo simple de acceso a objetos (SOAP) que se utiliza para la administración de sistemas. La iDRAC utiliza WSMan 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 WSMan los proporciona la interfaz de instrumentación de iDRAC asignada a los perfiles de extensión y DMTF. Para obtener más información, consulte lo siguiente: • Lifecycle Controller-Remote Services User's Guide (Guía del usuario de Lifecycle Controller Remote Services) disponible en **dell.com/idracmanuals**. • Lifecycle Controller Integration Best Practices Guide (Guía de prácticas recomendadas para la integración de Lifecycle Controller) disponible en **dell.com/support/manuals**. • Página de Lifecycle Controller en Dell TechCenter: **delltechcenter.com/page/Lifecycle+Controller** • Centro de secuencias de comandos WSMan de Lifecycle Controller: **delltechcenter.com/page/Scripting+the+Dell+Lifecycle+Controller** • MOF y perfiles: **delltechcenter.com/page/DCIM.Library** • Sitio web de DTMF: **dmtf.org/standards/profiles/**

Interfaz o protocolo	Descripción
SSH	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. El servicio SSH está activado de forma predeterminada en iDRAC. El servicio SSH se puede desactivar en iDRAC. La iDRAC solo admite SSH, versión 2, con el algoritmo de clave de host RSA. Al encender iDRAC por primera vez, se genera una clave de host única RSA de 1024 bits.
Telnet	Utilice Telnet para acceder a iDRAC, donde puede ejecutar comandos RACADM y SMCLP. Para obtener información detallada acerca de RACADM, consulte *iDRAC RACADM Command Line Interface Reference Guide (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC)*, disponible en **dell.com/idracmanuals**. Para obtener información acerca de SMCLP, consulte Uso de SMCLP. **NOTA: Telnet no es un protocolo seguro y está desactivado de manera predeterminada. Transmite todos los datos, incluidas las contraseñas, en texto sin formato. Al transmitir información confidencial, utilice la interfaz SSH.**
VMCLI	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.
IPMITool	Utilice IPMITool para acceder a las funciones de administración básicas del sistema remoto a través de iDRAC. La interfaz incluye IPMI local, IPMI en la LAN, IPMI en comunicación en serie y comunicación en serie en la LAN. Para obtener más información acerca de IPMITool, consulte *Dell OpenManage Baseboard Management Controller Utilities User's Guide (Guía del usuario de las utilidades de la controladora de administración de la placa base de Dell OpenManage)*, disponible en **dell.com/idracmanuals**. **NOTA: No se admite IPMI versión 1.5.**
SMCLP	Utilice el protocolo de línea de comandos de administración de servidores (SMCLP) de Server Management Workgroup para realizar tareas de administración de sistemas. Esto está disponible a través de SSH o Telnet. Para obtener más información sobre SMCLP, consulte Uso de SMCLP.
NTLM	La iDRAC permite NTLM para proporcionar autenticación, integridad y confidencialidad a los usuarios. NT LAN Manager (**NTLM**) es un conjunto de protocolos de seguridad de Microsoft y funciona en una red de Windows.
SMB	La iDRAC9 admite el protocolo de bloqueo de mensajes de servidor (SMB). Se trata de un protocolo de uso compartido de archivos de red.
NFS	La iDRAC9 es compatible con el **Sistema de archivos de red** (**NFS**). Se trata de un protocolo de sistema de archivos distribuido que permite a los usuarios **montar** directorios remotos en los servidores.

Información sobre puertos iDRAC

Se requieren los siguientes puertos para acceder a iDRAC de forma remota por medio de servidores de seguridad. Son los puertos predeterminados que iDRAC escucha para las conexiones. Opcionalmente, puede modificar la mayoría de los puertos. Para ello, consulte Configuración de servicios.

Tabla 4. Puertos que iDRAC utiliza en espera para las conexiones

Número de puerto	Función
22*	SSH
23*	Telnet
80*	HTTP

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

* Puerto configurable

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

Tabla 5. Puertos que iDRAC utiliza como cliente

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

* Puerto configurable

Otros documentos que podrían ser de utilidad

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

- En la *Ayuda en línea de iDRAC* se proporciona información acerca de los campos disponibles en la interfaz web de iDRAC y sus descripciones. Puede acceder a la ayuda en línea después de instalar iDRAC.
- En *Redfish API Reference Guide (Guía de referencia de la API de Redfish)*, se proporciona información sobre la API de Redfish.
- En *iDRAC RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC) se proporciona información acerca de los subcomandos RACADM, las interfaces admitidas y los grupos de bases de datos de propiedades y las definiciones de objetos de iDRAC.

- La *Tabla de compatibilidades de RACADM para iDRAC* incluye la lista de comandos y objetos que son aplicables para una determinada versión de iDRAC.
- En la *Systems Management Overview Guide* (Guía de información general de Systems Management) se proporciona información acerca de los distintos programas de software disponibles para realizar tareas de administración de sistemas.
- *Dell Remote Access Configurarlos Tool User's Guide* (Guía del usuario de la herramienta de configuración de Dell Remote Access) proporciona información sobre cómo utilizar la herramienta para descubrir las direcciones IP de iDRAC en la red, realizar actualizaciones del firmware de uno a varios y activar la configuración del directorio para las direcciones IP descubiertas.
- La *Matriz de compatibilidad de software de los sistemas Dell* ofrece información sobre los diversos sistemas Dell, los sistemas operativos compatibles con esos sistemas y los componentes de Dell OpenManage que se pueden instalar en estos sistemas.
- *iDRAC Service Module Installation Guide* (Guía de instalación del módulo de servicio del iDRAC) proporciona información para instalar el módulo de servicio del iDRAC.
- En la *Guía de instalación de Dell OpenManage Server Administrator* se incluyen instrucciones para ayudar a instalar Dell OpenManage Server Administrator.
- En la *Guía de instalación de Dell OpenManage Management Station Software* se incluyen instrucciones para ayudar a instalar este software que incluye la utilidad de administración de la placa base, herramientas de DRAC y el complemento de Active Directory.
- En la *Dell OpenManage Baseboard Management Controller Management Utilities User's Guide* (Guía del usuarios de las utilidades de administración de OpenManage Baseboard Management Controller) se incluye información acerca de la interfaz IPMI.
- Las *Notas de publicación* proporcionan actualizaciones de última hora relativas al sistema o a la documentación o material avanzado de consulta técnica destinado a técnicos o usuarios experimentados.
- En el *Glossary* (Glosario) se proporciona información acerca de los términos utilizados en este documento.

Están disponibles los siguientes documentos para proporcionar más información:

- Las instrucciones de seguridad incluidas con el sistema proporcionan información importante sobre la seguridad y las normativas. Para obtener más información sobre las normativas, consulte la página de inicio de cumplimento normativo en **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.
- En el *Owner's Manual* (Manual de propietario) se proporciona información acerca de las funciones del sistema y se describe cómo solucionar problemas del sistema e instalar o sustituir componentes.

Referencia de medios sociales

Para conocer más sobre el producto y las mejoras prácticas, y obtener información sobre las soluciones y los servicios Dell, puede acceder a las plataformas de medios sociales tales como Dell TechCenter. Puede acceder a blogs, foros, notas técnicas, videos explicativos, etc. desde la página wiki de iDRAC en **www.delltechcenter.com/idrac**.

Para consultar documentos de iDRAC y otro firmware relacionado, visite **dell.com/idracmanuals** y **dell.com/esmmanuals**.

Cómo ponerse en contacto con Dell

NOTA: Si no tiene una conexión a Internet activa, puede encontrar información de contacto en su factura de compra, en su albarán de entrega, en su recibo o en el catálogo de productos Dell.

Dell proporciona varias opciones de servicio y asistencia en línea y por teléfono. La disponibilidad varía según el país y el producto y es posible que algunos de los servicios no estén disponibles en su área. Si desea ponerse en contacto con Dell para tratar cuestiones relacionadas con las ventas, la asistencia técnica o el servicio de atención al cliente:

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

Acceso a documentos desde el sitio de asistencia de Dell

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

- Mediante los siguientes enlaces:
  - Para todos los documentos de Enterprise Systems Management: **Dell.com/SoftwareSecurityManuals**
  - Para documentos de OpenManage: Dell.com/OpenManageManuals
  - Para documentos de Remote Enterprise System Management: **Dell.com/esmmanuals**
  - Para consultar los documentos de iDRAC y Lifecycle Controller: Dell.com/idracmanuals
  - Para documentos de OpenManage Connections Enterprise Systems Management: **Dell.com/OMConnectionsEnterpriseSystemsManagement**
  - Para documentos de Herramientas de servicio: **Dell.com/ServiceabilityTools**
  - Para documentos de Client Command Suite Systems Management: **Dell.com/DellClientCommandSuiteManuals**
- En el sitio web de asistencia de Dell:
  a. Vaya a **Dell.com/Support/Home**.
  b. En **Select a product (Seleccionar un producto)**, haga clic en **Software & Security (Software y seguridad)**.
  c. En el grupo **Software & Security (Software y seguridad)**, haga clic en el enlace requerido que corresponda:
     - **Enterprise Systems Management (Administración de sistemas empresariales)**
     - **Remote Enterprise Systems Management (Administración remota de sistemas empresariales)**
     - **Serviceability Tools (Herramientas de servicio)**
     - **Dell Client Command Suite (Conjunto de comandos del cliente de Dell)**
     - **Connections Client Systems Management (Administración de las conexiones de sistemas del cliente)**
  d. Para ver un documento, haga clic en la versión del producto requerida.
- Mediante los motores de búsqueda:
  - Escriba el nombre y la versión del documento en el cuadro de búsqueda.

2

Inicio de sesión en iDRAC

Puede iniciar sesión en iDRAC como usuario de iDRAC, como usuario de Microsoft Active Directory o como usuario de protocolo ligero de acceso a directorios (LDAP). También puede iniciar sesión mediante inicio de sesión único o tarjeta inteligente.

Para mejorar la seguridad, cada sistema se entrega con una contraseña exclusiva para iDRAC, que está disponible en la etiqueta de información del sistema. Esta contraseña exclusiva mejora la seguridad de iDRAC y del servidor. El nombre de usuario predeterminado es *root*.

Al pedir el sistema, tiene la opción de conservar la contraseña heredada (calvin) como la contraseña predeterminada. Si opta por conservar la contraseña heredada, la contraseña no estará disponible en la etiqueta de información del sistema.

En esta versión, DHCP está activado de manera predeterminada y la dirección IP para iDRAC se asignará dinámicamente.

NOTA:

- Debe disponer del privilegio Iniciar sesión en iDRAC para poder iniciar sesión en iDRAC.
- La GUI de iDRAC no admite los botones del explorador como **Atrás**, **Siguiente** o **Actualizar**.

NOTA: Para obtener más información sobre los caracteres recomendados para los nombres de usuario y las contraseñas, consulte Caracteres recomendados para nombres de usuario y contraseñas.

Para cambiar la contraseña predeterminada, consulte Cambio de la contraseña de inicio de sesión predeterminada.

Personalización del banner de seguridad

Puede personalizar el aviso de seguridad que aparece en la página de inicio de sesión. Puede utilizar RACADM, Redfish o WSMan para personalizar el aviso. Según el idioma que utilice, el aviso puede contener 1024 o 512 caracteres UTF-8.

Temas:

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

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

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

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

NOTA: Se admite la autenticación de LDAP con openDS. La clave DH debe ser mayor que 768 bits.

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

1 Abra un explorador de web compatible.

2 En el campo **Address (Dirección)**, escriba `https://[iDRAC-IP-address]` y presione <Intro>.

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

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

3 Para un usuario local:

- En los campos **Nombre de usuario** y **Contraseña**, introduzca el nombre de usuario y la contraseña de iDRAC.
- En el menú desplegable **Dominio**, seleccione **Este iDRAC**.

4 Para un usuario de Active Directory, en los campos **Username (Nombre de usuario)** y **Password (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 la opción **This iDRAC (Esta iDRAC)** en el menú desplegable. El formato del nombre de usuario puede ser el siguiente: <dominio>\<nombredeusuario>, <dominio>/<nombredeusuario> 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 de LDAP, en los campos **Username (Nombre de usuario)** y **Password (Contraseña)**, introduzca el nombre de usuario y la contraseña de LDAP. Para el inicio de sesión de LDAP, no se necesita el nombre de dominio. De manera predeterminada, se selecciona la opción **This iDRAC (Esta iDRAC)** en el menú desplegable.

6 Haga clic en **Enviar**. Ha iniciado sesión en iDRAC con los privilegios de usuario necesarios.

Si inicia sesión con el privilegio de configuración de usuarios y las credenciales predeterminadas de la cuenta, y si está activada la función de advertencia de contraseña predeterminada, aparecerá la página **Advertencia de contraseña predeterminada** donde puede cambiar fácilmente la contraseña.

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

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

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

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

NOTA: De acuerdo con la configuración del explorador, el sistema puede solicitarle que descargue e instale el complemento ActiveX para lector de tarjeta inteligente cuando utiliza esta función por primera vez.

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

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

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

2 Inserte la tarjeta inteligente en el lector y haga clic en **Iniciar sesión**.
Se muestra una petición para el PIN de la tarjeta inteligente. No es necesario especificar una contraseña.

3 Introduzca el PIN para los usuarios de tarjeta inteligente.
Ahora está conectado a iDRAC.

> **NOTA: Si usted es un usuario local para el que se ha activado la opción Enable CRL check for Smart Card Logon (Activar revisión CRL para inicio de sesión mediante tarjeta inteligente), iDRAC intenta descargar CRL y busca en ella el certificado del usuario. El inicio de sesión falla si el certificado se indica como revocado en CRL o si CRL no se puede descargar por algún motivo.**

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

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

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

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

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

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

2 Inserte la tarjeta inteligente y haga clic en **Iniciar sesión**.
Aparece la página **PIN**.

3 Introduzca el PIN y haga clic en **Enviar**.
Ha iniciado sesión en iDRAC con sus credenciales de Active Directory.

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

Inicio de sesión en iDRAC mediante inicio de sesión único

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

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

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

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

Para iniciar sesión en iDRAC mediante la interfaz web:

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

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

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

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

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

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

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

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

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

Acceso a iDRAC mediante RACADM remoto

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

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

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

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

Validación del certificado de CA para usar RACADM remoto en Linux

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

Para validar el certificado para usar RACADM remoto:

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

```
openssl x509 -inform pem -in [yourdownloadedderformatcert.crt] -outform pem -out
[outcertfileinpemformat.pem] -text
```

2 Busque la ubicación del conjunto de certificados de CA predeterminados en la estación de administración. Por ejemplo: para RHEL5 de 64 bits, es **/etc/pki/tls/cert.pem**.

3 Agregue el certificado CA con formato PEM al certificado CA de la estación de administración.

Por ejemplo: utilice `cat command: cat testcacert.pem >> cert.pem`.

4 Genere y cargue el certificado de servidor en iDRAC.

Acceso a iDRAC mediante RACADM local

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

Acceso a iDRAC mediante RACADM de firmware

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

Inicio de sesión en iDRAC mediante la autentificación de clave pública

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

Por ejemplo:

Inicio de sesión:

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

o

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

donde `IP_address` es la dirección IP de iDRAC.

Envío de comandos RACADM:

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

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

Varias sesiones de iDRAC

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

Tabla 6. Varias sesiones de iDRAC

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

Acceso a iDRAC mediante SMCLP

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

Contraseña predeterminada segura

Todos los sistemas compatibles se envían con una contraseña predeterminada exclusiva para iDRAC, a menos que usted seleccione configurar *calvin* como la contraseña al pedir el sistema. La contraseña exclusiva ayuda a mejorar la seguridad de iDRAC y su servidor. Para mejorar aún más la seguridad, se recomienda cambiar la contraseña predeterminada.

La contraseña exclusiva de su sistema está disponible en la etiqueta de información del sistema. Para localizar la etiqueta, consulte la documentación de su servidor en **dell.com/support/manuals**.

NOTA: El restablecimiento de la iDRAC a los valores predeterminados de fábrica vuelve la contraseña predeterminada al valor con la que se envió el servidor.

Si ha olvidado la contraseña y no tiene acceso a la etiqueta de información del sistema, hay algunos métodos para restablecer la contraseña de manera local o remota.

Restablecimiento de la contraseña de iDRAC predeterminada a nivel local

Si tiene acceso físico al sistema, puede restablecer la contraseña mediante lo siguiente:

- Utilidad de configuración de iDRAC (configuración del sistema)
- RACADM local
- OpenManage Mobile
- Puerto USB de administración de servidores
- USB-NIC

Restablecimiento de la contraseña predeterminada mediante la utilidad de configuración de iDRAC

Acceda a esta utilidad mediante la configuración del sistema de su servidor. Para obtener más información, consulte la sección **System Setup (Configuración del sistema)** de la documentación de su sistema en **dell.com/support/manuals**.

Restablecimiento de la contraseña predeterminada mediante la RACADM local

1 Inicie sesión en el sistema operativo host instalado en el sistema.
2 Acceda a la interfaz de RACADM local.
3 Siga las instrucciones que se incluyen en Cambio de la contraseña de inicio de sesión predeterminada mediante RACADM.

Restablecimiento de la contraseña predeterminada mediante OpenManage Mobile

Puede utilizar OpenManage Mobile (OMM) para iniciar sesión y cambiar la contraseña predeterminada. Para iniciar sesión en iDRAC mediante OMM, escanee el código QR de la etiqueta de información del sistema. Para obtener más información sobre el uso de OMM, consulte la documentación de OMM en **Dell.com/openmanagemanuals**.

NOTA: El escaneo del código QR inicia sesión en iDRAC solo si las credenciales predeterminadas se encuentran en los valores predeterminados. Si ha modificado sus valores predeterminados, especifique las credenciales actualizadas.

Restablecimiento de la contraseña predeterminada mediante el puerto USB de administración de servidores

NOTA: Estos pasos requieren que el puerto USB de administración esté activado y configurado.

Mediante el archivo de perfil de configuración del servidor

Cree un archivo de perfil de configuración del servidor (SCP) con una nueva contraseña para la cuenta predeterminada, colóquelo en una llave de memoria y utilice el puerto USB de administración de servidores en el servidor para cargar el archivo de SCP. Para obtener más información sobre la creación del archivo, consulte Uso de un puerto USB para la administración del servidor.

Acceso a iDRAC mediante una computadora portátil

Conecte una computadora portátil al puerto USB de administración de servidores y acceda a iDRAC para cambiar la contraseña. Para obtener más información, consulte Acceso a la interfaz de iDRAC por medio de la conexión USB directa.

Cambio de la contraseña predeterminada mediante USB-NIC

Si usted tiene acceso a un teclado, un mouse y un dispositivo de pantalla, conecte al servidor con USB-NIC para acceder a la interfaz de iDRAC y cambiar la contraseña predeterminada.

1 Conecte los dispositivos al sistema.
2 Utilice un navegador compatible para acceder a la interfaz de iDRAC con la IP de iDRAC.

3 Siga las instrucciones que se incluyen en Cambio de la contraseña de inicio de sesión predeterminada mediante la interfaz web.

Restablecimiento de la contraseña predeterminada de iDRAC de forma remota

Si no tiene acceso físico al sistema, puede restablecer la contraseña predeterminada de forma remota.

Sistema remoto: con aprovisionamiento

Si tiene un sistema operativo instalado en el sistema, utilice un cliente de escritorio remoto para iniciar sesión en el servidor. Después de iniciar sesión en el servidor, utilice cualquiera de las interfaces locales como RACADM o la interfaz web para cambiar la contraseña.

Sistema remoto: no aprovisionado

Si no hay ningún sistema operativo instalado en el servidor y si tiene una configuración de PXE disponible, utilice PXE y, a continuación, RACADM para restablecer la contraseña.

Cambio de la contraseña de inicio de sesión predeterminada

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

- Inicia sesión en iDRAC con el privilegio Configurar usuario.
- Está activada la función de advertencia de contraseña predeterminada.
- El nombre de usuario y la contraseña predeterminados para iDRAC se proporcionan en la etiqueta de información.

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

NOTA: Para obtener más información sobre los caracteres recomendados para los nombres de usuario y las contraseñas, consulte Caracteres recomendados para nombres de usuario y contraseñas.

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

Cuando se conecta a la interfaz web de iDRAC, si aparece la página **Default Password Warning (Advertencia de contraseña predeterminada)**, puede cambiar la contraseña. Para hacerlo:

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

NOTA: Para obtener más información sobre los caracteres recomendados para los nombres de usuario y las contraseñas, consulte Caracteres recomendados para nombres de usuario y contraseñas.

3 En el campo **Confirmar contraseña**, introduzca nuevamente la contraseña.
4 Haga clic en **Continue (Continuar)**. Se configura la contraseña nueva y queda conectado a iDRAC.

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

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

Cambio de la contraseña de inicio de sesión predeterminada mediante RACADM

Para cambiar la contraseña, ejecute el siguiente comando RACADM:

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

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

NOTA: El índice de la cuenta predeterminada es 2.

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

NOTA: Para obtener más información sobre los caracteres recomendados para los nombres de usuario y las contraseñas, consulte Caracteres recomendados para nombres de usuario y contraseñas.

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

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

1. En la utilidad de configuración de iDRAC, vaya a **Configuración de usuario**.
   Se muestra la página **Configuración de iDRAC - Configuración de usuario**.
2. En el campo **Cambiar contraseña**, introduzca la contraseña nueva.

   NOTA: Para obtener más información sobre los caracteres recomendados para los nombres de usuario y las contraseñas, consulte Caracteres recomendados para nombres de usuario y contraseñas.
3. Haga clic en **Atrás**, en **Terminar** y, a continuación, en **Sí**.
   Los detalles se guardan.

Activación o desactivación del mensaje de advertencia de contraseña predeterminada

Puede activar o desactivar la pantalla del mensaje de aviso de contraseña predeterminada. Para ello, debe contar con el privilegio de configuración de usuarios.

Bloqueo de IP

El bloqueo de IP detecta de forma dinámica cuando se presentan fallas de inicio de sesión provenientes de una dirección IP específica y bloquea (o impide) el inicio de sesión de dicha dirección en iDRAC9 durante un lapso de tiempo predefinido. El bloqueo de IP incluye:

- El número de fallas de inicio de sesión permitidas.
- El período en segundos dentro del que se deben presentar estas fallas.
- La cantidad de tiempo en segundos durante el que se impide que la dirección IP "problemática" establezca una sesión después de haber excedido el número total de fallas permitidas.

A medida que se acumulan las fallas de inicio de sesión de una dirección IP específica, estas se registran mediante un contador interno. Cuando el usuario inicie sesión correctamente, el historial de fallas se borrará y el contador interno se restablecerá.

NOTA: Cuando se rechazan los intentos de inicio de sesión provenientes de la dirección IP cliente, algunos clientes de SSH pueden mostrar el siguiente mensaje:

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

.

Tabla 7. Propiedades de restricción de reintentos de inicio de sesión

Propiedad	Definición
`iDRAC.IPBlocking.BlockEnable`	Activa la función de bloqueo de IP. Cuando se presenten fallas consecutivas (`iDRAC.IPBlocking.FailCount`) provenientes de una única dirección IP dentro de un lapso de tiempo específico (`iDRAC.IPBlocking.FailWindow`), todos los intentos posteriores de establecer una sesión que provengan de dicha dirección se rechazarán durante un período establecido (`iDRAC.IPBlocking.PenaltyTime`).
`iDRAC.IPBlocking.FailCount`	Establece el número de fallas de inicio de sesión provenientes de una dirección IP antes de rechazar los intentos de inicio de sesión.
`iDRAC.IPBlocking.FailWindow`	El período en segundos dentro del que se cuentan las fallas. Cuando las fallas superan este límite, se eliminan del contador.
`iDRAC.IPBlocking.PenaltyTime`	Define el período en segundos dentro del que se rechazan todos los intentos de inicio de sesión provenientes de una dirección IP que tenga un número excesivo de fallas.

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

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

1 Vaya a **iDRAC Settings (Configuración de iDRAC)** > **Connectivity (Conectividad)** > **Network (Red)** > **OS to iDRAC Pass-through (Paso del sistema operativo a iDRAC)**.

Se mostrará la página **Paso del sistema operativo a iDRAC**.

2 Seleccione cualquiera de las siguientes opciones para activar el paso del sistema operativo al iDRAC:

- **LOM**: el vínculo de paso del sistema operativo al iDRAC entre el iDRAC y el sistema operativo host se establece mediante la LOM o NDC.
- **NIC de USB**: el vínculo de paso del sistema operativo al iOS entre el iDRAC y el sistema operativo host se establece mediante la DRAC o USB.

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

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

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

4 Si selecciona **NIC de USB** como configuración de paso, introduzca la dirección IP de la NIC del USB.

El valor predeterminado es 169.254.0.1. Se recomienda utilizar la dirección IP predeterminada. Sin embargo, si esta dirección IP entra en conflicto con una dirección IP de otras interfaces del sistema host o la red local, deberá cambiarla.

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

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

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

Activación o desactivación de alertas mediante RACADM

Utilice el comando siguiente:

```
racadm set iDRAC.IPMILan.AlertEnable <n>
```

n=0: Inhabilitado

n=1: Habilitado

3

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
- Administrador del servidor

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

Temas:

Configuración de la dirección IP de iDRAC

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

- Utilidad iDRAC Settings (Configuración de iDRAC)
- Lifecycle Controller (consulte la *Lifecycle Controller User's Guide* (Guía del usuario de Dell Lifecycle Controller)
- Dell Deployment Toolkit (consulte *Dell Deployment Toolkit User's Guide* (Guía del usuario de Dell Deployment Toolkit)
- Panel LCD del chasis o servidor (consulte el *Manual de propietario del hardware* del sistema)

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

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

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

Después de configurar la dirección IP de iDRAC:

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

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

Para configurar la dirección IP de iDRAC:

1 Encienda el sistema administrado.

2 Presione <F2> durante la Power-on Self-test (Autoprueba de encendido - POST).

3 En la página **System Setup Main Menu (Menú principal de Configuración del sistema)**, haga clic en **iDRAC Settings (Configuración de iDRAC)**.

Aparece la página **Configuración de iDRAC**.

4 Haga clic en **Red**.

Aparecerá la página **Red**.

5 Especifique los valores siguientes:

- Configuración de red
- Configuración común
- Configuración de IPv4
- Configuración de IPv6
- Configuración de IPMI
- Configuración de VLAN

6 Haga clic en **Atrás**, en **Terminar** y, a continuación, en **Sí**.

Se guarda la información de red y el sistema se reinicia.

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 host y dirige el tráfico de administración a una red física separada, lo que permite separarlo 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 Dedicated (Dedicado) permite a iDRAC recibir una dirección IP desde la misma subred o una subred diferente, en comparación con las direcciones IP asignadas a NIC o LOM de host.

NOTA: En el caso de servidores blade, la opción Dedicada se muestra como Chasis (dedicado).

- **LOM1**
- **LOM2**
- **LOM3**
- **LOM4**

NOTA: En el caso de servidores tipo bastidor y torre, hay dos opciones LOM (LOM1 y LOM2) o cuatro opciones LOM disponibles según el modelo del servidor. En servidores blade con dos puertos NDC, hay dos opciones LOM (LOM1 y LOM2) disponibles y en un servidor con cuatro puertos NDC, las cuatro opciones LOM están disponibles.

NOTA: LOM compartida no es compatible con las siguientes bNDC si se usan en un servidor de altura completa con dos NDC, ya que no son compatibles con el arbitraje de hardware:

- Intel X520-k 2P bNDC de 10 G

3 En el menú desplegable **Failover Network (Red de protección contra fallas)**, seleccione una de las LOM restantes: Si falla una red, el tráfico se enruta a través de la red de protección contra fallas.

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

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

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

5 Bajo **Velocidad de la red**, seleccione 10 Mbps o 100 Mbps.

NOTA: No puede configurar manualmente la velocidad de la red en 1000 Mbps. Esta opción solo está disponible si la opción Auto Negotiation (Negociación automática) está activada.

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

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

Configuración común

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

Para registrar iDRAC:

1 Active la opción **Registrar DRAC en DNS**.

2 Introduzca el **Nombre DNS del DRAC**.

3 Seleccione **Auto Config Domain Name (Configuración automática de nombre de dominio)** para adquirir automáticamente el nombre de dominio de DHCP. De lo contrario, proporcione el valor para **DNS Domain Name (Nombre de dominio DNS)**.

Configuración de IPv4

Para configurar los valores de IPv4:

1 Seleccione la opción **Activado** en **Activar IPv4**.

NOTA: En sistemas de 14 G, DHCP está activado de manera predeterminada.

2 Seleccione la opción **Enabled (Activado)** en **Enable DHCP (Activar DHCP)**, de modo que DHCP pueda asignar automáticamente la dirección IP, la puerta de enlace y la máscara de subred en iDRAC. De lo contrario, seleccione **Disabled (Desactivado)** e introduzca los valores para las siguientes opciones:

- Dirección IP estática

- Puerta de enlace estática
- Máscara de subred estática

3 De manera opcional, active la opción **Use DHCP to obtain DNS server address (Usar DHCP para obtener la dirección del servidor DNS)** para que el servidor DHCP pueda asignar los valores de **Static Preferred DNS Server (Servidor DNS preferido estático)** y **Static Alternate DNS Server (Servidor DNS alternativo estático)**. De lo contrario, introduzca las direcciones IP para **Static Preferred DNS Server (Servidor DNS preferido estático)** y **Static Alternate DNS Server (Servidor DNS alternativo estático)**.

Configuración de IPv6

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

Para configurar los valores IPv6:

1 Seleccione la opción **Activado** en **Activar IPv6**.

2 Para que el servidor DHCPv6 asigne automáticamente la dirección IP, puerta de enlace y la máscara de subred al iDRAC, seleccione la opción **Activado** en **Activar configuración automática**.

NOTA: Puede configurar IP estática e IP de DHCP al mismo tiempo.

3 En el cuadro **Dirección IP estática 1**, introduzca la dirección IPv6 estática.

4 En el cuadro **Longitud de prefijo estático**, introduzca un valor entre 0 y 128.

5 En el cuadro **Puerta de enlace estática**, introduzca la dirección de la puerta de enlace.

NOTA: Si configura una dirección IP estática, la dirección IP actual 1 muestra una dirección IP estática y la dirección IP 2 muestra una dirección IP dinámica. Si borra la configuración de dirección IP estática, la dirección IP actual 1 muestra una dirección IP dinámica.

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. Puede configurar lo siguiente según sea necesario:

- En el cuadro **Servidor DNS preferido estático**, introduzca la dirección IPv6 del servidor DNS.
- En el cuadro **Servidor DNS alternativo estático**, introduzca el servidor DNS alternativo estático.

Configuración de IPMI

Para configurar los valores de IPMI:

1 Bajo **Activar IPMI en la LAN**, seleccione **Activado**.

2 En **Límite de privilegio de canal**, seleccione **Administrador**, **Operador** o **Usuario**.

3 En el cuadro **Clave de cifrado**, introduzca la clave de cifrado en el formato de 0 a 40 caracteres hexadecimales (sin caracteres en blanco). El valor predeterminado es todo ceros.

Configuración de VLAN

Se puede configurar iDRAC en la infraestructura de VLAN. Para configurar los valores de VLAN, realice los siguientes pasos:

NOTA: En los servidores blade que se establecen como Chassis (Dedicated) (Chasis [dedicado]), los valores de VLAN son de solo lectura y solo se puede cambiar mediante la CMC. Si el servidor está configurado en modo compartido, puede configurar los valores de VLAN en modo compartido en la iDRAC.

1 En **Activar identificación de VLAN**, seleccione **Activado**.

2 En el cuadro **Identificación de VLAN**, introduzca un número válido de 1 a 4094.

3 En el cuadro **Prioridad**, introduzca un número de cuadro de 0 a 7 para establecer la prioridad de la identificación de VLAN.

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

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

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

NOTA: Debe contar con privilegios de administrador de configuración del chasis para definir la configuración de la red de iDRAC desde CMC. La opción Chassis Management Controller (CMC) está disponible solamente para los servidores blade.

1 Inicie sesión en la interfaz web de CMC.

2 Vaya a **iDRAC Settings (Configuración de iDRAC)** > **Settings (Configuración)** > **CMC**.

Aparecerá la página **Implementar iDRAC**.

3 En **iDRAC Network Settings (Configuración de red de iDRAC)**, seleccione **Enable LAN (Activar LAN)** y otros parámetros de la red según los requisitos. Para obtener más información, consulte *CMC Online Help (Ayuda en línea para la CMC)*.

4 Para conocer valores de red adicionales específicos a cada servidor blade, vaya a **Server Overview (Información general de servidor)** > **<nombre del servidor>**.

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

5 Haga clic en **Launch iDRAC (Iniciar iDRAC)** y vaya a **iDRAC Settings (Configuración de iDRAC)** > **Connectivity (Conectividad)** > **Network (Red)**.

6 En la página **Red**, especifique los valores de configuración siguientes:

- Configuración de red
- Configuración común
- Configuración de IPv4
- Configuración de IPv6
- Configuración de IPMI
- Configuración de VLAN
- Configuración avanzada de red

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

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

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

Activación de servidor de aprovisionamiento

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

El servidor de aprovisionamiento 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 IP del servidor de aprovisionamiento se recupera de DNS y no se requiere la configuración de DHCP. Si se especifica el servidor de aprovisionamiento, el descubrimiento se omite, por lo que no se necesita ni DHCP ni DNS.

Puede activar la función de servidor de aprovisionamiento mediante la utilidad de configuración de iDRAC o Lifecycle Controller. Para obtener más información sobre cómo usar Lifecycle Controller, consulte *Lifecycle Controller User's Guide (Guía del usuario de Lifecycle Controller)*, disponible en **dell.com/idracmanuals**.

Si la función de servidor de aprovisionamiento no está activada en el sistema enviado de fábrica, la cuenta de administrador predeterminada (el nombre de usuario y la contraseña predeterminados para iDRAC se proporcionan en el distintivo del sistema) estará activada. Antes de

activar el servidor de aprovisionamiento, asegúrese de desactivar esta cuenta de administrador. Si la función de servidor de aprovisionamiento está activada en Lifecycle Controller, todas las cuentas de usuario de iDRAC quedarán desactivadas hasta que se *detecte* el servidor de aprovisionamiento.

Para activar el servidor de aprovisionamiento mediante la utilidad de configuración del iDRAC:

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

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

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

NOTA: IPv6 no es compatible para el descubrimiento automático.

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

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

Configuración de servidores y componentes del servidor mediante la configuración automática

La función de configuración automática configura y proporciona todos los componentes en un servidor en una sola operación. Estos componentes incluyen el BIOS, iDRAC y PERC. La configuración automática importará automáticamente un archivo JSON o XML de perfil de configuración del servidor (SCP) con todos los parámetros configurables. El servidor DHCP que asigna la dirección IP también proporciona los detalles para acceder al archivo de SCP.

Los archivos de SCP se crean mediante la configuración de un servidor de configuración Gold. Esta configuración luego se exporta a una ubicación de red NFS, CIFS, HTTP o HTTPS a la cual se puede acceder a través del servidor DHCP y la iDRAC del servidor que se está configurando. El nombre de archivo de SCP puede basarse en la etiqueta de servicio o el número de modelo del servidor de destino o puede ser un nombre genérico. El servidor DHCP usa una opción de servidor DHCP para especificar el nombre de archivo de SCP (opcionalmente), la ubicación del archivo de SCP y las credenciales de usuario para acceder a la ubicación del archivo.

Cuando iDRAC obtiene la dirección IP del servidor DHCP que se ha configurado para la configuración automática, iDRAC utiliza el SCP para configurar los dispositivos del servidor. La configuración automática se invocará solo después de que iDRAC haya obtenido la dirección IP del servidor DHCP. Si no obtiene una respuesta o una dirección IP del servidor DHCP, la configuración automática no se invoca.

Las opciones de uso compartido de archivos HTTP y HTTPS son compatibles con el firmware de iDRAC 3.00.00.00 o posterior. Debe proporcionarse los detalles de la dirección HTTP o HTTPS. En caso de que el proxy esté habilitado en el servidor, el usuario deberá proporcionar además la configuración de proxy para permitir que HTTP o HTTPS transfiera información. El distintivo de la opción `-s` se ha actualizado de la siguiente manera:

Tabla 8. Diferentes tipos de recursos compartidos y valores de paso

-s (ShareType)	pass in
NFS	`0` o `nfs`
CIFS	`2` o `cifs`

-s (ShareType)	pass in
HTTP	`5` o `http`
HTTPS	`6` o `https`

NOTA: Los certificados de HTTPS no son compatibles con la configuración automática. La configuración automática ignora advertencias de certificados.

A continuación, se muestra la lista de los parámetros obligatorios y opcionales para pasar por el valor de cadena:

`-f (Filename)`: nombre del archivo de perfil de configuración del servidor exportado. Es obligatorio para las versiones del firmware de iDRAC anteriores a 2.20.20.20.

`-n (Sharename)`: nombre de recurso compartido de red. Es obligatorio para NFS o CIFS.

`-s (ShareType)`: paso 0 para NFS, 2 para CIFS, 5 para HTTP y 6 para HTTPS. Es un campo obligatorio para las versiones del firmware de iDRAC 3.00.00.00.

`-i (IPAddress)`: la dirección IP del recurso compartido de red. Este es un campo obligatorio.

`-u (Username)`: nombre de usuario que tiene acceso al recurso compartido de red. Este es un campo obligatorio para CIFS.

`-p (Password)`: contraseña de usuario que tiene acceso al recurso compartido de red. Este es un campo obligatorio para CIFS.

`-d (ShutdownType)`: ya sea 0 para ordenado o 1 para forzado (el valor predeterminado es 0). Este campo es opcional.

`-t (Timetowait)`: el tiempo que se debe esperar para que se apague el host (el valor predeterminado es 300). Este campo es opcional.

`-e (EndHostPowerState)`: ya sea 0 para apagado o 1 para encendido (el valor predeterminado es 1). Este campo es opcional.

Los distintivos de opción adicionales son compatibles con el firmware de iDRAC 3.00.00.00 o posterior para activar la configuración de los parámetros proxy HTTP y establecer el tiempo de espera de reintento para acceder al archivo de perfil:

`—pd (ProxyDefault)`: utilice la configuración de proxy predeterminada. Este campo es opcional.

`—pt (ProxyType)`: el usuario puede pasar `http` o `socks` (la configuración predeterminada es http). Este campo es opcional.

`—ph (ProxyHost)`: dirección IP del host proxy. Este campo es opcional.

`—pu (ProxyUserName)`: nombre de usuario que tiene acceso al servidor proxy. Es obligatorio para compatibilidad con proxy.

`—pp (ProxyPassword)`: contraseña de usuario que tiene acceso al servidor proxy. Es obligatorio para compatibilidad con proxy.

`—po (ProxyPort)`: puerto del servidor proxy (el valor predeterminado es 80). Este campo es opcional.

`—to (Timeout)`: especifica el tiempo de espera de reintento en minutos para obtener el archivo de configuración (el valor predeterminado es 60 minutos).

Para el firmware de iDRAC 3.00.00.00 o posterior, se admiten los archivos de perfil con formato JSON. Los siguientes nombres de archivo se utilizarán en caso de que el parámetro Filename (Nombre de archivo) no esté presente:

- <etiqueta de servicio>-config.xml. Por ejemplo: CDVH7R1-config.xml
- <número de modelo>-config.xml. Por ejemplo: R640-config.xml
- config.xml
- <etiqueta de servicio>-config.json. Por ejemplo: CDVH7R1-config.json
- <número de modelo>-config.json. Por ejemplo: R630-config.json

- config.json

NOTA: Puede obtener más información sobre HTTP en las notas técnicas *14G Support for HTTP and HTTPS across IDRAC/LC Interface (Compatibilidad de 14 G con HTTP y HTTPS en la interfaz de iDRAC/LC)*, disponibles en delltechcenter.com.

NOTA:

- La configuración automática solo se puede activar cuando las opciones **DHCPv4** y **Enable IPV4 (Activar IPV4)** están activadas.
- Las funciones de configuración automática y detección automática son mutuamente excluyentes. Desactive la detección automática para que funcione la configuración automática.
- La configuración automática se desactivará después de que un servidor haya llevado a cabo una operación de configuración automática.

Si todos los servidores Dell PowerEdge de la agrupación de servidores DHCP son del mismo tipo y número de modelo, se necesitará un solo archivo de SCP (**config.xml**). El nombre del archivo **config.xml** se utiliza como el nombre de archivo de SCP predeterminado. Además del archivo **.xml**, los archivos **.json** también se puede utilizar con sistemas de 14 G. El archivo puede ser **config.json**.

El usuario puede configurar servidores individuales que requieran diferentes archivos de configuración asignados con los modelos de servidor o las etiquetas de servicio de los servidores individuales. En un entorno con diferentes servidores con requisitos específicos, se pueden usar nombres de archivo de SCP diferentes para distinguir cada servidor o tipo de servidor. Por ejemplo, si hay dos modelos de servidor que se deben configurar (PowerEdge R740 y PowerEdge R540), use dos archivos de SCP: **R740-config.xml** y **R540-config.xml**.

NOTA: El agente de configuración del servidor de iDRAC genera automáticamente el nombre de archivo de configuración con la etiqueta de servicio, el número de modelo o el nombre de archivo predeterminado (config.xml) del servidor.

NOTA: Si ninguno de estos archivos están en el recurso compartido de red, el trabajo de importación del perfil de configuración del servidor se marca como fallido para el archivo no encontrado.

Secuencia de configuración automática

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

Opciones de DHCP

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

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

```
option myname code 43 = text;
subnet 192.168.0.0 netmask 255.255.255.0 {
# default gateway
        option routers 192.168.0.1;
    option subnet-mask 255.255.255.0;
    option nis-domain  "domain.org";
    option domain-name "domain.org";
    option domain-name-servers 192.168.1.1;
```

```
    option time-offset -18000; #Eastern Standard Time
    option vendor-class-identifier "iDRAC";
    set vendor-string = option vendor-class-identifier;
    option myname "-f system_config.xml -i 192.168.0.130 -u user -p password -n cifs -s 2 -d 0 -
t 500";
```

donde, -i es la ubicación del recurso compartido de archivos remoto y -f es el nombre de archivo en la cadena junto con las credenciales para el recurso compartido de archivos remotos.

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

Configuración de la opción 43 en Windows

Para configurar la opción 43 en Windows:

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

Configuración de la opción 60 en Windows

Para configurar la opción 60 en Windows:

1 En el servidor DHCP, vaya a **Start (Inicio)** > **Administration Tools (Herramientas de administración)** > **DHCP** para abrir la herramienta de administración del servidor DHCP.
2 Encuentre el servidor y expanda los elementos que se ubican en él.
3 Haga clic con el botón derecho en **IPv4** y elija **Definir clases de proveedores**.
4 Haga clic en **Add** (Agregar).
Aparece un cuadro de diálogo con los siguientes campos:
- **Nombre de visualización:**
- **Descripción:**
- **Id.: binario: ASCII:**

5 En el campo **Nombre de visualización:**, escriba `iDRAC`.
6 En el campo **Descripción:**, escriba `Clase de proveedor`.
7 Haga clic en la sección **ASCII:** y escriba `iDRAC`.
8 Haga clic en **Aceptar** y luego en **Cerrar**.
9 En la ventana de DHCP, haga clic con el botón derecho del mouse en **IPv4** y seleccione **Establecer opciones predefinidas**.
10 Desde el menú desplegable **Clase de la opción** , seleccione **iDRAC** (creado en el paso 4) y haga clic en **Agregar**.
11 En el cuadro de diálogo **Tipo de opción**, introduzca la siguiente información:
- **Nombre**: `iDRAC`
- **Tipo de dato**: cadena
- **Código**: 60

- **Descripción**: identificador de clase de proveedor de Dell

12 Haga clic en **Aceptar** para volver a la ventana **DHCP** .

13 Expanda de todos los elementos en el nombre del servidor, haga clic con el botón derecho en **Opciones del ámbito** y seleccione **Configurar opciones**.

14 Haga clic en la pestaña **Opciones avanzadas**.

15 Desde el menú desplegable **Clase de proveedor**, seleccione **iDRAC**. Se muestra `060 iDRAC` en la columna **Available Options (Opciones disponibles)**.

16 Seleccione la opción **060 iDRAC**.

17 Introduzca el valor de cadena que se debe enviar al iDRAC (junto con una dirección IP estándar proporcionada por DHCP). El valor de cadena ayuda a importar el archivo de SCP correcto.

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

- `Filename (-f)`: indica el nombre del archivo XML del perfil de configuración del servidor exportado.
- `Sharename (-n)`: indica el nombre del recurso compartido de red.
- `ShareType (-s)`:

  Además de la compatibilidad con el uso compartido de archivos basado en NFS y CIFS, el firmware de iDRAC 3.00.00.00 o posterior también es compatible con el acceso a archivos de perfil mediante HTTP y HTTPS. El distintivo **opción -s** se actualiza de la siguiente forma:

  -s (ShareType): escriba nfs o 0 para NFS; cif o 2 para CIFS; http o 5 para HTTP; https o 6 para HTTPS (obligatorio).
- `IPAddress (-i)`: indica la dirección IP del recurso de archivos compartidos.

  NOTA: `Sharename (-n)`, `ShareType (-s)` y `IPAddress (-i)` son atributos obligatorios que se deben pasar. No se requiere -n para HTTP o HTTPS.
- `Username (-u)`: indica el nombre de usuario necesario para acceder al recurso compartido de red. Esta información es obligatoria solo para CIFS.
- `Password (-p)`: indica la contraseña necesaria para acceder al recurso compartido de red. Esta información es obligatoria solo para CIFS.
- `ShutdownType (-d)`: indica el modo de apagado. 0 indica un apagado ordenado y 1 indica un apagado forzado.

  NOTA: El valor predeterminado es 0.
- `Timetowait (-t)`: indica el tiempo que el sistema host espera antes del apagado. El valor predeterminado es 300.
- `EndHostPowerState (-e)`: indica el estado de alimentación del host. 0 indica apagado y 1 indica encendido. El valor predeterminado es 1.

  NOTA: `ShutdownType (-d)`, `Timetowait (-t)` y `EndHostPowerState (-e)` son atributos opcionales.

NFS: -f system_config.xml -i 192.168.1.101 -n /nfs_share -s 0 -d 1

CIFS: -f system_config.xml -i 192.168.1.101 -n cifs_share -s 2 -u <*USERNAME*> -p <*PASSWORD*> -d 1 -t 400

HTTP: -f system_config.json -i 192.168.1.101 -s 5

HTTP: -f http_share/system_config.xml -i 192.168.1.101 -s http

HTTP: -f system_config.xml -i 192.168.1.101 -s http -n http_share

HTTPS: -f system_config.json -i 192.168.1.101 -s https

Configuración de la opción 43 y la opción 60 en Linux

Actualice el archivo **/etc/dhcpd.conf**. Los pasos para configurar las opciones son similares a los pasos para Windows:

1 Deje un bloque o agrupación de direcciones que este servidor DHCP puede asignar.

2 Establezca la opción 43 y utilice el identificador de clase de nombre de proveedor para la opción 60.

```
option myname code 43 = text;
subnet 192.168.0.0 netmask 255.255.0.0  {
```

```
#default gateway
    option routers            192.168.0.1;
    option subnet-mask        255.255.255.0;
    option nis-domain        "domain.org";
    option domain-name        "domain.org";
    option domain-name-servers    192.168.1.1;
    option time-offset        -18000;    # Eastern Standard Time
    option vendor-class-identifier "iDRAC";
    set vendor-string = option vendor-class-identifier;
    option myname "-f system_config.xml -i 192.168.0.130 -u user -p password -n cifs -s 2 -d
0 -t 500";
    range dynamic-bootp 192.168.0.128 192.168.0.254;
    default-lease-time 21600;
    max-lease-time 43200;
        }
}
```

Los siguientes son los parámetros necesarios y opcionales que se deben pasar en la cadena del identificador de clase de proveedor:

- Filename (-f): indica el nombre del archivo XML del perfil de configuración del servidor exportado.

  NOTA: Para obtener más información sobre las reglas de asignación de nombres de archivo, consulte Configuración de servidores y componentes del servidor mediante la configuración automática.
- Sharename (-n): indica el nombre del recurso compartido de red.
- ShareType (-s): indica el tipo de recurso compartido. 0 indica NFS y 2 indica CIFS.
- IPAddress (-i): indica la dirección IP del recurso de archivos compartidos.

  NOTA: Sharename (-n), ShareType (-s) y IPAddress (-i) son atributos necesarios que se deben pasar. No se requiere -n para HTTP o HTTPS.
- Username (-u): indica el nombre de usuario necesario para acceder al recurso compartido de red. Esta información es obligatoria solo para CIFS.
- Password (-p): indica la contraseña necesaria para acceder al recurso compartido de red. Esta información es obligatoria solo para CIFS.

  NOTA: Ejemplo para recurso compartido NFS y CIFS de Linux:
  - **NFS:** -f system_config.xml -i 192.168.0.130 -n /nfs -s 0 -d 0 -t 500
  - **CIFS:** -f system_config.xml -i 192.168.0.130 -n sambashare/config_files -s 2 -u user -p password -d 1 -t 400

  Asegúrese de utilizar NFS2 o NFS3 para el recurso compartido de red NFS
- ShutdownType (-d): indica el modo de apagado. 0 indica un apagado ordenado y 1 indica un apagado forzado.

  NOTA: El valor predeterminado es 0.
- Timetowait (-t): indica el tiempo que espera el sistema host antes de apagarse. El valor predeterminado es 300.
- EndHostPowerState (-e): indica el estado de la alimentación del host. 0 indica apagado y 1 indica encendido. El valor predeterminado es 1.

  NOTA: ShutdownType (-d), Timetowait (-t) y EndHostPowerState (-e) son atributos opcionales.

El siguiente es un ejemplo de una reserva de DHCP estática desde un archivo dhcpd.conf:

```
host my_host {

hardware ethernet 8:2 a:72:fb:6:56;

  fixed-address 192.168.0.211;

option host-name "my_host";

option myname " -f r630_raid.xml -i 192.168.0.1 -n /nfs -s 0 -d 0 -t 300 ";

}
```

NOTA: Después de editar el archivo dhcpd.conf , asegúrese de reiniciar el servicio dhcpd para aplicar los cambios.

Prerrequisitos antes de activar Configuración automática

Antes de activar la función Configuración automática, asegúrese de que los siguientes elementos ya estén configurados:

- El recurso compartido de red admitido (NFS, CIFS, HTTP y HTTPS) está disponible en la misma subred que iDRAC y el servidor DHCP. Pruebe el recurso compartido de red para asegurarse de que se pueda acceder a este y que el servidor de seguridad y los permisos del usuario están establecidos correctamente.
- El perfil de configuración del servidor se exporta al recurso compartido de red Además, asegúrese de que se hayan realizado los cambios necesarios en el archivo XML de manera que se puede aplicar la configuración adecuada cuando se inicie el proceso de configuración automática.
- El servidor DHCP está configurado y la configuración de DHCP se ha actualizado según el iDRAC para llamar al servidor e iniciar la función de configuración automática.

Activación de la configuración automática mediante la interfaz web de iDRAC

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

Para activar la configuración automática:

1 En la interfaz web de iDRAC, vaya a **iDRAC Settings (Configuración de iDRAC)** > **Connectivity (Conectividad)** > **Network (Red)** > **Auto Config (Configuración automática)**.

Aparecerá la página **Red**.

2 En la sección **Configuración automática**, seleccione una de las opciones siguientes en el menú desplegable **Activar aprovisionamiento de DHCP**:

- **Activar una vez**: configura el componente solo una vez mediante el archivo XML sugerido por el servidor DHCP. Después de esto, se desactiva la configuración automática.
- **Enable once after reset (Activar una vez después de restablecer)**: después de restablecer iDRAC, se configuran los componentes solo una vez mediante el archivo XML sugerido por el servidor DHCP. Después de esto, se desactiva la configuración automática.
- **Desactivar**: desactiva la función Configuración automática.

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

La página de la red se actualiza automáticamente.

Activar configuración automática mediante RACADM

Para activar la función de configuración automática mediante RACADM, utilice el objeto `iDRAC.NIC.AutoConfig`.

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

Para obtener más información sobre la función de configuración automática, consulte el documento técnico *Zero-Touch Bare Metal Server Provisioning using Dell iDRAC con Lifecycle Controller Auto Config* (Aprovisionamiento de servidores físicos (bare-metal) sin intervención mediante la configuración automática de Lifecycle Controller) disponible en **delltechcenter.com/idrac**.

Cómo usar contraseñas de algoritmos hash para obtener una mayor seguridad

En los servidores PowerEdge con iDRAC, versión 3.00.00.00, puede establecer las contraseñas de usuario y las contraseñas del BIOS utilizando un formato de hash unidireccional. El mecanismo de autentificación de usuarios no se verá afectado (excepto para SNMPv3 e IPMI) y puede proporcionar la contraseña en texto sin formato.

Con la nueva función de contraseña de algoritmos hash:

- Puede generar sus propios algoritmos hash SHA256 para configurar contraseñas de usuario de iDRAC y contraseñas del BIOS. Esto permite tener los valores de SHA256 en el perfil de configuración del servidor, RACADM y WSMan. Si ingresa los valores de contraseña de SHA256, no puede autentificar a través de SNMPv3 e IPMI.

  NOTA: No se puede usar la RACADM remota, WSMan ni Redfish para la configuración/sustitución de contraseñas de algoritmos hash para iDRAC. Puede utilizar SCP para la configuración/sustitución de contraseñas de algoritmos hash en la RACADM remota, WSMan o Redfish.
- Puede configurar un servidor de plantillas que incluya todas las cuentas de usuario de iDRAC y las contraseñas del BIOS mediante el mecanismo actual de texto sin formato. Después de configurar el servidor, puede exportar el perfil de configuración del servidor con los valores de contraseña de algoritmos hash. La exportación incluirá los valores de algoritmos hash requeridos para la autentificación de SNMPv3. La importación de este perfil generará la pérdida de la autenticación de IPMI para usuarios que tengan los valores de contraseña de algoritmos hash establecidos y la interfaz de iDRAC F2 mostrará que la cuenta de usuario está desactivada.
- Las otras interfaces, como la interfaz gráfica de usuario de IDRAC, mostrarán las cuentas de usuario activadas.

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

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

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

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

Contraseña de algoritmos hash mediante RACADM

Para configurar contraseñas de algoritmos hash, utilice los siguientes objetos con el comando **set**:

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

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

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

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

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

Contraseña de algoritmos hash en el perfil de configuración del servidor

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

Al importar el perfil de configuración del servidor, puede quitar el comentario del atributo de contraseña existente o de los nuevos atributos de contraseña de algoritmos hash. Si se quita el comentario de ambos atributos, se genera un error y no se establece la contraseña. Un atributo comentado no se aplica durante una importación.

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

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

1 Para cuentas de usuario de iDRAC, debe configurar el atributo Salt de la contraseña con SHA256.

Al configurar el atributo Salt de la contraseña, se agregará una cadena de binarios de 16 bytes. El atributo Salt debe tener 16 bytes, si se proporciona.

2 Proporcione el valor del algoritmo hash y del atributo Salt en el perfil de configuración del servidor importado, los comandos de RACADM, Redfish o WSMan.

3 Después de configurar la contraseña, la autentificación de contraseña de texto sin formato normal funcionará, excepto que falle la autentificación de SNMP v3 e IPMI para cuentas de usuario de iDRAC que poseen contraseñas actualizadas con algoritmos hash.

Modificación de la configuración de la cuenta de administrador local

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

1 En la utilidad de configuración de iDRAC, vaya a **Configuración de usuario**.

Se muestra la página **Configuración de usuario de la configuración de iDRAC**.

2 Especifique los detalles de **Nombre de usuario**, **Privilegio de usuario en la LAN**, **Privilegio de usuario de puerto serie** y **Contraseña**.

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

3 Haga clic en **Atrás**, en **Terminar** y, a continuación, en **Sí**.

Se habrán configurado los valores de la cuenta de administrador local.

Configuración de la ubicación de Managed System

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

Configuración de la ubicación de Managed System mediante la interfaz web

Para especificar los detalles de ubicación del sistema:

1 En la interfaz web de iDRAC, vaya a **System (Sistema)** > **Details (Detalles)** > **System Details (Detalles del sistema)**.

Aparecerá la página **Detalles del sistema**.

2 En **Ubicación del sistema**, introduzca los detalles de la ubicación del sistema administrado en el centro de datos.

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

3 Haga clic en **Aplicar**. Los detalles de la ubicación del sistema se guardan en iDRAC.

Configuración de la ubicación de Managed System mediante RACADM

Para especificar los detalles de ubicación del sistema, utilice los objetos de grupo `System.Location`.

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

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 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.

Optimización del rendimiento y el consumo de alimentación del sistema

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

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

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

Modificación de la configuración térmica mediante la interfaz web de iDRAC

Para modificar la configuración térmica:

1 En la interfaz web de iDRAC, vaya a **Configurations (Configuraciones)** > **System Settings (Configuración del sistema)** > **Hardware Settings (Configuración de hardware)** > **Fans configuration (Configuración de ventiladores)**.

Aparece la página **Configuración del ventilador**.

2 Especifique lo siguiente:

- **Perfil térmico**: seleccione el perfil térmico:

- **Default Thermal Profile Settings (Configuración del perfil térmico predeterminado)**: implica que al algoritmo térmico utiliza la misma configuración de perfil del sistema que se ha definido en **System BIOS (BIOS del sistema)** > **System BIOS Settings (Configuración del BIOS del sistema) System Profile Settings (Configuración del perfil del sistema)**.

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

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

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

- **Maximum Exhaust Temperature Limit (Límite de temperatura de salida máximo)**: en el menú desplegable, seleccione la temperatura de aire de salida máxima. Los valores se muestran según el sistema.

  El valor predeterminado es **Valor predeterminado, 70 ºC (158 ºF)**.

  Esta opción permite cambiar las velocidades de los ventiladores del sistema para que la temperatura de salida no supere el límite de temperatura de salida seleccionado. Esto no se puede garantizar siempre bajo todas las condiciones de funcionamiento del sistema debido a la dependencia en la carga del sistema y la capacidad de enfriamiento del sistema.
- **Fan Speed Offset (Desplazamiento de la velocidad del ventilador)**: la selección de esta opción permite enfriamiento adicional para el servidor. En caso de que se agregue hardware (por ejemplo, tarjetas de PCIe nuevas), es posible que requiera enfriamiento adicional. Un desplazamiento en la velocidad del ventilador causa el aumento de las velocidades del ventilador (por el valor % de desplazamiento) por encima de la línea base de las velocidades del ventilador calculadas mediante el algoritmo de control térmico. Los posibles valores son:
  - **Velocidad baja del ventilador**: lleva la velocidad del ventilador a una velocidad moderada.
  - **Velocidad media del ventilador**: lleva la velocidad del ventilador a un valor cercano al valor medio.
  - **Velocidad alta del ventilador**: lleva la velocidad del ventilador a un valor cercano a la velocidad máxima.
  - **Velocidad máxima del ventilador**: lleva la velocidad del ventilador a la velocidad máxima.
  - **Off (Desactivado)**: el desplazamiento de la velocidad del ventilador se configura en desactivado. Este es el valor predeterminado. Cuando se establece en apagado, el porcentaje no se mostrará. La velocidad predeterminada los ventiladores se aplica sin desplazamiento. Por el contrario, la configuración máxima hará funcionar a todos los ventiladores a su velocidad máxima.

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

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

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

  El escenario de uso más común es el enfriamiento del adaptador PCIe no estándar. Sin embargo, la función se puede utilizar para aumentar el enfriamiento del sistema para otros fines.
- **Minimum Fan Speed in PWM (% of Max) (Velocidad mínima del ventilador en PWM [% del máximo])** : seleccione esta opción para ajustar la velocidad del ventilador. Al usar esta opción, puede configurar una velocidad más alta del ventilador en el sistema de referencia o aumentar la velocidad del ventilador del sistema si otras opciones personalizadas de velocidad del ventilador no producen las velocidades más altas del ventilador requeridas.

- **Predeterminado**: configura la velocidad mínima del ventilador con el valor predeterminado según lo establecido por el algoritmo de refrigeración del sistema.
- **Personalizado**: introduzca el valor de porcentaje.

El rango permitido para la velocidad mínima del ventilador PWM es dinámico y se basa en la configuración del sistema. El primer valor es la velocidad de inactividad y el segundo valor es el máximo de la configuración (que pueden o no ser el 100 % en función de la configuración del sistema).

Los ventiladores del sistema pueden funcionar a velocidades más altas que esta según los requisitos térmicos del sistema, pero no a menor velocidad que la velocidad mínima definida. Por ejemplo, la configuración de la velocidad mínima del ventilador en 35 % limita la velocidad del ventilador para que nunca sea inferior al 35 % en PWM.

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

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

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

Aparece el siguiente mensaje:

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

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

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

Modificación de la configuración térmica mediante RACADM

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

Tabla 9. Configuración térmica

Objeto	Descripción	Uso	Ejemplo

`AirExhaustTemp`	Permite configurar el límite de temperatura máxima de la salida de aire.	Configure esta opción con alguno de los siguientes valores (según el sistema):
		• 0: indica 40 °C
		• 1: indica 45 °C
		• 2: indica 50 °C
		• 3: indica 55 °C
		• 4: indica 60 °C
		• 255: indica 70 °C (predeterminado)
			Para comprobar la configuración existente en el sistema:
			`racadm get system.thermalsettings.AirExhaustTemp`
			El resultado es:
			`AirExhaustTemp=70`
			Este resultado significa que el sistema está configurado para limitar la temperatura de salida de aire a 70 °C.
			Para establecer el límite de temperatura de salida en 60 °C:
			`racadm set system.thermalsettings.AirExhaustTemp 4`

Objeto	Descripción	Uso	Ejemplo

			El resultado es:
			`Object value modified successfully.`
			
			Si un sistema no admite un determinado límite de temperatura de salida de aire, cuando ejecute el comando
			
			`racadm set system.thermalsettings.AirExhaustTemp 0`
			
			Se muestra el siguiente mensaje de error:
			
			`ERROR: RAC947: Invalid object value specified.`
			
			Asegúrese de especificar el valor según el tipo de objeto.
			
			Para obtener más información, consulte la ayuda de RACADM.
			
			Para establecer el límite del valor predeterminado:
			
			`racadm set system.thermalsettings.AirExhaustTemp 255`

`FanSpeedHighOffsetVal`	• Al obtener esta variable, se lee el valor de desplazamiento de velocidad del ventilador en % de PWM en la opción Desplazamiento de velocidad alta del ventilador.
	• Este valor depende del sistema.
	• Utilice el objeto `FanSpeedOffset` para configurar este valor con el valor de índice 1.
		Valores de 0 a 100	`racadm get system.thermalsettings FanSpeedHighOffsetVal`
			
			Se genera un valor numérico; por ejemplo, 66. Este valor indica que al utilizar el siguiente comando, se aplica una compensación de velocidad alta del ventilador (66 % de PWM) sobre la línea de base de la velocidad del ventilador.
			`racadm set system.thermalsettings FanSpeedOffset 1`

`FanSpeedLowOffsetVal`	• Al obtener esta variable, se lee el valor de desplazamiento de velocidad del ventilador en % de PWM en la opción Desplazamiento de velocidad baja del ventilador.
	• Este valor depende del sistema.
	• Utilice el objeto `FanSpeedOffset` para configurar este valor con el valor de índice 0.
		Valores de 0 a 100	`racadm get system.thermalsettings FanSpeedLowOffsetVal`
			
			Esta acción devuelve un valor como "23". Esto significa que al utilizar el siguiente comando, se aplica una compensación de velocidad baja del ventilador (23 % de PWM) sobre la línea de base de la velocidad del ventilador.
			`racadm set system.thermalsettings FanSpeedOffset 0`

Objeto	Descripción	Uso	Ejemplo
FanSpeedMaxOffsetVal	• Al obtener esta variable, se lee el valor de desplazamiento de velocidad del ventilador en % de PWM en la opción Desplazamiento de velocidad máxima del ventilador. • Este valor depende del sistema. • Utilice FanSpeedOffset para configurar este valor con el valor de índice 3.	Valores de 0 a 100	racadm get system.thermalsettings FanSpeedMaxOffsetVal Esta acción devuelve un valor como "100". Esto significa que al utilizar el siguiente comando, se aplica una compensación de velocidad máxima del ventilador (es decir la velocidad máxima, 100 % de PWM). Usualmente, este desplazamiento produce velocidades de ventilador en aumento hasta llegar a la velocidad máxima. racadm set system.thermalsettings FanSpeedOffset 3
FanSpeedMediumOffsetVal	• Al obtener esta variable, se lee el valor de desplazamiento de velocidad del ventilador en % de PWM en la opción Desplazamiento de velocidad media del ventilador. • Este valor depende del sistema. • Utilice el objeto FanSpeedOffset para configurar este valor con el valor de índice 2.	Valores de 0 a 100	racadm get system.thermalsettings FanSpeedMediumOffsetVal Esta acción devuelve un valor como "47". Esto significa que cuando al utilizar el siguiente comando, se aplica un desplazamiento de velocidad media del ventilador (47 % de PWM) sobre la línea de base de la velocidad del ventilador. racadm set system.thermalsettings FanSpeedOffset 2
FanSpeedOffset	• Si se usa este objeto con el comando get, se muestra el valor de desplazamiento de velocidad del ventilador existente. • Si se usa este objeto con el comando set, se puede establecer el valor de desplazamiento de velocidad del ventilador requerido. • El valor de índice decide qué desplazamiento se aplica y los objetos FanSpeedLowOffsetVal, FanSpeedMaxOffsetVal, FanSpeedHighOffsetVal y FanSpeedMediumOffsetVal (definidos anteriormente) son los valores en los cuales se aplica el desplazamiento.	Los valores son: • 0: velocidad baja del ventilador • 1: velocidad alta del ventilador • 2: velocidad media del ventilador • 3: velocidad máx. del ventilador • 255: ninguno	Para ver la configuración existente: racadm get system.thermalsettings.FanSpeedOffset Para establecer el valor de desplazamiento de velocidad alta del ventilador (como se define en FanSpeedHighOffsetVal): racadm set system.thermalsettings.FanSpeedOffset 1

Objeto	Descripción	Uso	Ejemplo
`MFSMaximumLimit`	Límite de lectura máximo para MFS	Valores de 1 a 100	Para mostrar el valor más alto que se puede configurar con la opción `MinimumFanSpeed`: `racadm get system.thermalsettings.MFSMaximumLimit`
`MFSMinimumLimit`	Límite de lectura mínimo para MFS	Valores de 0 a `MFSMaximumLimit` El valor predeterminado es 255 (significa None [Ninguno])	Para mostrar el valor más bajo que se puede configurar con la opción `MinimumFanSpeed`: `racadm get system.thermalsettings.MFSMinimumLimit`
`MinimumFanSpeed`	• Permite configurar la velocidad mínima del ventilador que se requiere para que el sistema funcione. • Define el valor de la línea de base (piso) de velocidad del ventilador. El sistema permitirá que los ventiladores perforen este valor de velocidad del ventilador definido. • Este es el valor de % de PWM para la velocidad del ventilador.	Valores de `MFSMinimumLimit` a `MFSMaximumLimit` Cuando el comando get devuelve el valor 255, significa que no se aplica el desplazamiento configurado por el usuario.	Para asegurarse de que la velocidad mínima del sistema no caiga por debajo del 45 % de PWM (45 debe ser un valor entre `MFSMinimumLimit` y `MFSMaximumLimit`): `racadm set system.thermalsettings.MinimumFanSpeed 45`

`ThermalProfile`	• Permite especificar el algoritmo térmico de base.
	• Permite configurar el perfil del sistema según sea necesario para el comportamiento térmico asociado con el perfil.
		Valores:
		• 0 — Automático
		• 1 — Máximo rendimiento
		• 2 — Alimentación mínima
			Para ver la configuración del perfil térmico existente:
			`racadm get system.thermalsettings.ThermalProfile`
			Para establecer el perfil térmico como rendimiento máximo:
			`racadm set system.thermalsettings.ThermalProfile 1`

`ThirdPartyPCIFanResponse`	• Supresiones térmicas para tarjetas PCI de terceros. • Permite desactivar o activar la respuesta predeterminada del ventilador del sistema para las tarjetas PCI de terceros detectadas. • Para confirmar la presencia de una tarjeta PCI de terceros, visualice la Id. de mensaje PCI3018 en el registro de Lifecycle Controller.	Valores: • 1: Activado • 0: Desactivado **NOTA: El valor predeterminado es 1.**	Para desactivar cualquier conjunto de respuestas de velocidad del ventilador predeterminado para una tarjeta de PCI detectada de terceros: `racadm set system.thermalsettings.ThirdPartyPCIFanResponse 0`

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

Para modificar la configuración térmica:

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

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

Configuración de la estación de administración

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

Para configurar la estación de administración.

1 Instale un sistema operativo compatible. Para obtener más información, consulte las notas de la versión.
2 Instale y configure un navegador web compatible. Para obtener más información, consulte las notas de la versión.
3 Instale el Java Runtime Environment (JRE) más reciente (obligatorio si el tipo de complemento Java se utiliza para acceder a iDRAC mediante un explorador web).

NOTA: Necesita Java 8 o posterior para poder usar esta función y para iniciar la consola virtual de iDRAC a través de la red IPv6.

4 Desde el DVD *Dell Systems Management Tools and Documentation* (DVD de herramientas y documentación de Dell Systems Management), instale VMCLI y RACADM remoto desde la carpeta SYSMGMT. O bien, ejecute el archivo **Setup** en el DVD para instalar RACADM remoto de manera predeterminada y otro software OpenManage. Para obtener más información sobre RACADM, consulte *iDRAC RACADM Command Line Interface Reference Guide (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC)* disponible en **dell.com/idracmanuals**.
5 Instale los elementos siguientes según los requisitos:
- Telnet
- Cliente SSH
- TFTP
- Dell OpenManage Essentials

Acceso a iDRAC de manera remota

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

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

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

Configuración de exploradores web compatibles

NOTA: Para obtener información sobre las versiones de exploradores compatibles, consulte las *Notas de la versión* disponibles en dell.com/idracmanuals.

La mayoría de las funciones de la interfaz web de iDRAC se pueden acceder mediante el uso de estos navegadores con valores predeterminados. Para que trabajen ciertas funciones, debe cambiar algunos valores de configuración. Estos valores incluyen la desactivación de bloqueadores de elementos emergentes, la activación de la compatibilidad con complementos de Java, ActiveX o HTML5, etc.

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

NOTA: Si usa Internet Explorer o Firefox para acceder a la interfaz web de iDRAC, es posible que deba configurar ciertas opciones tal y como se describe en esta sección. Puede utilizar otros navegadores compatibles con su configuración predeterminada.

NOTA: Las configuraciones de proxy en blanco se tratan como no proxy.

Configuración de Internet Explorer

En esta sección, se proporcionan detalles sobre la configuración de Internet Explorer (IE) para garantizar que usted pueda acceder a todas las funciones de la interfaz web de iDRAC y pueda usarlas. Estos valores incluyen:

- Restablecer la configuración de seguridad
- Agregar el IP de iDRAC a los sitios de confianza
- Configurar IE para activar el inicio de sesión único (SSO) de Active Directory
- Desactivación de la configuración de seguridad mejorada de IE

Cómo restablecer la configuración de seguridad de Internet Explorer

Asegúrese de que la configuración de Internet Explorer (IE) tenga los valores predeterminados recomendados por Microsoft y personalice la configuración tal y como se describe en esta sección.

1 Abra IE como administrador o mediante una cuenta de administrador.
2 Haga clic en **Herramientas Opciones de Internet Seguridad Red local** o **Intranet local**.
3 Haga clic en **Nivel personalizado** , seleccione la opción **Medio-bajo** y haga clic en **Restablecer**. Haga clic en **OK** (Aceptar) para confirmar.

Cómo agregar el IP de iDRAC a la lista de sitios de confianza

Cuando accede a la interfaz web de iDRAC, se le solicitará que agregue la dirección IP de iDRAC a la lista de los dominios de confianza si la dirección no está incluida en la lista. Cuando termine, haga clic en **Refresh (Actualizar)** o vuelva a iniciar el navegador web para establecer una conexión con la interfaz web de iDRAC. Si no se le solicita que agregue la dirección IP, se recomienda agregarla manualmente a la lista de sitios de confianza.

NOTA: Al conectar a la interfaz web de iDRAC con un certificado que no es de confianza para el explorador, aparece por segunda vez la advertencia de error de certificado del explorador después de confirmar la primera advertencia.

Para agregar la dirección IP de iDRAC a la lista de sitios de confianza:

1 Haga clic en **Herramientas** > **Opciones de Internet** > **Seguridad** > **Sitios de confianza** > **Sitios**.
2 Ingrese la dirección IP de iDRAC en **Agregar este sitio web a la zona**.
3 Haga clic en **Agregar**, en **Aceptar** y, a continuación, en **Cerrar**.
4 Haga clic en **Aceptar** y actualice el explorador.

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 **Advanced (Opciones avanzadas)**.
4 Agregue todos los nombres de dominio relativos que se usarán en instancias de iDRAC y que forman parte de la configuración del SSO (por ejemplo: **myhost.example.com**).
5 Haga clic en **Cerrar** y luego en **Aceptar** dos veces.

Desactivación de la configuración de seguridad mejorada de Internet Explorer

Para asegurarse de que puede descargar archivos de registro y otros elementos locales por medio de la interfaz web, se recomienda desactivar la configuración de seguridad mejorada de Internet Explorer desde las funciones de Windows. Para obtener información sobre cómo desactivar esta función en su versión de Windows, consulte la documentación de Microsoft.

Configuración de Mozilla Firefox

En esta sección, se proporcionan detalles sobre la configuración de Firefox para garantizar que usted pueda acceder a todas las funciones de la interfaz web de iDRAC y pueda usarlas. Estos valores incluyen:

- Desactivación de la función de lista blanca
- Configuración de Firefox para activar el inicio de sesión único de Active Directory

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 está activada, la función de lista blanca requiere que se instale un visor de consola virtual para cada iDRAC que usted visita, aunque las versiones del visor sean 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 **Preference Name (Nombre de preferencia)**, **Status (Estado)**, **Type (Tipo)** y **Value (Valor)** cambian a texto en negrita. El valor de **Status (Estado)** cambia al valor establecido por el usuario y el de **Value (Valor)** cambia a false (falso).

4 En la columna **Nombre de la preferencia**, busque **xpinstall.enabled**.

Asegúrese de que en **Value (Valor)** esté **true (verdadero)**. De no ser así, haga doble clic en **xpinstall.enabled** para establecer **Value (Valor)** en **true (verdadero)**.

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 **Filter (Filtro)**, introduzca `network.negotiate`.

3 Agregue el nombre de dominio a network.negotiate-auth.trusted-uris (usando lista de valores separados por coma).

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

Configuración de exploradores web para usar la consola virtual

Para utilizar la consola virtual en la estación de administración:

1 Asegúrese de tener instalada una versión de explorador compatible [Internet Explorer (Windows) o Mozilla Firefox (Windows o Linux), Google Chrome, Safari].

Para obtener más información sobre las versiones de exploradores compatibles, consulte las *Notas de la versión* disponibles en **dell.com/idracmanuals**.

2 Para utilizar Internet Explorer, establezca IE en **Ejecutar como administrador**.

3 Configure el explorador web para utilizar el complemento ActiveX, Java o HTML5.

El visor de ActiveX se admite solo con Internet Explorer. Un visor de HTML5 o Java se admite en cualquier navegador.

> **NOTA: Necesita Java 8 o posterior para poder usar esta función y para iniciar la consola virtual de iDRAC a través de la red IPv6.**

4 Importe los certificados raíz en el sistema administrado para evitar las ventanas emergentes que solicita la verificación de los certificados.

5 Instale el paquete **compat-libstdc++-33-3.2.3-61**.

> **NOTA: En Windows, el paquete relacionado compat-libstdc++-33-3.2.3-61 puede incluirse en el paquete de .NET Framework o el paquete de sistema operativo.**

6 Si utiliza un sistema operativo MAC, seleccione la opción **Activar acceso para dispositivos de asistencia** en la ventana **Acceso universal**.

Para obtener más información, consulte la documentación del sistema operativo MAC.

Configuración de Internet Explorer para el complemento basado en HTML5

Las API de consola virtual y medios virtuales HTML5 se crean con la tecnología HTML5. A continuación, se enumeran las ventajas de la tecnología HTML5:

- No es necesaria la instalación en la estación de trabajo cliente.
- La compatibilidad se basa en explorador y no en el sistema operativo o en los componentes instalados.
- Es compatible con la mayoría de los equipos de escritorio y las plataformas móviles.
- Implementación rápida y el cliente se descarga como parte de una página web.

Debe configurar Internet Explorer (IE) antes de iniciar y ejecutar las aplicaciones de consola virtual y medios virtuales basadas en HTML5. Para configurar los valores del explorador:

1 Desactive el bloqueador de elementos emergentes. Para ello, haga clic en **Herramientas** > **Opciones de Internet** > **Privacidad** y desmarque la casilla de verificación **Activar el bloqueador de elementos emergentes**.

2 Inicie la consola virtual de HTML5 mediante cualquiera de los métodos siguientes:
   - En IE, haga clic en **Herramientas** > **Configuración de vista de compatibilidad** y desmarque la casilla de verificación **Mostrar sitios de intranet en la Vista de compatibilidad**.
   - En IE mediante una dirección IPv6, modifique la dirección IPv6 como se indica a continuación:
     ```
     https://[fe80::d267:e5ff:fef4:2fe9]/ to https://fe80--d267-e5ff-fef4-2fe9.ipv6-literal.net/
     ```
   - Dirija la consola virtual de HTML5 en IE mediante una dirección IPv6, modifique la dirección IPv6 como se indica a continuación:
     ```
     https://[fe80::d267:e5ff:fef4:2fe9]/console to https://fe80--d267-e5ff-fef4-2fe9.ipv6-literal.net/console
     ```

3 Para mostrar la información de la barra de título en IE, vaya a **Panel de control** > **Apariencia y personalización** > **Personalización** > **Windows Classic**.

Configuración de exploradores web para usar el complemento Java

Instale Java Runtime Environment (JRE) si utiliza Firefox o IE y desea utilizar el visor de Java.

NOTA: Instale una versión de 32 bits o de 64 bits de JRE en un sistema operativo de 64 bits o una versión de 32 bits de JRE en un sistema operativo de 32 bits.

Para configurar IE para utilizar el complemento Java:

- Desactive la solicitud automática de descargas de archivo en Internet Explorer.
- Desactive la opción *Modo de seguridad mejorado* en Internet Explorer.

Configuración de IE para usar el complemento ActiveX

Debe configurar los valores del navegador IE antes de iniciar y ejecutar la consola virtual basada en ActiveX y las aplicaciones de medios virtuales. Las aplicaciones de ActiveX se proporcionan como archivos CAB firmados desde el servidor de iDRAC. Si el tipo de complemento se establece en ActiveX nativo en la consola virtual, cuando se intente iniciar la consola virtual, se descargará el archivo CAB en el sistema cliente y se iniciará la consola virtual basada en ActiveX. Internet Explorer requiere algunas configuraciones para descargar, instalar y ejecutar estas aplicaciones basadas en ActiveX.

Internet Explorer se encuentra disponible en exploradores con versiones de 32 bits y de 64 bits. Se puede utilizar cualquier versión, pero si se instala el complemento en el explorador web de 64 bits y, a continuación, se intenta ejecutar el visor en un explorador de 32 bits, será necesario volver a instalar el complemento.

NOTA: El complemento ActiveX solo se puede utilizar con Internet Explorer.

NOTA: Para utilizar el complemento ActiveX en los sistemas con Internet Explorer 9, antes de configurar Internet Explorer, asegúrese de desactivar el Modo de seguridad mejorada en Internet Explorer o en el administrador de servidores en los sistemas operativos Windows Server.

Para aplicaciones de ActiveX en Windows 7, Windows 2008 y Windows 10, configure los siguientes valores de Internet Explorer para utilizar el complemento ActiveX:

1 Borre la memoria caché del explorador.

2 Agregue la dirección IP de iDRAC o el nombre de host a la lista **Sitio de Internet local**.

3 Restablezca la configuración personaliza en **Medio-bajo** o cambie los valores para permitir la instalación de complementos ActiveX firmados.

4 Active el explorador para descargar contenido cifrado y activar las extensiones de explorador de terceros. Para ello, vaya a **Herramientas** > **Opciones de Internet** > **Opciones avanzadas**, desactive la opción **No guardar las páginas cifradas en el disco** y active la opción **Habilitar extensiones de explorador de terceros**.

NOTA: Reinicie Internet Explorer para que la opción Habilitar las extensiones de explorador de terceros surta efecto.

5 Vaya a **Herramientas** > **Opciones de Internet** > **Seguridad** y seleccione la zona en la que desee ejecutar la aplicación.

6 Haga clic en **Nivel personalizado**. En la ventana **Configuración de seguridad**, realice lo siguiente:

- Seleccione **Activar** para **Preguntar automáticamente si se debe usar un control ActiveX**.
- Seleccione **Preguntar** para **Descargar los controles ActiveX firmados**.
- Seleccione **Habilitar** o **Preguntar** para **Ejecutar controles y complementos de ActiveX**.
- Seleccione **Habilitar** o **Preguntar** para **Generar scripts de los controles ActiveX marcados como seguros para scripts**.

7 Haga clic en **Aceptar** para cerrar la ventana **Configuración de seguridad**.

8 Haga clic en **Aceptar** para cerrar la ventana **Opciones de Internet**.

NOTA: En los sistemas con Internet Explorer 11, asegúrese de agregar la dirección IP de iDRAC. Para ello, haga clic en Herramientas > Configuración de vista de compatibilidad.

NOTA:

- Las diferentes versiones de Internet Explorer comparten el mismo valor de **Opciones de Internet**. Por lo tanto, después de agregar el servidor a la lista de *sitios de confianza* para un explorador, el otro explorador utilizará la misma configuración.
- Antes de instalar el control de ActiveX, Internet Explorer puede mostrar una advertencia de seguridad. Para completar el procedimiento de instalación del control de ActiveX, acepte este control cuando Internet Explorer muestre una advertencia de seguridad.
- Si aparece el error **Unknown Publisher (Editor desconocido)** mientras se inicia la consola virtual, es posible que se deba al cambio de la ruta del certificado de firma de código. Para solucionar este error, debe descargar una clave adicional. Use un motor de búsqueda para buscar **Symantec SO16958** y, en los resultados de la búsqueda, siga las instrucciones que aparecen en el sitio web de Symantec.

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 **Enable Protected Mode (Habilitar modo protegido)** no esté seleccionada para la zona de sitios de confianza. También puede agregar la dirección de iDRAC a los sitios de la zona de Intranet. De manera predeterminada, el modo protegido está desactivado para los sitios de la zona de Intranet y la zona de sitios de confianza.

4 Haga clic en **Sitios**.

5 En el campo **Agregar este sitio web a la zona**, agregue la dirección de iDRAC y haga clic en **Agregar**.

6 Haga clic en **Cerrar** y, a continuación, en **Aceptar**.

7 Cierre y reinicie el explorador para que la configuración tenga efecto.

Borrado de la caché del explorador

Si tiene problemas para usar la consola virtual (errores de fuera de rango, problemas de sincronización, etc.) borre la caché del explorador para quitar o eliminar las versiones anteriores del visor que pudieran estar almacenadas en el sistema e inténtelo nuevamente.

NOTA: Debe tener privilegios de administrador para borrar la caché del explorador.

Borrado de versiones anteriores de Java

Para borrar las versiones anteriores del visor de Java en Windows o Linux, haga lo siguiente:

1 En el símbolo del sistema, ejecute `javaws-viewer` o `javaws-uninstall`.

Aparece el **Visor de la caché de Java**.

2 Elimine los elementos con el título *Cliente de consola virtual de iDRAC*.

Importación de certificados de CA a la estación de administración

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 en el almacén de certificados de confianza de Java o 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**. La ventana **Java Control Panel (Panel de control de Java)** se cierra.

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 algoritmo hash del certificado mediante el algoritmo hash seguro (SHA). Se recomienda usar la herramienta OpenSSL 1.0.x o una versión posterior, ya que esta utiliza SHA de manera predeterminada. El certificado de CA debe tener el formato PEM codificado en Base64. Este es un proceso único que se debe realizar para importar cada certificado de 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 algoritmo hash de 8 bytes en el certificado de CA que se esté utilizando actualmente en la estación de administración mediante el comando: `openssl x509 -in (name of CA cert) -noout -hash`.

Se genera un archivo de salida. Por ejemplo, si el nombre de archivo del certificado de CA es **cacert.pem**, el 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: **C: \Documents and Settings\Directorio de <usuario>**.

Visualización de las versiones traducidas de la interfaz web

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

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

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

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

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

Actualización del firmware de dispositivos

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

- Tarjetas Fibre Channel (FC)
- Diagnóstico
- Paquete de controladores del sistema operativo
- Tarjeta de interfaz de red (NIC)
- Controladora RAID
- Unidad de fuente de alimentación (PSU)
- Dispositivos PCIe NVMe
- Unidades de disco duro SAS/SATA
- Actualización de plano posterior para gabinetes internos y externos
- Recopilador del sistema operativo

PRECAUCIÓN: La actualización del firmware de la unidad de fuente de alimentación (PSU) puede tardar varios minutos, según la configuración del sistema y el modelo de la PSU. Para evitar daños en la PSU, no interrumpa el proceso de actualización ni encienda el sistema durante la actualización del firmware de la PSU.

Se debe cargar el firmware requerido en iDRAC. Una vez finalizada la carga, se muestra la versión actual del firmware instalado en el dispositivo y la versión aplicada. Si el firmware que se carga no es válido, aparecerá un mensaje de error. Las actualizaciones que no requieren un reinicio se aplican de inmediato. Las actualizaciones que requieren el reinicio del sistema se administran por etapas y se ejecutan en el siguiente reinicio del sistema. Un solo reinicio del sistema es suficiente para realizar todas las actualizaciones.

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

Los tipos de archivo de imagen admitidos del firmware son:

- **.exe**: Dell Update Package (DUP) basado en Windows
- **.d9**: contiene el firmware de iDRAC y de Lifecycle Controller.

Para los archivos con extensión **.exe**, debe contar con privilegio de control del sistema. La función con licencia de actualización remota del firmware debe estar activada; también debe estar activado Lifecycle Controller.

Para los archivos con extensión **.d9**, debe contar con privilegio de configuración.

NOTA: Después de actualizar el firmware del iDRAC, puede observar una diferencia en la fecha y la hora se muestran en el registro de Lifecycle Controller hasta que la hora del iDRAC se restablezca mediante NTP. El registro de Lifecycle muestra la hora del BIOS hasta que se restablezca la hora del iDRAC.

Puede realizar actualizaciones de firmware mediante los siguientes métodos:

- La carga de un tipo de imagen admitida, de una a la vez, desde un sistema local o recurso compartido de red.
- Conexión a un sitio FTP, TFTP, HTTP o HTTPS o a un repositorio de red que contenga los DUP de Windows y un archivo de catálogo correspondiente.

Puede crear repositorios personalizados con Dell Repository Manager. Para obtener más información, consulte *Dell Repository Manager Data Center User's Guide* (Guía del usuario de Dell Repository Manager Data Center). La iDRAC puede proporcionar un informe de diferencias entre el BIOS y el firmware instalados en el sistema y las actualizaciones disponibles en el repositorio. Todas las actualizaciones aplicables contenidas en el repositorio se aplican al sistema. Esta función está disponible con la licencia iDRAC Enterprise.

- Programación de actualizaciones recurrentes y automatizadas del firmware mediante el archivo de catálogo y el repositorio personalizado.

Hay varias interfaces y herramientas que se pueden usar para actualizar el firmware de iDRAC. La siguiente tabla se aplica únicamente al firmware de iDRAC. En la tabla, se muestran las interfaces compatibles, los tipos de archivos de imagen y si Lifecycle Controller debe estar en estado activado para que el firmware se actualice.

Tabla 10. Tipos de archivos de imagen y dependencias

	Imagen .d9		DUP de iDRAC	
Interfaz	**Compatible**	**Requiere LC activado**	**Compatible**	**Requiere LC activado**
Utilidad BMCFW64.exe	Sí	No	No	N/A
Racadm FWUpdate (antiguo)	Sí	No	No	N/A
Actualización de Racadm (nuevo)	Sí	Sí	Sí	Sí
UI de iDRAC	Sí	Sí	Sí	Sí
WSMan	Sí	Sí	Sí	Sí
DUP del sistema operativo en banda	No	N/A	Sí	No

La siguiente tabla proporciona información sobre si es necesario reiniciar el sistema cuando se actualiza el firmware de un componente en particular.

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

Tabla 11. Actualización del firmware: componentes admitidos

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

Nombre del componente	¿Reversión del firmware admitida? (Sí o No)	Fuera de banda: ¿es necesario reiniciar el sistema?	En banda: ¿es necesario reiniciar el sistema?	Interfaz gráfica de usuario de Lifecycle Controller: ¿es necesario reiniciar?
CPLD	No	Sí	Sí	Sí
Tarjetas de FC	Sí	Sí	Sí	Sí
Unidades SSD PCIe NVMe	Sí	No	No	No
Unidades de disco duro SAS/SATA	No	Sí	Sí	No
CMC (en servidores PowerEdge FX2)	No	Sí	Sí	Sí
Recopilador del sistema operativo	No	No	No	No

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

Cuando busque actualizaciones, la versión marcada como **Available (Disponible)** no siempre indica que se trata de la versión más reciente disponible. Antes de instalar la actualización, asegúrese de que la versión que seleccione para instalar sea más reciente que la versión instalada actualmente. Si desea controlar la versión que iDRAC detecta, cree un repositorio personalizado mediante Dell Repository Manager (DRM) y configure iDRAC para que use ese repositorio para buscar actualizaciones.

Actualización del firmware mediante la interfaz web de iDRAC

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

Actualización del firmware de un dispositivo individual

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

NOTA: Asegúrese de que el nombre del archivo para los DUP de un solo componente no tiene ningún espacio en blanco.

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

1. Vaya a **Maintenance (Mantenimiento)** > **System Update (Actualización del sistema)**.
   Se muestra la ventana **Actualización del firmware**.
2. En la ficha **Update (Actualizar)**, seleccione **Local** como la ubicación del archivo.
3. Haga clic en **Examinar**, seleccione el archivo de imagen del firmware del componente requerido y, a continuación, haga clic en **Cargar**.
4. Una vez finalizada la carga, la sección **Detalles de la actualización** muestra cada archivo del firmware cargado en el iDRAC y su estado.
   Si el archivo de imagen de firmware es válido y se cargó correctamente, en la columna **Contents (Contenido)** se muestra un icono más (+) junto al nombre del archivo de imagen de firmware. Expanda el nombre para ver la información de **Nombre del dispositivo**, **Actual** y **Versión del firmware disponible**.
5. Seleccione el archivo de firmware necesario y realice una de las acciones siguientes:
   - Para las imágenes del firmware que no requieren un reinicio del sistema host, haga clic en **Install (Instalar)**. Por ejemplo, en el archivo del firmware del iDRAC.
   - Para las imágenes de firmware que requieren un reinicio del sistema host, haga clic **Instalar y reiniciar** o **Instalar en el próximo reinicio**.

- Para cancelar la actualización del firmware, haga clic en **Cancelar**.

Al hacer clic en **Install (Instalar)**, **Install and Reboot (Instalar y reiniciar)** o **Install Next Reboot (Instalar en el próximo reinicio)**, se muestra el mensaje `Updating Job Queue`.

6 Para mostrar la página **Job Queue (Cola de trabajos)**, haga clic en **Job Queue (Cola de trabajos)**. Use esta página para ver y administrar las actualizaciones por etapas del firmware o haga clic en **OK (Aceptar)** para actualizar la página actual y ver el estado de la actualización del firmware.

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

Actualización del firmware mediante la actualización automática

1 En la interfaz web de iDRAC, vaya a **Maintenance (Mantenimiento)** > **System Update (Actualización del sistema)** > **Automatic Update (Actualización automática)**.

Se muestra la ventana **Automatic Update (Actualización automática)**.

2 Tiene la opción de seleccionar **Schedule Updates (Programar actualizaciones)** o **Schedule Updates and Reboot Server (Programar actualizaciones y reiniciar el servidor)** para automatizar las actualizaciones.

3 En la ficha **Location type (Tipo de ubicación)**, seleccione cualquiera de las opciones **Network Share (Recurso compartido de red)**, **FTP**, **TFTP**, **HTTP** o **HTTPS** para **File Location (Ubicación del archivo)**.

4 Según la opción seleccionada, deberá proporcionar más detalles de configuración.

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

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

5 La programación de la actualización de Windows le permite establecer los siguientes detalles:

- **Current iDRAC Time (Hora actual de iDRAC)**: muestra la hora del servidor real.
- **Start (24hr format) (Inicio [formato de 24 horas])**: permite establecer la hora.
- **Recurrence Pattern (Patrón de repetición)**: puede elegir la opción en función de sus requisitos empresariales. Las opciones disponibles son: **Daily (Diariamente)**, **Weekly (Semanalmente)**, **Monthly (Mensualmente)** o **Every <occurrence in number>Day (Cada <ocurrencia en número> días)**.

6 Haga clic en **Enable Automatic Update (Activar actualización automática)**.

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

NOTA: Puede optar por Disable Automatic Update (Desactivar actualización automática) según sus requisitos.

Actualización del firmware de dispositivos mediante RACADM

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

Ejemplos:

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

```
racadm update -f catalog.xml -l //192.168.1.1 -u test -p passwd --verifycatalog
```

- Para llevar a cabo todas las actualizaciones aplicables desde un repositorio de actualizaciones mediante **myfile.xml** como un archivo de catálogo y realizar un reinicio ordenado:

```
racadm update -f "myfile.xml" -b "graceful" -l //192.168.1.1 -u test -p passwd
```

- Para llevar a cabo todas las actualizaciones aplicables desde un repositorio de actualizaciones FTP mediante Catalog.xml como un archivo de catálogo:

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

Programación de actualizaciones automáticas del firmware

Puede crear un programa periódico recurrente para que el iDRAC compruebe las nuevas actualizaciones del firmware. En la fecha y la hora programadas, iDRAC se conecta al destino especificado, busca nuevas actualizaciones y aplica o divide en etapas todas las actualizaciones aplicables. Se crea un archivo de registro en el servidor remoto, que contiene información sobre el acceso al servidor y las actualizaciones del firmware en etapas.

Se recomienda crear un repositorio con Dell Repository Manager (DRM) y configurar iDRAC para que use este repositorio para buscar y realizar las actualizaciones del firmware. El uso de un depósito interno le permite controlar el firmware y las versiones disponibles para iDRAC y ayuda a evitar cualquier cambio no intencionado del firmware.

NOTA: Para obtener más información sobre DRM, consulte delltechcenter.com/repositorymanager.

Se necesita una licencia de iDRAC Enterprise para programar las actualizaciones automáticas.

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

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

Programación de la actualización automática del firmware mediante la interfaz web

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

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

1 En la interfaz web de iDRAC, vaya a **Maintenance (Mantenimiento)** > **System Update (Actualización del sistema)** > **Automatic Update (Actualización automática)**.

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

2 Haga clic en la ficha **Actualización automática**.

3 Seleccione la opción **Activar actualización automática** .

4 Seleccione cualquiera de las siguientes opciones para especificar si es necesario reiniciar el sistema después de apilar las actualizaciones:
- **Programar actualizaciones:** se apilan las actualizaciones del firmware pero no se reinicia el servidor.
- **Programar actualizaciones y reiniciar el servidor**: se activa el reinicio del servidor una vez apiladas las actualizaciones del firmware.

5 Seleccione una de las siguientes opciones para especificar la ubicación de las imágenes del firmware:
- **Network (Red)**: use el archivo de catálogo de un recurso compartido de red (CIFS, NFS, HTTP/HTTPS o TFTP). Introduzca los detalles de ubicación del recurso compartido de red.

  NOTA: Mientras se especifica la configuración para el recurso compartido de red, se recomienda evitar el uso de caracteres especiales en el nombre de usuario y la contraseña o codificar por porcentaje los caracteres especiales.
- **FTP**: utilice el archivo de catálogo del sitio FTP. Escriba los detalles del sitio FTP.
- **HTTP** o **HTTPS**: permite la transmisión por secuencias del archivo de catálogo y a través de la transferencia de archivos HTTP y HTTPS.

6 Según la opción elegida en el paso 5, introduzca los valores de configuración de la red o la configuración de FTP.

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

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

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

8 Haga clic en **Programar actualización**.

Se crea el próximo trabajo programado en la cola de trabajos. Cinco minutos después de que comienza la primera instancia de un trabajo recurrente, se crea el trabajo del próximo período de tiempo.

Programación de la actualización automática del firmware mediante RACADM

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

- Para activar la actualización automática del firmware:

```
racadm set lifecycleController.lcattributes.AutoUpdate.Enable 1
```

- Para ver el estado de la actualización automática del firmware:

```
racadm get lifecycleController.lcattributes.AutoUpdate
```

- Para programar la hora de inicio y la frecuencia de la actualización del firmware:

```
racadm AutoUpdateScheduler create -u username -p password -l <location>  [-f catalogfilename -pu <proxyuser> -pp<proxypassword> -po <proxy port> -pt <proxytype>] -time < hh:mm> [-dom < 1 – 28,L,'*'> -wom <1-4,L,'*'> -dow <sun-sat,'*'>] -rp <1-366> -a <applyserverReboot (1-enabled | 0-disabled)>
```

  Por ejemplo,

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

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

  - Para actualizar de forma automática el firmware mediante FTP:

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

- Para ver el programa actual de actualización del firmware:

```
racadm AutoUpdateScheduler view
```

- Para desactivar la actualización automática del firmware:

```
racadm set lifecycleController.lcattributes.AutoUpdate.Enable 0
```

- Para borrar los detalles de programa:

```
racadm AutoUpdateScheduler clear
```

- Cargue el archivo de actualización desde un recurso compartido HTTP remoto:

```
racadm update -f <updatefile> -u admin -p mypass -l http://1.2.3.4/share
```

- Cargue el archivo de actualización desde un recurso compartido HTTPS remoto:

```
racadm update -f <updatefile> -u admin -p mypass -l https://1.2.3.4/share
```

Actualización del firmware mediante la interfaz web de la CMC

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

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

1 Inicie sesión en la interfaz web de CMC.

2 Vaya a **iDRAC Settings (Configuración de iDRAC)** > **Settings (Configuración)** > **CMC**.

Aparecerá la página **Implementar iDRAC**.

3 Haga clic en **Iniciar iDRAC** para iniciar la interfaz web y seleccione **Actualización del firmware de iDRAC**.

Actualización del firmware mediante DUP

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

- Instalar y activar los controladores de sistema administrado y la IPMI correspondientes.
- Activar e iniciar el servicio Instrumental de administración de Windows (WMI) si el sistema ejecuta el sistema operativo Windows.

  NOTA: Mientras actualice el firmware de iDRAC mediante la utilidad de DUP en Linux, si aparecen mensajes de error como `usb 5-2: device descriptor read/64, error -71` en la consola, puede omitirlos.
- Si el sistema tiene el hipervisor ESX instalado, para que se ejecute el archivo DUP, asegúrese de que el servicio "usbarbitrator" se detenga mediante el comando `service usbarbitrator stop`.

Para actualizar iDRAC mediante DUP:

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

Actualización del firmware mediante RACADM remoto

1 Descargue la imagen del firmware en el servidor TFTP o FTP. Por ejemplo: **C:\downloads\firmimg.d9**.
2 Ejecute el siguiente comando de RACADM:
  Servidor TFTP:
  - Utilización del comando **fwupdate**:
    ```
    racadm -r <iDRAC IP address> -u <username> -p <password> fwupdate -g -u -a <path>
    ```
    `path` La ubicación en el servidor TFTP donde **firmimg.d9** está almacenado.
  - Utilización del comando **update**:
    ```
    racadm -r <iDRAC IP address> -u <username> -p <password> update –f <filename>
    ```

  Servidor FTP:
  - Utilización del comando **fwupdate**:
    ```
    racadm -r <iDRAC IP address> -u <username> -p <password> fwupdate –f <ftpserver IP>
    <ftpserver username> <ftpserver password> –d <path>
    ```
    `path` La ubicación en el servidor FTP donde **firmimg.d9** está almacenado.
  - Utilización del comando **update**:
    ```
    racadm -r <iDRAC IP address> -u <username> -p <password> update –f <filename>
    ```

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

Actualización del firmware mediante Lifecycle Controller Remote Services

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

Actualización del firmware de la CMC desde el iDRAC

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

Antes de aplicar la actualización, asegúrese de lo siguiente:

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

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

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

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

1 Inicie la interfaz web de la CMC.

2 Vaya a **iDRAC Settings (Configuración de iDRAC)** > **Settings (Configuración)** > **CMC**.

Aparecerá la página **Implementar iDRAC**.

3 En el menú desplegable **Chassis Management at Server Mode (Modo administración de chasis en el servidor)**, seleccione **Manage and Monitor (Administrar y supervisar)** y haga clic en **Apply (Aplicar)**.

Actualización del iDRAC para actualizar el firmware de la CMC

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

1 Vaya a **iDRAC Settings (Configuración de iDRAC)** > **Settings (Configuración)** > **CMC**.

2 Haga clic en **Chassis Management Controller Firmware Update (Actualización del firmware de Chassis Management Controller)**.

Aparecerá la página **Configuración de la actualización del firmware de Chassis Management Controller.**

3 Para **Permitir actualizaciones del a través de SO y Lifecycle Controller**, seleccione **Activado** para activar la actualización de firmware de la CMC desde el iDRAC.

4 En **Current CMC Setting (Configuración actual de la CMC)**, asegúrese de que la opción **Chassis Management at Server Mode (Administración de chasis en modo de servidor)** muestre **Manage and Monitor (Administrar y supervisar)**. Puede configurar esto en CMC.

Visualización y administración de actualizaciones preconfiguradas

Es posible ver y eliminar los trabajos programados, incluidos los trabajos de configuración y actualización. Esta es una función con licencia. Se pueden borrar todos los trabajos puestos en cola para ejecutarse en el próximo reinicio.

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

Para ver la lista de trabajos programados mediante la interfaz web de iDRAC, vaya a **Maintenance (Mantenimiento)** > **Job Queue (Cola de trabajos)**. En la página **Job Queue (Cola de trabajos)**, se muestra el estado de los trabajos en la cola de trabajos de Lifecycle Controller. Para obtener información acerca de los distintos campos, consulte *iDRAC Online Help (Ayuda en línea de iDRAC)*.

Para eliminar uno o varios trabajos, seleccione los trabajos y haga clic en **Delete (Eliminar)**. La página se actualiza y el trabajo seleccionado se elimina de la fila de trabajos en espera de Lifecycle Controller. Podrá eliminar todos los trabajos puestos en cola para la ejecución durante el próximo reinicio. No podrá eliminar trabajos activos; es decir, con el estado *Running (En ejecución)* o *Downloading (Descargando)*.

Para poder hacerlo, debe contar con privilegio de Control del servidor.

Visualización y administración de actualizaciones preconfiguradas mediante RACADM

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

Reversión del firmware del dispositivo

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

En los servidores PowerEdge de Dell de 14.ª generación que tienen un solo firmware de iDRAC y Lifecycle Controller, la reversión del firmware de la iDRAC también revierte el firmware de Lifecycle Controller.

Se recomienda para mantener el firmware actualizado asegurarse de tener las últimas funciones y actualizaciones de seguridad. Es posible que deba realizar una reversión de una actualizar o instalar una versión anterior si se produce algún problema después de una actualización. Para instalar una versión anterior, use Lifecycle Controller para comprobar si hay actualizaciones y seleccione la versión que desea instalar.

Puede realizar la reversión del firmware para los siguientes componentes:

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

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

Antes de revertir el firmware, asegúrese de:

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

- Cambiar el modo de NIC a **Dedicada** si el modo se establece como **LOM compartida**.

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

- Interfaz web del iDRAC
- Interfaz web del CMC
- CLI de RACADM: iDRAC y CMC
- Interfaz gráfica de usuario de Lifecycle Controller
- Lifecycle Controller–Remote Services

Reversión del firmware mediante la interfaz web de iDRAC

Para revertir el firmware de un dispositivo:

1 En la interfaz web de iDRAC, vaya a **Maintenance (Mantenimiento)** > **System Update (Actualización del sistema)** > **Rollback (Reversión)**.

La página **Revertir** muestra los dispositivos cuyo firmware se puede revertir. Puede ver el nombre del dispositivo, los dispositivos asociados, la versión del firmware instalado actualmente y la versión de reversión del firmware disponible.

2 Seleccione uno o más de los dispositivos cuyo firmware desea revertir.

3 Según los dispositivos seleccionados, haga clic en **Instalar y reiniciar** o **Instalar en el próximo reinicio**. Si sólo se selecciona el iDRAC, haga clic en **Instalar**.

Cuando hace clic en **Instalar y reiniciar** o en **Instalar en próximo reinicio**, aparecerá el mensaje "Actualizando fila de trabajo en espera".

4 Haga clic en **Cola de trabajo**.

Aparece la página **Fila de trabajo en espera**, donde podrá ver y administrar las actualizaciones de firmware apiladas.

NOTA:

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

Aparece un mensaje de error si:

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

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

Reversión del firmware mediante la interfaz web de la CMC

Para revertir mediante la interfaz web de CMC:

1 Inicie sesión en la interfaz web de CMC.

2 Vaya a **iDRAC Settings (Configuración de iDRAC)** > **Settings (Configuración)** > **CMC**.

Aparecerá la página **Implementar iDRAC**.

3 Haga clic en **Launch iDRAC (Iniciar iDRAC)** y realice una reversión del firmware del dispositivo como se indica en Reversión del firmware mediante la interfaz web de iDRAC.

Reversión del firmware mediante RACADM

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

```
racadm swinventory
```

Para el dispositivo para el que desea revertir el firmware, el valor de `Rollback Version` debe ser `Available`. Además, anote el valor de FQDD.

2 Revierta el firmware del dispositivo mediante:

```
racadm rollback <FQDD>
```

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

Reversión del firmware mediante Lifecycle Controller

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

Reversión del firmware mediante Lifecycle Controller Remote Services

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

Recuperación de iDRAC

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

- El cargador de inicio de la CLI de iDRAC detecta que no hay ninguna imagen iniciable.
- El LED de condición e identificación del sistema parpadea en intervalos de ~1/2 segundo. (El LED se encuentra en la parte posterior de los servidores en rack y torre, y en la parte delantera 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.d9** 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.d9, vuelve a programar iDRAC y luego reinicia iDRAC.

Copia de seguridad del perfil del servidor

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

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

Es posible restablecer iDRAC incluso cuando está en curso una operación de restauración o copia de seguridad de perfil de servidor.

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

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

- La opción Recopilar inventario del sistema al reiniciar (CSIOR) está activada. Si inicia una operación de recuperación mientras la opción CSIOR está desactivada, se muestra el siguiente mensaje:
  ```
  System Inventory with iDRAC may be stale,start CSIOR for updated inventory
  ```
- Para realizar una copia de seguridad en una tarjeta vFlash SD:
  - Tarjeta vFlash SD insertada, activada e inicializada.
  - Tarjeta vFlash SD tiene al menos 100 MB de espacio libre para almacenar el archivo de la copia de seguridad.

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

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

NOTA: Si va a exportar el perfil de servidor mediante NFS en el sistema operativo Windows 10 y tiene problemas para acceder al perfil de servidor exportado, active el cliente para NFS en las funciones de Windows.

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

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

1. Vaya a **iDRAC Settings (Configuración de iDRAC)** > **Settings (Configuración)** > **Backup and Export Server Profile (Hacer copia de seguridad y exportar perfil del servidor)**.
   Aparece la página **Hacer copia de seguridad y exportar perfil del servidor**.
2. Seleccione una de las siguientes opciones para guardar la imagen del archivo de copia de seguridad:
   - **Network Share (Recurso compartido de red)** para guardar la imagen del archivo de copia de seguridad en un recurso compartido CIFS o NFS.
   - **HTTP** o **HTTPS** para guardar la imagen del archivo de copia de seguridad en un archivo local a través de la transferencia de archivos HTTP/S.

     NOTA: Una vez montado el recurso compartido NFS, dentro de iDRAC, el usuario que no es raíz no puede escribir en el recurso compartido. Esto es para hacer que la iDRAC sea más segura.
3. Introduzca los siguientes detalles de la copia de seguridad: **File Name (Nombre de archivo)**, **Backup File Passphrase (Frase de contraseña del archivo de copia de seguridad)** (opcional) y **Confirm Passphrase (Confirmar frase de contraseña)**.
4. Si la opción **Network (Red)** está seleccionada como la ubicación del archivo, introduzca la configuración de la red correspondiente.

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

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

Copia de seguridad del perfil del servidor mediante RACADM

Para crear una copia de seguridad del perfil del servidor mediante RACADM, utilice el comando **systemconfig backup**.

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

Programación de la copia de seguridad automática del perfil del servidor

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

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

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

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

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

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

1. En la interfaz web de iDRAC, vaya a **iDRAC Settings (Configuración de iDRAC)** > **Settings (Configuración)** > **Backup and Export Server Profile (Hacer copia de seguridad y exportar perfil del servidor)**.
   Aparece la página **Hacer copia de seguridad y exportar perfil del servidor**.
2. Seleccione una de las siguientes opciones para guardar la imagen del archivo de copia de seguridad:
   - **Red** para guardar la imagen del archivo de copia de seguridad en un recurso compartido CIFS o NFS.
   - **HTTP o HTTPS** para guardar la imagen del archivo de copia de seguridad mediante la transferencia de archivos de HTTP/S.
3. Introduzca los siguientes detalles de la copia de seguridad: **File Name (Nombre de archivo)**, **Backup File Passphrase (Frase de contraseña del archivo de copia de seguridad)** (opcional) y **Confirm Passphrase (Confirmar frase de contraseña)**.
4. Si **Red** está seleccionada como la ubicación del archivo, introduzca la configuración de la red.

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

   Para obtener información acerca de los campos, consulte la *Ayuda en línea de iDRAC*
5. Haga clic en **Backup Now (Realizar copia de seguridad ahora)**.
   El trabajo recurrente se representa en la cola de trabajos con una fecha y hora de inicio para la próxima operación de copia de seguridad programada. Cinco minutos después de que comienza la primera instancia de un trabajo recurrente, se crea el trabajo del próximo período de tiempo. La operación de copia de seguridad del perfil del servidor se lleva a cabo a la fecha y hora programadas.

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

Para activar la copia de seguridad automática utilice el comando:

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

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

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

Para ver el programa de copia de seguridad actual:

```
racadm systemconfig getbackupscheduler
```

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

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

Para borrar el programa de copia de seguridad:

```
racadm systemconfig clearbackupscheduler
```

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

Importación del perfil del servidor

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

La función de importación no está bajo licencia.

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

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

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

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

```
Restore is already running
```

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

Restauración fácil

Después de colocar la placa base en el servidor, Restauración fácil le permite restaurar automáticamente los siguientes datos:

- System Service Tag
- Datos de licencias
- Aplicación de diagnósticos UEFI
- Ajustes de configuración del sistema (BIOS, iDRAC y NIC)

La restauración fácil utiliza la memoria flash de restauración fácil para la copia de seguridad de los datos. Cuando vuelve a colocar la placa base y enciende el sistema, el BIOS verifica la iDRAC y le preguntará si desea restaurar la copia de seguridad de los datos. La primera pantalla del BIOS le preguntará si desea restaurar la etiqueta de servicio, las licencias y la aplicación de diagnóstico de UEFI. La segunda pantalla del BIOS le preguntará si desea restaurar los valores de configuración del sistema. Si elige no restaurar los datos en la primera pantalla del BIOS y si no establece la etiqueta de servicio mediante otro método, la primera pantalla del BIOS se mostrará otra vez. La segunda pantalla del BIOS se muestra solo una vez.

NOTA:

- Se realiza una copia de seguridad de los valores de configuración del sistema solo cuando la opción CSIOR está activada. Asegúrese de que Lifecycle Controller y la opción CSIOR estén activadas.
- El Borrado del sistema no borra los datos almacenados en la memoria flash de Restauración fácil.
- Restauración fácil no hace copias de seguridad de otros datos como, por ejemplo, imágenes de firmware, datos vFlash o datos de tarjetas adicionales.

Importación del perfil del servidor mediante la interfaz web de iDRAC

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

1 Vaya a **iDRAC Settings (Configuración de iDRAC)** > **Settings (Configuración)** > **Import Server Profile (Importar perfil de servidor)**.

Aparecerá la sección **Importar perfil de servidor**.

2 Seleccione una de las siguientes opciones para especificar la ubicación del archivo de copia de seguridad:

- **Network Share (Recurso compartido de red)** para guardar la imagen del archivo de copia de seguridad en un recurso compartido CIFS o NFS.
- **HTTP/HTTPS** para guardar la imagen del archivo de copia de seguridad en un archivo local a través de la transferencia de archivos HTTP/S.

3 Introduzca los siguientes detalles de la copia de seguridad: **File Name (Nombre de archivo)**, **Backup File Passphrase (Frase de contraseña del archivo de copia de seguridad)** (opcional) y **Confirm Passphrase (Confirmar frase de contraseña)**.

4 Introduzca el **File Name (Nombre de archivo)** de la copia de seguridad y la frase de contraseña de descifrado (opcional).

5 Si **Red** está seleccionada como la ubicación del archivo, introduzca la configuración de la red.

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

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

6 Seleccione una de las siguientes opciones para **Configuración de discos virtuales y datos del disco duro**:

- **Preservar**: preserva el nivel de RAID, el disco virtual, los atributos de la controladora y los datos del disco duro en el sistema y restaura el sistema a un estado anterior conocido mediante el archivo de imagen de copia de seguridad.
- **Eliminar y reemplazar**: elimina y reemplaza el nivel de RAID, el disco virtual, los atributos de la controladora y la información de configuración del disco duro en el sistema con los datos del archivo de imagen de copia de seguridad.

7 Haga clic en **Importar**.

Se inicia la operación de importación del perfil del servidor.

Importación del perfil del servidor mediante RACADM

Para importar el perfil del servidor mediante RACADM, utilice el comando **systemconfig restore**.

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

Secuencia de operaciones de restauración

La secuencia de operaciones de restauración es la siguiente:

1 El sistema host se apaga.

2 La información del archivo de copia de seguridad se utiliza para restaurar Lifecycle Controller.

3 El sistema host se enciende.
4 El proceso de restauración del firmware y de la configuración de los dispositivos se completa.
5 El sistema host se apaga.
6 El proceso de restauración del firmware y de la configuración de iDRAC se completa.
7 iDRAC se reinicia.
8 El sistema host restaurado se enciende para reanudar el funcionamiento normal.

Supervisión de iDRAC mediante otras herramientas de administración del sistema

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

Compatibilidad con el perfil de configuración del servidor (SCP): importación y exportación

El perfil de configuración del servidor le permite importar y exportar archivos de configuración de servidor.

El usuario puede importar y exportar de la estación de administración local y desde un recurso compartido de red a través de CIFS, NFS, HTTP o HTTPS. El usuario puede especificar una importación o exportación orientada del SCP, donde el valor predeterminado es All (Todo). Con el SCP, puede seleccionar e importar o exportar configuraciones de nivel de componente para el BIOS, una NIC y RAID.

El usuario puede especificar una vista previa de la importación o la exportación del SCP donde se está ejecutando el trabajo y se genera el resultado de la configuración, pero no se aplica nada de la configuración.

Un trabajo se crea una vez que la importación o la exportación se inicia a través de la GUI. El estado de los trabajos puede verse en la página Job Queue (Cola de trabajos).

NOTA: Solo se acepta el nombre de host o la dirección IP para la dirección de destino.

NOTA: Puede buscar una ubicación específica para importar los archivos de configuración del servidor. Deberá seleccionar el archivo de configuración del servidor correcto que desee importar. Por ejemplo: import.xml.

NOTA: Según el formato del archivo exportado (que usted haya seleccionado), la extensión se agrega automáticamente. Por ejemplo: `export_system_config.xml`.

Configuración de inicio seguro desde la configuración del BIOS (F2)

El inicio seguro de UEFI es una tecnología que elimina la posibilidad de que se produzcan los principales vacíos de seguridad que pueden ocurrir durante la transferencia entre el firmware de UEFI y el sistema operativo (SO) de UEFI. En el inicio seguro de UEFI, cada componente de la cadena se valida y autoriza contra un certificado específico antes de permitir la carga o la ejecución. El inicio seguro elimina las amenazas heredadas y proporciona verificación de identidad de software en cada paso del inicio: el firmware de la plataforma, las tarjetas opcionales y el cargador de inicio del sistema operativo.

El foro de interfaz de firmware extensible unificada (UEFI) (un organismo del sector que desarrolla estándares para software previo al inicio) define el inicio seguro en la especificación de UEFI. Proveedores de sistemas para computadoras, tarjetas de expansión y sistemas operativos colaboran en esta especificación para promover la interoperabilidad. Como parte de la especificación de UEFI, el inicio seguro representa un estándar de todo el sector para la seguridad en el entorno previo al inicio.

Cuando está activado, el inicio seguro de UEFI impide que se carguen drivers de dispositivos UEFI no firmados, muestra un mensaje de error y no permitir que los dispositivos funcionen. Deberá desactivar el inicio seguro para cargar drivers de dispositivos no firmados.

En la 14.ª generación y versiones posteriores de los servidores Dell PowerEdge, puede activar o desactivar la función Secure Boot (Inicio seguro) mediante interfaces diferentes (RACADM, WSMAN, REDFISH y LC-UI).

Formatos de archivo aceptables

La política de inicio seguro solo contiene una clave en PK, pero varias claves pueden residir en KEK. Lo ideal sería que el fabricante de la plataforma o el propietario de la plataforma mantenga la clave privada correspondiente a la PK pública. Los otros fabricantes (como los proveedores de sistemas operativos y los proveedores de dispositivos) mantienen las claves privadas correspondientes a las claves públicas en KEK. De esta forma, los propietarios de la plataforma y los otros fabricantes pueden agregar o quitar entradas en DB o DBX de un sistema específico.

La política de inicio seguro utiliza DB y DBX para autorizar la ejecución del archivo de imagen previa al inicio. Para que se ejecute un archivo de imagen, debe estar asociado con una clave o un valor de algoritmo hash en DB y no debe estar asociado con una clave o un valor de algoritmo hash en DBX. Todo intento para actualizar el contenido de DB o DBX debe estar firmado con una KEK o PK privada. Todo intento para actualizar el contenido de PK o KEK debe estar firmado con una PK privada.

Componente de la política	Formatos de archivo aceptables	Extensiones de archivo aceptables	Registros máximos permitidos
PK	Certificado X.509 (solo con formato DER binario)	1 `.cer` 2 `.der` 3 .crt	Uno
KEK	Certificado X.509 (solo con formato DER binario) Almacenamiento de claves públicas	1 `.cer` 2 `.der` 3 `.crt` 4 `.pbk`	Más de uno
DB y DBX	Certificado X.509 (solo con formato DER binario) Imagen EFI (el BIOS del sistema calculará e importará el resumen de imagen).	1 `.cer` 2 `.der` 3 `.crt` 4 `.efi`	Más de uno

Se puede acceder a la función Secure Boot Settings (Configuración de inicio seguro) al hacer clic en System Security (Seguridad del sistema) en System BIOS Settings (Configuración del BIOS del sistema). Para ir a System BIOS Settings (Configuración del BIOS del sistema), presione F2 cuando aparezca el logotipo de la empresa durante la POST.

- De forma predeterminada, la opción Secure Boot (Inicio seguro) estará en el modo Disabled (Desactivado) y la política de inicio seguro está configurada en Standard (Estándar). Si se debe activar el inicio seguro, se debe configurar como Enabled (Activado).
- La política de inicio seguro configurada en Standard (Estándar) describe que el sistema tiene certificados predeterminados y resúmenes de imagen o un algoritmo hash cargados de la fábrica. Esto suma para la seguridad de firmware, drivers, ROM de opciones y cargadores de inicio estándares.
- En el caso de que deba admitirse un nuevo driver o firmware en el servidor, se debe inscribir el correspondiente certificado en la DB del almacén de certificados de inicio seguro. Por lo tanto, la política de inicio seguro se debe configurar en Custom (Personalizada).

Cuando la política de inicio seguro está configurada en Custom (Personalizada), hereda los certificados estándares y los resúmenes de imagen cargados en el sistema de forma predeterminada, en los que usted puede realizar cualquier cambio según sea necesario. La política de inicio seguro configurada en Custom (Personalizada) le permite realizar operaciones como ver, exportar, importar, eliminar, eliminar todo, restablecer y restablecer todo, mediante las cuales puede configurar las políticas de inicio seguro correspondientes a sus requisitos.

La configuración de la política de inicio seguro en Custom (Personalizada) activa las opciones para administrar el almacén de certificados mediante diversas acciones como exportar, importar, eliminar, eliminar todo, restablecer y restablecer todo en PK, KEK, DB y DBX. Puede seleccionar la política (PK/KEK/DB/DBX) en la que desea hacer el cambio y realizar las acciones pertinentes haciendo clic en el vínculo correspondiente. Cada sección tendrá vínculos para realizar las operaciones de importación, exportación, eliminación y restablecimiento. Los vínculos se activan según a qué se aplican, lo cual depende de la configuración en el momento. Las opciones Delete All (Borrar todo) y Reset All (Restablecer todo) son las operaciones que tienen impacto en todas las políticas. La opción Delete All (Eliminar todo) elimina todos los certificados y los resúmenes de imagen de política personalizada, y la opción Reset All (Restaura todo) restaura todos los certificados y resúmenes de imagen del almacén de certificados predeterminado o estándar.

4

Configuración de iDRAC

iDRAC permite configurar las propiedades de iDRAC, configurar usuarios y establecer alertas para realizar tareas de administración remotas. Antes de configurar iDRAC, asegúrese de que la configuración de red de iDRAC sea la correcta y de que esté configurado un navegador compatible, así como también que las licencias requeridas estén actualizadas. Para obtener más información acerca de la función con licencia en iDRAC, consulte Administración de licencias .

Puede configurar iDRAC con los siguientes elementos:

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

Para configurar iDRAC:

1 Inicie sesión en iDRAC.
2 Si fuera necesario, modifique la configuración de la red.

> **NOTA: Si ha configurado las opciones de red de iDRAC mediante la utilidad de configuración de iDRAC durante la configuración de la dirección IP de iDRAC, puede omitir este paso.**

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

Temas:

- Modificación de la configuración de red
- Modo FIPS (INTERFAZ)
- Configuración de servicios
- Configuración de TLS
- Uso del cliente de VNC Client para administrar el servidor remoto
- Configuración del panel frontal
- Configuración de zona horaria y NTP
- Configuración del primer dispositivo de inicio
- Activación o desactivación del paso del sistema operativo a iDRAC
- Obtención de certificados
- Configuración de varios iDRAC mediante RACADM
- Desactivación del acceso para modificar los valores de configuración de iDRAC en el sistema host

Visualización de la información de iDRAC

Puede ver las propiedades básicas de iDRAC.

Visualización de la información de iDRAC mediante la interfaz web

En la interfaz web de iDRAC, vaya a **iDRAC Settings (Configuración de iDRAC)** > **Overview (Descripción general)** para ver la siguiente información relacionada con iDRAC. Para obtener información sobre las propiedades, consulte *iDRAC Online Help (Ayuda en línea de iDRAC)*.

Detalles de iDRAC

- Tipo de dispositivo
- Versión del hardware
- Versión del firmware
- Actualización del firmware
- Hora del RAC
- Versión de IPMI
- Número de sesiones posibles
- Número actual de sesiones activas
- Versión de IPMI

Módulo de servicios de iDRAC

- Estado

Vista de conexión

- Estado
- Id. de conexión del switch
- Id. de conexión del puerto de switch

Configuración de red actual

- Dirección MAC de iDRAC
- Interfaz de NIC activa
- Nombre de dominio de DNS

Configuración de IPv4 actual

- IPv4 activado
- DHCP
- Dirección IP actual
- Máscara de subred actual
- Puerta de enlace actual
- Usar DHCP para obtener direcciones de servidor DNS
- Servidor DNS preferido actual
- Servidor DNS alternativo actual

Configuración IPv6 actual

- IPv6 habilitado
- Configuración automática
- Dirección IP actual
- Puerta de enlace de IP actual
- Dirección local de vínculo
- Usar DHCPv6 para obtener DNS
- Servidor DNS preferido actual
- Servidor DNS alternativo actual

Visualización de la información de iDRAC mediante RACADM

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

Modificación de la configuración de red

Después de establecer la configuración de red de iDRAC mediante la utilidad de configuración de iDRAC, también puede modificarla mediante la interfaz web de iDRAC, RACADM, Lifecycle Controller, Dell Deployment Toolkit y Server Administrator (después de iniciar en el sistema operativo). Para obtener más información sobre las herramientas y la configuración de privilegios, consulte las guías del usuario correspondientes.

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

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

Modificación de la configuración de red mediante la interfaz web

Para modificar la configuración de red de iDRAC:

1 En la interfaz web de iDRAC, vaya a **iDRAC Settings (Configuración de iDRAC)** > **Connectivity (Conectividad)** > **Network (Red)** > **Network Settings (Configuración de red)**.

Aparecerá la página **Red**.

2 Especifique la configuración de red, los valores comunes, IPv4, IPv6, IPMI y/o la configuración de VLAN según sus requisitos y haga clic en **Aplicar**.

Si selecciona la opción **Auto Dedicated NIC (NIC dedicada automáticamente)** en **Network Settings (Configuración de red)**, cuando la iDRAC tenga su selección de NIC como LOM compartida (1, 2, 3 o 4) y se detecte un vínculo en la NIC dedicada de iDRAC, la iDRAC

cambiará su selección de NIC para utilizar la NIC dedicada. Si no se detecta ningún vínculo en la NIC dedicada, la iDRAC utilizará la LOM compartida. El cambio del tiempo de espera de compartida a dedicada es de 5 segundos y de dedicada a compartida es de 30 segundos. Puede configurar este valor de tiempo de espera mediante RACADM o WSMAN.

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

Modificación de la configuración de red mediante RACADM local

Para generar una lista de las propiedades de red disponibles, utilice el comando:

```
racadm get iDRAC.Nic
```

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

```
racadm set iDRAC.IPv4.DHCPEnable 1
```

El siguiente es un ejemplo de cómo se puede utilizar el comando para configurar las propiedades de la red LAN necesarias.

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

NOTA: Si iDRAC.Nic.Enable se establece en 0, la LAN de iDRAC se desactiva aunque DHCP esté activado.

Configuración del filtrado de IP

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

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

A medida que se acumulan las fallas de inicio de sesión de una dirección IP específica, estas se registran mediante un contador interno. Cuando el usuario inicie sesión correctamente, el historial de fallas se borrará y el contador interno se restablecerá.

NOTA: Cuando se rechazan los intentos de inicio de sesión provenientes de la dirección IP cliente, algunos clientes de SSH pueden mostrar el siguiente mensaje: `ssh exchange identification: Connection closed by remote host`.

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

Configuración del filtrado IP mediante la interfaz web de iDRAC

Debe disponer del privilegio Configurar para realizar estos pasos.

Para configurar el filtrado de IP:

1 En la interfaz web de iDRAC, vaya a **iDRAC Settings (Configuración de iDRAC)** > **Network (Red)** > **Network Settings (Configuración de red)** > **Advanced Network Settings (Configuración avanzada de red)**.

Aparecerá la página **Red**.

2 Haga clic en **Advanced Network Settings (Configuración avanzada de red)**.

Se muestra la página **Seguridad de la red**.

3 Especifique la configuración de filtrado de IP mediante **IP Range Address (Dirección del rango de IP)** y **IP Range Subnet Mask (Máscara de subred del rango de IP)**.

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

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

Federal Information Processing Standards (FIPS) (Estándares federales de procesamiento de la información [FIPS]): es un conjunto de estándares utilizados por contratistas y agencias gubernamentales de Estados Unidos. El modo de FIPS está destinado a satisfacer los requisitos del Nivel 1 de FIPS 140-2. Para obtener más información sobre FIPS, consulte FIPS User Guide for iDRAC and CMC (Guía del usuario de FIPS para iDRAC y CMC).

NOTA: La activación de FIPS Mode (Modo de FIPS) restablece iDRAC a la configuración predeterminada.

Configuración del filtrado de IP mediante RACADM

Debe disponer del privilegio Configurar para realizar estos pasos.

Para configurar el filtrado de IP, utilice los siguientes objetos de RACADM en el grupo **iDRAC.IPBlocking**:

- RangeEnable
- RangeAddr
- RangeMask

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

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

```
RangeMask & (<incoming-IP-address> ^ RangeAddr)
```

&	AND bit a bit de las cantidades
^	OR bit a bit exclusivo

Ejemplos del filtrado IP

Los siguientes comandos de RACADM bloquean todas las direcciones IP, excepto la dirección 192.168.0.57:

```
racadm set iDRAC.IPBlocking.RangeEnable 1
racadm set iDRAC.IPBlocking.RangeAddr 192.168.0.57
racadm set iDRAC.IPBlocking.RangeMask 255.255.255.255
```

Para restringir los inicios de sesión a un conjunto de cuatro direcciones IP adyacentes (por ejemplo, de 192.168.0.212 a 192.168.0.215), seleccione todo excepto los últimos dos bits de la máscara:

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

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

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

Modo FIPS (INTERFAZ)

FIPS es un estándar de seguridad para computadoras que deben utilizar las agencias gubernamentales de Estados Unidos y los contratistas. A partir de la versión 2.40.40.40 de iDRAC, iDRAC admite la activación del modo FIPS.

iDRAC estará oficialmente certificado para admitir el modo FIPS en el futuro.

Diferencia entre admisión del modo FIPS y validación según FIPS

El software que se ha validado mediante la finalización del programa de validación del módulo criptográfico se denomina FIPS validado. Debido al tiempo que tarda la validación FIPS, no todas las versiones de iDRAC se valida. Para obtener más información sobre el estado más reciente de la validación FIPS de iDRAC, consulte la página Cryptographic Module Validation Program (Programa de validación del módulo criptográfico) en el sitio web de NIST.

Habilitación del modo FIPS

PRECAUCIÓN: La activación del modo FIPS restablece iDRAC a la configuración predeterminada de fábrica. Si desea restaurar la configuración, cree una copia de seguridad del perfil de configuración del servidor (SCP) antes de activar el modo FIPS y restaure el SCP después de que se reinicie iDRAC.

NOTA: Si reinstala o actualiza firmware del iDRAC, el modo FIPS se inhabilita.

Activar el modo FIPS mediante la interfaz web

1. En la interfaz web de iDRAC, vaya a **iDRAC Settings (Configuración de iDRAC)** > **Connectivity (Conectividad)** > **Network (Red)** > **Network Settings (Configuración de red)** > **Advanced Network Settings (Configuración avanzada de red)**.
2. En **Modo FIPS**, seleccione **Activado** y haga clic en **Aplicar**.

   NOTA: La activación de FIPS Mode (Modo de FIPS) restablece iDRAC a la configuración predeterminada.
3. Aparece un mensaje que le solicita que confirme el cambio. Haga clic en **OK** (Aceptar).

   Se reinicia iDRAC en el modo de FIPS. Espere al menos 60 segundos antes de volver a conectarse con iDRAC.
4. Instale un certificado de confianza para iDRAC.

   NOTA: El certificado de SSL predeterminado no se permite en modo FIPS.

NOTA: Algunas interfaces de iDRAC, como las implementaciones compatibles con los estándares de IPMI y SNMP, no admiten la conformidad con FIPS.

Activación del modo de FIPS mediante RACADM

Utilice CLI de RACADM para ejecutar el siguiente comando:

```
racadm set iDRAC.Security.FIPSMode <Enable>
```

Desactivación del modo FIPS

Para desactivar el modo FIPS, debe restablecer el iDRAC a los valores predeterminados de fábrica.

Configuración de servicios

Puede configurar y activar los siguientes servicios en iDRAC:

Configuración local	Desactive el acceso a la configuración de iDRAC (desde el sistema host) mediante RACADM local y la utilidad de configuración de iDRAC.
Servidor web	Active el acceso a la interfaz web de iDRAC. Si desactiva la interfaz web, la RACADM remota también se desactivará. Utilice la RACADM local para volver a activar el servidor web y la RACADM remota.
SSH	Acceda a iDRAC mediante el firmware RACADM.
Telnet	Acceda a iDRAC mediante el firmware RACADM.
RACADM remoto	Acceda a iDRAC de forma remota.
Redfish	Activa la compatibilidad de la API RESTful de Redfish.
Agente SNMP	Activa el soporte de consultas de SNMP (operaciones GET, GETNEXT y GETBULK) en iDRAC.
Agente de recuperación automática del sistema	Active la pantalla de último bloqueo del sistema.
Servidor VNC	Active el servidor VNC con o sin cifrado de SSL.

Configuración de servicios mediante la interfaz web

Para configurar los servicios mediante la interfaz web de iDRAC:

1 En la interfaz web de iDRAC, vaya a **iDRAC Settings (Configuración de iDRAC)** > **Services (Servicios)**.
Aparecerá la página **Servicios de directorio**.

2 Especifique la información necesaria y haga clic en **Aplicar**.
Para obtener información acerca de los distintos valores, consulte la *Ayuda en línea de iDRAC*.

> **NOTA: No seleccione la casilla de verificación Prevent this page from creating additional dialogs (Impedir que esta página cree diálogos adicionales). Al seleccionar esta opción, se impide la configuración de servicios.**

Configuración de servicios mediante RACADM

Para activar y configurar los servicios mediante RACADM, utilice el comando **set** con los objetos de los siguientes grupos de objetos:

- iDRAC.LocalSecurity
- iDRAC.LocalSecurity
- iDRAC.SSH
- iDRAC.Webserver
- iDRAC.Telnet
- iDRAC.Racadm

- iDRAC.SNMP

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

Activación o desactivación de la redirección de HTTPS

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

Debe tener el privilegio de configuración de iDRAC para poder activar o desactivar la redirección de HTTPS.

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

Para desactivar la redirección de HTTP a HTTPS:

```
racadm set iDRAC.Webserver.HttpsRedirection Disabled
```

Para activar la redirección de HTTP a HTTPS:

```
racadm set iDRAC.Webserver.HttpsRedirection Enabled
```

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

```
racadm get iDRAC.Webserver.HttpsRedirection
```

Configuración de TLS

De forma predeterminada, la iDRAC está configurada para utilizar TLS 1.1 y superior. Se puede configurar la iDRAC para que utilice cualquiera de las siguientes opciones:

- TLS 1.0 y superiores
- TLS 1.1 y superiores
- TLS 1.2 únicamente

NOTA: Para garantizar una conexión segura, Dell recomienda el uso de TLS 1.1 y posteriores.

Configuración de TLS por medio de la interfaz web

1 Vaya a **iDRAC Settings (Configuración de iDRAC)** > **Services (Servicios)**.
2 Haga clic en la pestaña **Servicios** y, a continuación, haga clic en **Servidor web**.
3 En la lista desplegable **Protocolo TLS**, seleccione la versión de TLS y haga clic en **Aplicar**.

Configuración del servidor TLS mediante RACADM

Para verificar la versión de TLS configurada:

```
racadm get idrac.webserver.tlsprotocol
```

Para establecer la versión de TLS:

```
racadm set idrac.webserver.tlsprotocol <n>
```

<n>=0	TLS 1.0 y superior
<n>=1	TLS 1.1 y superior
<n>=2	Sólo TLS 1.2

Uso del cliente de VNC Client para administrar el servidor remoto

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

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

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

Se pueden activar 2 sesiones de cliente VNC al mismo tiempo. La segunda estará en el modo de solo lectura.

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

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

NOTA:

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

Configuración del servidor VNC mediante la interfaz web del iDRAC

Para configurar los valores del servidor VNC:

1. En la interfaz web de iDRAC, vaya a **Configuration (Configuración)** > **Virtual Console (Consola virtual)**.
   Aparece la página **Consola virtual**.
2. En la sección **Servidor VNC**, active el servidor VNC, especifique la contraseña, el número de puerto y active o desactive el cifrado SSL.
   Para obtener información acerca de los campos, consulte la *Ayuda en línea de iDRAC7*.
3. Haga clic en **Aplicar**.
   El servidor VNC está configurado.

Configuración del servidor VNC mediante RACADM

Para configurar el servidor VNC, utilice el comando `set` con los objetos en `VNCserver`.

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

Configuración del visor VNC con cifrado SSL

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

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

Para configurar la aplicación de túnel SSL:

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

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

Configuración del visor VNC sin Cifrado SSL

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

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

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

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

Configuración del panel frontal

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

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

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

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

Configuración de los valores de LCD

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

Configuración de los valores LCD mediante la interfaz web

Para configurar la pantalla de panel anterior LCD del servidor:

1 En la interfaz web de iDRAC, vaya a **Configurations (Configuraciones)** > **System Settings (Configuración del sistema)** > **Hardware Settings (Configuración de hardware)** > **Front Panel configuration (Configuración del panel frontal)**.

2 En la sección **Configuración de LCD**, en el menú desplegable **Configurar mensaje de inicio** seleccione cualquiera de los elementos siguientes:

- Etiqueta de servicio (predeterminado)
- Asset Tag
- Dirección MAC de DRAC
- Dirección IPv4 de DRAC
- Dirección IPv6 de DRAC
- Alimentación del sistema
- Temperatura ambiente
- Modelo del sistema
- Nombre del host
- Definido por el usuario
- Ninguno

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

  Si selecciona **Ninguno**, el mensaje de inicio no se muestra en el panel frontal del LCD.

3 Active la indicación de la consola virtual (opcional). Una vez activada, la sección de fuente en directo del panel frontal y el panel LCD del servidor mostrarán el mensaje `Virtual console session active` cuando haya una sesión de consola virtual activa.

4 Haga clic en **Aplicar**.

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

Configuración de los valores LCD mediante RACADM

Para configurar la pantalla LCD del panel frontal del servidor, utilice los objetos en el grupo System.LCD.

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

Configuración de LCD mediante la utilidad de configuración de iDRAC

Para configurar la pantalla de panel anterior LCD del servidor:

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

Se mostrará la página **Configuración de iDRAC - Seguridad del panel frontal**.

2 Active o desactive el botón de encendido.

3 Especifique lo siguiente:

- Acceso al panel frontal

- Cadena de mensajes de LCD
- Unidades de alimentación del sistema, unidades de temperatura ambiente y visualización de errores

4 Active o desactive la indicación de consola virtual.

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

5 Haga clic en **Atrás**, en **Terminar** y, a continuación, en **Sí**.

Configuración del valor LED del Id. del sistema

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

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

Para configurar la visualización de LED de ID del sistema:

1 En la interfaz web de iDRAC, vaya a **Configuration (Configuración)** > **System Settings (Configuración del sistema)** > **Hardware Settings (Configuración de hardware)** > **Front Panel configuration (Configuración del panel frontal)**. Se muestra la página **System ID LED Settings (Configuración de LED de Id. del sistema)**.

2 En la sección **Configuración de LED de ID del sistema**, seleccione cualquier de las opciones siguientes para activar o desactivar el parpadeo de LED:

- Desactivar parpadeo
- Activar parpadeo
- Activar parpadeo del tiempo de espera de 1 día
- Activar parpadeo del tiempo de espera de 1 semana
- Activar parpadeo del tiempo de espera de 1 mes

3 Haga clic en **Aplicar**.

Se habrá configurado el parpadeo de LED en el panel frontal.

Configuración del valor LED de Id. del sistema mediante RACADM

Para configurar el LED de identificación del sistema, utilice el comando **setled**.

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

Configuración de zona horaria y NTP

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

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

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

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

1 Vaya a **iDRAC Settings (Configuración de iDRAC)** > **Settings (Configuración)** > **Time zone and NTP Settings (Zona horaria y los parámetros de NTP)**.

Se mostrará la página **Zona horaria y NTP**.

2 Para configurar la zona horaria, en el menú desplegable **Zona horaria**, seleccione la zona horaria requerida y haga clic en **Aplicar**.

3 Para configurar NTP, active NTP, introduzca las direcciones del servidor NTP y haga clic en **Aplicar**.

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

Configuración de zona horaria y NTP mediante RACADM

Para configurar el huso horario y NTP, utilice el comando **set** con los objetos en el grupo **iDRAC.Time** y **iDRAC.NTPConfigGroup**.

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

Configuración del primer dispositivo de inicio

Puede configurar el primer dispositivo de inicio solo para el siguiente inicio o para todos los reinicios subsiguientes. Si configura el dispositivo para que se utilice para todos los inicios subsiguientes, permanecerá como el primer dispositivo de inicio en el orden de inicio del BIOS, hasta que se cambie de nuevo desde la interfaz web de iDRAC o desde la secuencia de inicio del BIOS.

Puede configurar el primer dispositivo de inicio en una de las siguientes opciones:

- Inicio normal
- PXE
- Configuración del BIOS
- Disco flexible local/unidades extraíbles principales
- CD/DVD local
- Unidad de disco duro
- Disco flexible virtual
- CD/DVD/ISO virtual
- Tarjeta SD local
- Lifecycle Controller
- Administrador de inicio del BIOS
- Ruta de acceso dispositivo UEFI
- HTTP de UEFI

NOTA:

- BIOS Setup (F2), Lifecycle Controller (F10) y BIOS Boot Manager (F11) no pueden configurarse como dispositivo de inicio permanente.
- La configuración del primer dispositivo de inicio en la interfaz web de iDRAC invalida la configuración de inicio del BIOS del sistema.

Configuración del primer dispositivo de inicio mediante la interfaz web

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

1 Vaya a **Configuration (Configuración)** > **System Settings (Configuración del sistema)** > **Hardware Settings (Configuración de hardware)** > **First Boot Device (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 **Boot Once (Iniciar una vez)**. A continuación, el sistema se inicia desde el primer dispositivo de inicio en el orden de inicio del BIOS.

Para obtener más información sobre las opciones, consulte la *Ayuda en línea de iDRAC*.

Configuración del primer dispositivo de inicio mediante RACADM

- Para configurar el primer dispositivo de inicio, utilice el objeto **iDRAC.ServerBoot.FirstBootDevice**.
- Para activar el inicio una única vez para un dispositivo, utilice el objeto **iDRAC.ServerBoot.BootOnce**.

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

Configuración del primer dispositivo de inicio mediante la consola virtual

Puede seleccionar el dispositivo desde el cual desea realizar el inicio, ya que el servidor se visualiza en el visor de la consola virtual antes de que el servidor se ejecute a través de su secuencia de inicio. Puede llevar a cabo el inicio una vez para todos los dispositivos compatibles que se enumeran en Configuración del primer dispositivo de inicio.

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

1 Inicie la consola virtual.

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

Activación de la pantalla de último bloqueo

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

NOTA: Para obtener información sobre Server Administrator, consulte *Dell OpenManage Server Administrator Installation Guide (Guía de instalación de Dell OpenManage Server Administrator)*, disponible en dell.com/support/manuals.

1 Desde el DVD de *herramientas y documentación de administración de sistemas Dell* o desde el sitio web de soporte de Dell, instale Server Administrator o iDRAC Service Module (iSM) en el sistema administrado.

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).

4 Active la opción **Apagado y recuperación automática** (ASR) mediante uno de los procedimiento siguientes:
- Server Administrator: consulte la *guía del usuario de Dell OpenManage Server Administrator*.
- RACADM local: utilice el comando `racadm config -g cfgRacTuning -o cfgRacTuneAsrEnable 1`.

5 Active la opción **Automated System Recovery Agent (Agente de recuperación automática del sistema)**. Para ello, vaya a **iDRAC Settings (Configuración de iDRAC)** > **Services (Servicios)** > **Automated System Recovery Agent (Agente de recuperación automatizada del sistema)** y seleccione **Enabled (Activado)** y haga clic en **Apply (Aplicar)**.

Activación o desactivación del paso del sistema operativo a iDRAC

En los servidores que tienen una tarjeta de red dependiente (NDC) o dispositivos LAN en la placa base (LOM) incorporados, puede activar la función OS to iDRAC Pass-through (Paso del sistema operativo a iDRAC). Esta función proporciona una comunicación en banda

bidireccional y de alta velocidad entre iDRAC y el sistema operativo host a través de una LOM compartida, una NIC dedicada o la NIC de USB. Esta función está disponible para la licencia iDRAC Enterprise.

NOTA: El Módulo de servicio de iDRAC (iSM) proporciona más funciones de administración de la iDRAC a través del sistema operativo. Para obtener más información, consulte *iDRAC Service Module Installation Guide (Guía de instalación del Módulo de servicio de iDRAC)*, disponible en dell.com/support/manuals.

Cuando se activa a través de la NIC dedicada, es posible iniciar el navegador en el sistema operativo host y acceder a la interfaz web de iDRAC. La NIC dedicada para los servidores blade es a través de Chassis Management Controller.

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

Es posible activar este canal mediante las siguientes opciones:

- Interfaz web del iDRAC
- RACADM o WSMan (entorno posterior al sistema operativo)
- Utilidad de configuración de iDRAC (entorno previo al sistema operativo)

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

Si configura el servidor con un perfil de configuración del servidor a través de RACADM, WSMan o Redfish y si se cambia la configuración de la red en este archivo, debe esperar 15 segundos para activar la función OS to iDRAC Pass-through (Paso del sistema operativo a iDRAC) o para establecer la dirección IP del sistema operativo host.

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

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

Cuando active esta función:

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

Si la función de paso de sistema operativo a iDRAC no funciona después de que está activada, asegúrese de comprobar lo siguiente:

- El cable de la NIC dedicada de iDRAC está conectado correctamente.
- Al menos una LOM está activa.

NOTA: Utilice la dirección IP predeterminada. Asegúrese de que la dirección IP de la interfaz de la NIC de USB no esté en la misma subred que las direcciones IP del sistema operativo host o iDRAC. Si esta dirección IP entra en conflicto con una dirección IP de otras interfaces del sistema host o la red local, deberá cambiarla.

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

Tarjetas admitidas para el paso del sistema operativo al iDRAC

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

Tabla 12. : paso del sistema operativo a iDRAC mediante LOM: tarjetas admitidas

Categoría	Fabricante	Tipo
NDC	Broadcom	• 5720 QP rNDC 1G BASE-T • 57810S DP bNDC KR • 57800S QP rNDC (10G BASE-T + 1G BASE-T) • 57800S QP rNDC (10G SFP+ + 1G BASE-T) • 57840 4x10G KR. • 57840 rNDC
	Intel	• i540 QP rNDC (10G BASE-T + 1G BASE-T) • i350 QP rNDC 1G BASE-T • x520/i350 rNDC de 1GB
	QLogic	QMD8262 Blade NDC

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

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

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

Sistemas operativos admitidos para la NIC de USB

Los sistemas operativos admitidos para la NIC de USB son:

- Server 2012 R2 Foundation Edition
- Server 2012 R2 Essentials Edition
- Server 2012 R2 Standard Edition
- Server 2012 R2 Datacenter Edition
- Server 2012 for Embedded Systems (base y R2 con SP1)
- Server 2016 Essentials Edition
- Server 2016 Standard Edition
- Server 2016 Datacenter Edition
- RHEL 7.3
- RHEL 6.9
- SLES 12 SP2
- ESXi 6.0 U3
- vSphere 2016
- XenServer 7.1

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

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

Instalación del archivo VIB

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

Para instalar el archivo VIB:

1 Mediante Win-SCP, copie el archivo VIB a la carpeta **/tmp/** del sistema operativo host ESX-i.

2 Vaya al símbolo de ESXi y ejecute el siguiente comando:

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

El resultado es:

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

3 Reinicie el servidor.

4 A petición de ESXi, ejecute el comando: `esxcfg-vmknic -l`.

El resultado muestra la anotación usb0.

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

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

1 Vaya a **iDRAC Settings (Configuración de iDRAC)** > **Connectivity (Conectividad)** > **Network (Red)** > **OS to iDRAC Pass-through (Paso del sistema operativo a iDRAC)**.

Se mostrará la página **Paso del sistema operativo a iDRAC**.

2 Seleccione cualquiera de las siguientes opciones para activar el paso del sistema operativo al iDRAC:

- **LOM**: el vínculo de paso del sistema operativo al iDRAC entre el iDRAC y el sistema operativo host se establece mediante la LOM o NDC.
- **NIC de USB**: el vínculo de paso del sistema operativo al iOS entre el iDRAC y el sistema operativo host se establece mediante la DRAC o USB.

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

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

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

4 Si selecciona **NIC de USB** como configuración de paso, introduzca la dirección IP de la NIC del USB.

El valor predeterminado es 169.254.0.1. Se recomienda utilizar la dirección IP predeterminada. Sin embargo, si esta dirección IP entra en conflicto con una dirección IP de otras interfaces del sistema host o la red local, deberá cambiarla.

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

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

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

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

Para activar o desactivar el paso del sistema operativo a iDRAC mediante RACADM, utilice los objetos en el grupo **iDRAC.OS-BMC**.

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

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

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

1 En la utilidad de configuración de iDRAC, vaya a **Permisos de comunicaciones**.

Aparecerá la página **Configuración de los permisos de comunicaciones de iDRAC**.

2 Seleccione cualquiera de las siguientes opciones para activar el paso del sistema operativo al iDRAC:

- **LOM**: el vínculo de paso del sistema operativo al iDRAC entre el iDRAC y el sistema operativo host se establece mediante la LOM o NDC.
- **NIC de USB**: el vínculo de paso del sistema operativo al iOS entre el iDRAC y el sistema operativo host se establece mediante la DRAC o USB.

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

> **NOTA: Solo se puede seleccionar la opción LOM si la tarjeta admite la función de paso del sistema operativo a iDRAC. De lo contrario, esta opción aparece en gris.**

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

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

4 Si selecciona **NIC de USB** como configuración de paso, introduzca la dirección IP de la NIC del USB.

El valor predeterminado es 169.254.0.1. Sin embargo, si esta dirección IP entra en conflicto con una dirección IP de otras interfaces del sistema host o la red local, deberá cambiarla. No introduzca las IP 169.254.0.3 y 169.254.0.4. Estas IP están reservadas para el puerto de NIC de USB en el panel frontal cuando se utiliza un cable A/A.

5 Haga clic en **Atrás**, en **Terminar** y, a continuación, en **Sí**.

Los detalles se guardan.

Obtención de certificados

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

Tabla 13. 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

Tipo de inicio de sesión	Tipo de certificado	Cómo obtenerlo
		También se admiten los certificados SHA-2.
Inicio de sesión mediante tarjeta inteligente como usuario local o de Active Directory	• Certificado de usuario • Certificado de CA de confianza	• 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. También se admiten los certificados SHA-2.
Inicio de sesión de usuario de Active Directory	Certificado de CA de confianza	Este certificado lo emite una CA. También se admiten los certificados SHA-2.
Inicio de sesión de usuario local	Certificado SSL	Generar una CSR y hacer que la firme una CA de confianza **NOTA: La iDRAC se entrega con un certificado del servidor SSL autofirmado predeterminado. El servidor web de iDRAC, los medios virtuales y la consola virtual utilizan este certificado.** También se admiten los certificados SHA-2.

Certificados de servidor SSL

La iDRAC incluye un servidor web configurado para usar el protocolo de seguridad estándar en la industria SSL para transferir datos cifrados a través de una red. Se proporciona una opción de cifrado SSL para desactivar los cifrados débiles. Basado en la tecnología de cifrado asimétrico, SSL se acepta ampliamente para el suministro de comunicaciones autenticadas y cifradas entre clientes y servidores para impedir el espionaje a través de una red.

Un sistema habilitado para SSL puede realizar las siguientes tareas:

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

NOTA: Si el cifrado SSL se configura en 256 bits o más y 168 bits o más, es posible que la configuración de la criptografía para el entorno de máquinas virtuales (JVM o IcedTea) necesite la instalación de la extensión Unlimited Strength Java Cryptography Extension Policy Files para permitir el uso de los complementos de iDRAC tales como vConsole con este nivel de cifrado. Para obtener información sobre cómo instalar los archivos de políticas, consulte la documentación de Java.

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

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

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

El certificado SSL del servidor web de iDRAC admite el carácter de asterisco (*) como parte del componente ubicado más a la izquierda del nombre común al generar una solicitud de firma de certificado (CSR). Por ejemplo: *.qa.com o *.company.qa.com. Esto se denomina certificado comodín. Si se genera una CSR comodín fuera de iDRAC, podrá contar con un solo certificado SSL comodín firmado que puede cargar para varias iDRAC y todas las iDRAC serán de confianza para todos los navegadores compatibles. Si se conecta a la interfaz web de iDRAC mediante un navegador compatible que admite un certificado comodín, la iDRAC será de confianza para el navegador. Al iniciar los visores, las iDRAC serán de confianza para los clientes de los visores.

Generación de una nueva solicitud de firma de certificado

Una CSR es una solicitud digital para una autoridad de certificado (CA) de un certificado del servidor SSL. Los certificados del servidor SSL les permiten a los clientes del servidor confiar en la identidad del servidor y 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 con 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 navegadores que se ejecutan en estaciones de administración.

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

Generación de CSR mediante la interfaz web

Para generar una CSR nueva:

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

1. En la interfaz web de iDRAC, vaya a **iDRAC Settings (Configuración de iDRAC)** > **Connectivity (Conectividad)** > **SSL** > **SSL certificate (Certificado SSL)**, seleccione **Generate Certificate Signing Request (CSR) (Generar solicitud de firma de certificado [CSR])** y, a continuación, haga clic en **Next (Siguiente)**.

   Aparece la página **Generar una nueva solicitud de firma de certificado (CSR)**.
2. Introduzca un valor para cada atributo de la CSR.

   Para obtener más información, consulte la *Ayuda en línea de iDRAC*.
3. Haga clic en **Generar**.

   Se genera una nueva CSR. Guárdela en la estación de administración.

Generación de CSR mediante RACADM

Para generar una CSR mediante RACADM, utilice el comando **set** con los objetos en el grupo **iDRAC.Security** y, a continuación, utilice el comando **sslcsrgen** para generar la CSR.

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

Carga del certificado del servidor

Después de generar una CSR, puede cargar el certificado del servidor SSL firmado en el firmware de iDRAC. La iDRAC debe restablecerse para aplicar el certificado. La iDRAC acepta solamente certificados de servidor web X.509 codificados en Base64. También se admiten los certificados SHA-2.

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

Carga del certificado del servidor mediante la interfaz web

Para cargar el certificado de servidor SSL:

1. En la interfaz web de iDRAC, vaya a **iDRAC Settings (Configuración de iDRAC)** > **Connectivity (Conectividad)** > **SSL** > **SSL certificate (Certificado SSL)**, seleccione **Upload Server Certificate (Cargar certificado del servidor)** y haga clic en **Next (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 iDRAC.
4. Aparecerá un mensaje emergente solicitándole que reinicie iDRAC de inmediato o más adelante. Haga clic en **Reiniciar iDRAC** o en **Reiniciar iDRAC más adelante**, según sea necesario.

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

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

Carga del certificado del servidor mediante RACADM

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

Si la CSR se genera fuera del iDRAC con una clave privada disponible, para cargar el certificado en el iDRAC:

1. Envíe la CSR a una Autoridad de certificados raíz reconocida. La autoridad de certificados firma la CSR y ésta se convierte en un certificado válido.
2. Cargue la clave privada mediante el comando de RACADM remota `sslkeyupload`.
3. Cargue el certificado firmado en iDRAC con el comando de RACADM remota `sslcertupload`.

   El nuevo certificado se ha cargado en iDRAC. Aparecerá un mensaje solicitándole que reinicie iDRAC.
4. Ejecute el comando racadm **racreset** para reiniciar iDRAC.

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

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

Visualización del certificado del servidor

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

Visualización del certificado del servidor mediante la interfaz web

En la interfaz web de iDRAC, vaya a **iDRAC Settings (Configuración de iDRAC)** > **Connectivity (Conectividad)** > **SSL** > **SSL Certificate (Certificado SSL)**. En la página **SSL**, se muestra el certificado del servidor SSL que se encuentra actualmente en uso en la parte superior de la página.

Visualización del certificado del servidor mediante RACADM

Para ver el certificado del servidor SSL, utilice el comando **sslcertview**.

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

Carga del certificado de firma personalizado

Puede cargar un certificado de firma personalizado para firmar el certificado SSL. También se admiten los certificados SHA-2.

Carga del certificado de firma personalizado mediante la interfaz web

Para cargar el certificado de firma personalizado mediante la interfaz web de iDRAC:

1. Vaya a **iDRAC Settings (Configuración de iDRAC)** > **Connectivity (Conectividad)** > **SSL**.
   Aparecerá la página **SSL**.
2. En **Custom SSL Certificate Signing Certificate (Certificado de firma del certificado SSL personalizado)**, haga clic en la opción **Upload Signing Certificate (Cargar certificado de firma)**.
   Aparecerá la página **Cargar certificado de firma del certificado SSL personalizado**.
3. Haga clic en **Choose File (Seleccionar archivo)** y seleccione el archivo del certificado de firma del certificado SSL personalizado.
   Solo se admite el certificado que cumple con las normas de criptografía de claves públicas N.º 12 (PKCS N.º 12).
4. Si el certificado está protegido con contraseña, introduzca la contraseña en el campo **Contraseña de PKCS N.º 12**.
5. Haga clic en **Aplicar**.
   El certificado se ha cargado en iDRAC.
6. Aparecerá un mensaje emergente solicitándole que reinicie iDRAC de inmediato o más adelante. Haga clic en **Reiniciar iDRAC** o en **Reiniciar iDRAC más adelante**, según sea necesario.
   Se reiniciará iDRAC y se aplicará el nuevo certificado. iDRAC no estará disponible por algunos minutos durante el reinicio.

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

Carga del certificado de firma del certificado SSL personalizado mediante RACADM

Para cargar el certificado de firma del certificado de SSL personalizado mediante RACADM, utilice el comando **sslcertupload** y, a continuación, utilice el comando **racreset** para restablecer el iDRAC.

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

Descarga del certificado de firma del certificado SSL personalizado

Puede descargar el certificado de firma personalizado mediante la interfaz web de iDRAC o RACADM.

Descarga del certificado de firma personalizado

Para descargar el certificado de firma personalizado mediante la interfaz web de iDRAC:

1 Vaya a **iDRAC Settings (Configuración de iDRAC)** > **Connectivity (Conectividad)** > **SSL**.
Aparecerá la página **SSL**.

2 En **Certificado de firma del certificado SSL personalizado**, seleccione **Descargar certificado de firma del certificado SSL personalizado** y haga clic en **Siguiente**.
Se mostrará un mensaje emergente que permite guardar el certificado de firma personalizado en la ubicación que seleccione.

Descarga del certificado de firma del certificado SSL personalizado mediante RACADM

Para descargar el certificado de firma del certificado SSL personalizado, utilice el subcomando **sslcertdownload**. Para obtener más información, consulte *iDRAC RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM de iDRAC), disponible en **dell.com/idracmanuals**.

Eliminación del certificado de firma del certificado SSL personalizado

También es posible eliminar un certificado de firma personalizado existente mediante la interfaz web de iDRAC o RACADM.

Eliminación del certificado de firma personalizado mediante la interfaz web de iDRAC

Para eliminar el certificado de firma personalizado mediante la interfaz web de iDRAC:

1 Vaya a **iDRAC Settings (Configuración de iDRAC)** > **Connectivity (Conectividad)** > **SSL**.
Aparecerá la página **SSL**.

2 En **Certificado de firma del certificado SSL personalizado**, seleccione **Eliminar certificado de firma del certificado SSL personalizado** y haga clic en **Siguiente**.

3 Aparecerá un mensaje emergente solicitándole que reinicie iDRAC de inmediato o más adelante. Haga clic en **Reiniciar iDRAC** o en **Reiniciar iDRAC más adelante**, según sea necesario.
Luego de reiniciar iDRAC, se generará un nuevo certificado autofirmado.

Eliminación del certificado de firma del certificado SSL personalizado mediante RACADM

Para eliminar el certificado de firma del certificado SSL personalizado con RACADM, utilice el subcomando **sslcertdelete**. Luego, use el comando **racreset** para restablecer iDRAC.

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

Configuración de varios iDRAC mediante RACADM

Puede configurar una o varias iDRAC con propiedades idénticas mediante RACADM. Cuando se realiza una consulta en una iDRAC específica con su Id. de grupo y su Id. de objeto, RACADM crea un archivo de configuración a partir de la información recuperada. Importe el archivo en otras iDRAC para configurarlas de manera idéntica.

NOTA:

- El archivo de configuración contiene información que es aplicable para el servidor en particular. La información se organiza en diferentes grupos de objetos.
- Algunos archivos de configuración contienen información de iDRAC única, tal como la dirección IP estática, que debe modificar antes de importar el archivo a otros iDRAC.

También puede utilizar el perfil de configuración del sistema para configurar varias iDRAC mediante RACADM. El archivo XML de configuración del sistema contiene la información de configuración de los componentes. Puede utilizar este archivo para aplicar la configuración a BIOS, iDRAC, RAID y NIC mediante la importación del archivo en un sistema objetivo. Para obtener más información, consulte las notas técnicas *XML Configuration Workflow (Flujo de trabajo de la configuración de XML)*, disponible en **dell.com/support/manuals** o en Dell Tech Center.

Para configurar varios iDRAC con el archivo de configuración:

1 Consulte el iDRAC de destino que contiene la configuración necesaria mediante el siguiente comando:.

```
racadm get -f <file_name>.xml -t xml -c iDRAC.Embedded.1
```

El comando solicita la configuración de iDRAC y genera el archivo de configuración.

NOTA: La redirección de la configuración de iDRAC hacia un archivo por medio de `get -f` solo se admite con las interfaces local y remota de RACADM.

NOTA: El archivo de configuración generado no contiene contraseñas de usuario.

El comando **get** 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.

2 Modifique el archivo de configuración con un editor de textos, de ser necesario.

NOTA: Se recomienda editar este archivo con un editor de textos simple. La utilidad RACADM utiliza un analizador de textos ASCII. Los elementos de formato confunden al analizador y esto puede dañar la base de datos de RACADM.

3 En el iDRAC de destino, utilice el siguiente comando para modificar la configuración:

```
racadm set -f <file_name>.xml -t xml
```

De este modo, la información se carga en la otra iDRAC. Puede utilizar el comando **set** para sincronizar la base de datos de usuarios y contraseñas con Server Administrator.

4 Reinicie la iDRAC de destino con el comando: `racadm racreset`.

Desactivación del acceso para modificar los valores de configuración de iDRAC en el sistema host

Puede desactivar el acceso para modificar la configuración de iDRAC a través de la utilidad de configuración de iDRAC o RACADM local. No obstante, puede ver estos valores de configuración. Para hacerlo:

1 En la interfaz web de iDRAC, vaya a **iDRAC Settings (Configuración de iDRAC)** > **Services (Servicios)** > **Local Configurations (Configuraciones locales)**.

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 iDRAC. Sin embargo, podrá utilizar IPMI en la LAN.

5

Visualización de la información de iDRAC y el sistema administrado

Es posible ver la condición y las propiedades de iDRAC y del sistema administrado, su inventario de hardware y firmware, la condición de los sensores, los dispositivos de almacenamiento y los dispositivos de red, así como ver y terminar las sesiones de usuario. En el caso de los servidores blade, también podrá ver la información de dirección flexible.

Temas:

Visualización de la condición y las propiedades de Managed System

Cuando se inicia sesión en la interfaz web de iDRAC, la página **Resumen del sistema** permite ver la condición del sistema administrado, la información básica de iDRAC y la vista previa de la consola virtual. También permite agregar y ver notas de trabajo e iniciar rápidamente tareas como apagado o encendido, ciclo de encendido, ver registros, actualizar y revertir firmware, encender y apagar el LED en el panel anterior y restablecer iDRAC.

Para acceder a la página **System Summary (Resumen del sistema)**, vaya a **System (Sistema)** > **Overview (Descripción general)** > **Summary (Resumen)**. Aparece la página **Resumen del sistema**. Para obtener más información, consulte la *Ayuda en línea de iDRAC*.

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 **System Summary (Resumen del sistema)**. Se muestra la página **iDRAC Settings System Summary (Resumen del sistema de la configuración de iDRAC)**. Para obtener información, consulte la *Ayuda en línea de la utilidad de configuración de iDRAC*.

Visualización del inventario del sistema

Puede ver información sobre los componentes de firmware y hardware instalados en el sistema administrado. Para ello, en la interfaz web de iDRAC, vaya a **System (Sistema)** > **Inventories (Inventarios)**. Para obtener información acerca de las propiedades que se muestran, consulte la *Ayuda en línea de iDRAC*.

La sección Inventario de hardware muestra información sobre los siguientes componentes disponibles en el sistema administrado:

- iDRAC

- Controladora RAID
- Baterías
- CPU
- DIMM
- HDD
- Planos posteriores
- Tarjetas de interfaz de red (integradas e incorporadas)
- Tarjeta de vídeo
- Tarjeta SD
- Unidades de suministro de energía (PSU)
- Ventiladores
- HBA de Fibre Channel
- USB
- Dispositivos SSD PCIe

La sección Inventario de firmware muestra la versión de firmware de los siguientes componentes:

- BIOS
- Lifecycle Controller
- iDRAC
- Driver Pack del SO
- Diagnósticos de 32 bits
- Sistema CPLD
- Controladoras PERC
- Baterías
- Discos físicos
- Fuente de alimentación
- NIC
- Fibre Channel
- Plano posterior
- Gabinete
- Unidades SSD PCIe

NOTA: El inventario de software muestra solo los últimos 4 bytes de la versión del firmware. Por ejemplo, si la versión del firmware es FLVDL06, el inventario del firmware muestra DL06.

NOTA: En los servidores Dell PowerEdge FX2/FX2S, la convención de nomenclatura de la versión de la CMC que se muestra en la interfaz gráfica de usuario de iDRAC es diferente de la versión que se muestra en la interfaz gráfica de usuario de CMC. Sin embargo, la versión sigue siendo la misma.

Si reemplaza algún componente de hardware o actualiza las versiones de firmware, asegúrese de activar y ejecutar la opción **Collect System Inventory on Reboot (Recopilar inventario del sistema al reiniciar)** (CSIOR) para recopilar el inventario del sistema al reiniciar. Después de unos minutos, inicie sesión en iDRAC y vaya a la página **System Inventory (Inventario del sistema)** para ver los detalles. Es posible que haya una demora de hasta 5 minutos para que la información esté disponible, según el hardware instalado en el servidor.

NOTA: La opción CSR está activada de forma predeterminada.

NOTA: Es posible que los cambios en la configuración y las actualizaciones de firmware que se realizan dentro del sistema operativo no se reflejen correctamente en el inventario hasta que realice un reinicio del servidor.

Haga clic en **Exportar** para exportar el inventario de hardware en formato XML y guárdelo en la ubicación que desee.

Visualización de la información del sensor

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

- **Baterías**: proporciona información acerca de las baterías del CMOS en la placa del sistema y del RAID de almacenamiento en la placa base (ROMB).

  NOTA: La configuración de las baterías de ROMB de almacenamiento solo se encuentra disponible si el sistema tiene ROMB con una batería.
- **Ventilador** (disponible solo para los servidores tipo bastidor y torre): proporciona información acerca de los ventiladores del sistema; la redundancia de ventiladores y la lista de ventiladores que muestra la velocidad de los ventiladores y los valores del umbral.
- **CPU**: indica la condición de las CPU en el sistema administrado. También informa la limitación automática del procesador y la falla predictiva.
- **Memoria**: indica la condición y el estado de los módulos de memoria doble en línea (DIMM) presentes en el sistema administrado.
- **Intrusión**: proporciona información sobre el chasis.
- **Suministros de energía** (disponible solo para los servidores tipo bastidor y torre): proporciona información acerca de los suministros de energía y el estado de redundancia del suministro de energía.

  NOTA: Si solo existe un suministro de energía en el sistema, la redundancia del mismo estará desactivada.
- **Medios flash extraíbles**: proporciona información acerca de los módulos SD internos; vFlash y módulo SD dual interno (IDSDM).
  - Cuando está activada la redundancia de IDSDM, se muestra el siguiente estado de sensor de IDSDM: el estado de la redundancia de IDSDM, IDSDM SD1, IDSDM SD2. Cuando la redundancia está desactivada, solo se muestra IDSDM SD1.
  - Si la redundancia de IDSDM está desactivada inicialmente cuando el sistema se enciende o después de restablecer el iDRAC, el estado del sensor IDSDM SD1 se muestra solo después de que se inserte una tarjeta.
  - Si está activada la redundancia de IDSDM con dos tarjetas SD presentes en el IDSDM y el estado de una tarjeta SD es en línea, mientras que el estado de la otra tarjeta es fuera de línea. Se requiere un reinicio del sistema para restaurar la redundancia entre las dos tarjetas SD en el IDSDM. Una vez restaurada la redundancia, el estado de ambas tarjetas SD en el IDSDM será en línea.
  - Durante la operación de regeneración para restaurar la redundancia entre dos tarjetas SD presentes en el IDSDM, el estado IDSDM no se muestra, ya que los sensores de IDSDM están apagados.

    NOTA: Si el sistema host se reinicia durante la operación de recreación, el sistema iDRAC no muestra la información de IDSDM. Para resolver esto, recree IDSDM nuevamente o restablezca el sistema iDRAC.
  - Los registros de sucesos de sistema (SEL) para una tarjeta SD protegida contra escritura o dañada en el módulo IDSDM no se repitan hasta que se borren. Para ello, se debe reemplazar la tarjeta SD con una tarjeta escribible o en buen estado, respectivamente.
- **Temperatura**: proporciona información acerca de la temperatura interna de la placa del sistema y la temperatura de expulsión (solo se aplica a servidores en rack). La sonda de temperatura indica si el estado de la sonda se encuentra dentro de los valores de umbral críticos y de advertencia.
- **Voltaje**: indica el estado y la lectura de los sensores de voltaje de los distintos componentes del sistema.

En la tabla siguiente, se proporciona información sobre la visualización de la información de los sensores mediante la interfaz web de iDRAC y RACADM. Para obtener información acerca de las propiedades que se muestran en la interfaz web, consulte *iDRAC Online Help (Ayuda en línea de iDRAC)*.

NOTA: En la página Descripción general de hardware se muestran solo los datos de los sensores presentes en su sistema.

Tabla 14. Información del sensor mediante la interfaz web y RACADM

Ver la información del sensor para	Mediante la interfaz web	Mediante RACADM
Baterías	**Dashboard (Panel)** > **System Health (Condición del sistema)** > **Batteries (Baterías)**	Utilice el comando **getsensorinfo**. Para suministros de energía, también puede usar el comando **System.Power.Supply** con el subcomando **get**.

Ver la información del sensor para	Mediante la interfaz web	Mediante RACADM
		Para obtener más información, consulte *iDRAC RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM de iDRAC), disponible en **dell.com/idracmanuals**.
Ventilador	**Dashboard (Panel)** > > **System Health (Condición del sistema)** > **Fans (Ventiladores)**	
CPU	**Dashboard (Panel)** > **System Health (Condición del sistema)** > **CPU**	
Memoria	**Dashboard (Panel)** > **System Health (Condición del sistema)** > **Memory (Memoria)**	
Intrusión	**Dashboard (Panel)** > **System Health (Condición del sistema)** > **Intrusion (Intrusión)**	
Sistemas de alimentación	> **Hardware** > **Power Supplies (Fuentes de alimentación)**	
Medios flash extraíbles	**Dashboard (Panel)** > **System Health (Condición del sistema)** > **Removable Flash Media (Medios flash extraíbles)**	
Temperatura	**Dashboard (Panel)** > **System Health (Condición del sistema)** > **Power/Thermal (Alimentación/Térmica)** > **Temperatures (Temperaturas)**	
Voltaje	**Dashboard (Panel)** > **System Health (Condición del sistema)** > **Power/Thermal (Alimentación/Térmica)** > **Voltages (Voltajes)**	

Supervisión del índice de rendimiento de CPU, memoria y módulos de E/S

En los servidores Dell PowerEdge de 14.ª generación, Intel ME admite la funcionalidad de cómputo de uso por segundo (CUPS). La funcionalidad CUPS proporciona supervisión en tiempo real de la CPU, la memoria y utilización de E/S, y el índice de utilización de nivel del sistema para el sistema. Intel ME permite la supervisión de rendimiento fuera de banda (OOB) y no consume recursos de la CPU. Intel ME tiene un sensor de CUPS del sistema que proporciona los valores de cálculo, memoria y utilización de recursos de E/S como un índice CUPS. La iDRAC supervisa este índice CUPS para comprobar la utilización del sistema en general y también supervisa el índice de utilización instantánea de CPU, memoria y E/S.

NOTA: Esta función no se admite en los servidores PowerEdge R930.

La CPU y el conjunto de chips tienen contadores de supervisión de recursos (RMC) dedicados. Los datos de esos RMC se consultan para obtener información sobre la utilización de los recursos del sistema. El administrador de nodos combina los datos de los RMC para medir la utilización acumulada de cada uno de estos recursos del sistema que se leen de iDRAC mediante mecanismos de intercomunicación existentes para proporcionar datos a través las interfaces de administración fuera de banda.

La representación de los sensores Intel de los parámetros de rendimiento y los valores de índice es para el sistema físico completo. Por lo tanto, la representación de los datos de rendimiento en las interfaces es para el sistema físico completo, aunque el sistema se haya virtualizado y tenga varios hosts virtuales.

Para mostrar los parámetros de rendimiento, los sensores admitidos deben estar presentes en el servidor.

Los cuatro parámetros de utilización del sistema son:

- **CPU Utilization (Utilización de la CPU)**: los datos de los RMC para cada núcleo de CPU se combinan para proporcionar la utilización acumulada de todos los núcleos en el sistema. Esta utilización se basa en el tiempo transcurrido en estados activos e inactivos. Se toma una muestra de RMC cada seis segundos.
- **Memory Utilization (Utilización de memoria)**: los RMC miden el tráfico de memoria que se produce en cada canal de memoria o instancia de la controladora de memoria. Los datos de estos RMC se combinan para medir el tráfico de memoria acumulativo a través de todos los canales de memoria del sistema. Esta es la de medida de consumo de ancho de banda de la memoria, y no la cantidad de utilización de memoria. La iDRAC combina esto por un minuto, por lo que es posible que coincida o no con la utilización de memoria que muestran otras herramientas del sistema operativo, como **Top** en Linux. La utilización del ancho de banda de la memoria que muestra la iDRAC es una indicación si la carga de trabajo de la memoria es intensiva o no.
- **I/O Utilization (Utilización de E/S)**: existe un RMC por cada puerto raíz en el complejo raíz de PCI Express para medir el tráfico de PCI Express que se emite desde o se dirige hacia ese puerto raíz y el segmento inferior. Los datos de estos RMC se combinan para medir el tráfico de PCI Express para todos los segmentos de PCI Express que se emiten desde el paquete. Esta es la de medida de la utilización del ancho de banda de E/S para el sistema.
- **System Level CUPS Index (Índice CUPS de nivel del sistema)**: el índice CUPS se calcula al combinar índice de E/S, memoria y CPU considerando un factor de carga predefinido de cada recurso del sistema. El factor de carga depende de la naturaleza de la carga de trabajo en el sistema. El índice CUPS representa la medición de la capacidad de aumento para cómputo disponible en el servidor. Si el sistema presenta un índice CUPS alto, habrá una capacidad de aumento limitada para colocar más carga de trabajo en ese sistema. A medida que el consumo de recursos disminuye, también disminuye el índice CUPS del sistema. Un índice CUPS bajo indica que existe una gran capacidad de aumento para cómputo y el servidor puede recibir nuevas cargas de trabajo y el servidor se encuentra en un estado de bajo consumo para reducir el consumo de alimentación. La supervisión de la carga de trabajo se puede aplicar a todo el centro de datos a fin de proporcionar una vista integral de alto nivel de la carga de trabajo en el centro de datos, lo que ofrece una solución dinámica para el centro de datos.

NOTA: Los índices de utilización E/S, memoria y CPU se combinan a cada minuto. Por lo tanto, si se produce algún pico instantáneo en estos índices, es posible suprimirlos. Indican los patrones de carga de trabajo, no la cantidad de utilización de recursos.

Se generan alertas IPMI, SEL y SNMP si se alcanzan los umbrales de los índices de utilización y se activan los sucesos de sensor. Los indicadores de sucesos de sensor se encuentran desactivados de manera predeterminada. Se pueden activar mediante la interfaz de IPMI estándar.

Los privilegios requeridos son:

- Se requiere el privilegio de inicio de sesión para supervisar los datos de rendimiento.
- Se requiere el privilegio de configuración para establecer los umbrales de advertencia y restablecer los picos históricos.
- Se requieren el privilegio de inicio de sesión y una licencia Enterprise para leer los datos estadísticos históricos.

Supervisión del índice de rendimiento de CPU, memoria y módulos de E/S mediante la interfaz web

Para supervisar el índice de rendimiento de CPU, memoria y módulos de E/S, en la interfaz web de iDRAC, vaya a **System (Sistema)** > **Performance (Rendimiento)**.

- Sección **Rendimiento del sistema**: se muestra la lectura actual y la lectura de advertencia para el índice de utilización de la CPU, la memoria y los módulos de E/S, así como el índice CUPS en el nivel del sistema en una vista gráfica.
- Sección **Datos históricos de rendimiento del sistema**:
  - Proporciona las estadísticas para CPU, memoria, utilización de E/S e índice CUPS de nivel del sistema. Si el sistema host está apagado, en el gráfico, se muestra la línea de apagado por debajo del 0 %.
  - Es posible restablecer la utilización pico para un determinado sensor. Haga clic en **Reset Historical Peak (Restablecer pico histórico)**. Debe tener el privilegio de configuración para restablecer el valor pico.
- Sección **Métricas de rendimiento**:
  - Muestra el estado y la lectura presente.
  - Muestra o especifica el límite de utilización del umbral de aviso. Debe tener el privilegio de configuración de servidores para establecer los valores de umbral.

Para obtener información acerca de las propiedades que se muestran, consulte la *Ayuda en línea de iDRAC*.

Supervisión del índice de rendimiento de CPU, memoria y módulos de E/S mediante RACADM

Utilice el subcomando **SystemPerfStatistics** para supervisar el índice de rendimiento de la CPU, la memoria y los módulos de E/S. Para obtener más información, consulte *iDRAC RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de iDRAC)* disponible en **dell.com/esmmanuals**.

Consulta del sistema para verificar el cumplimiento de aire fresco

La refrigeración de aire fresco utiliza directamente el aire exterior para enfriar los sistemas del centro de datos. Los sistemas que cumplen con el requisito de aire fresco pueden funcionar por encima de su rango de funcionamiento ambiente normal (temperaturas de hasta 113 °F [45 °C]).

NOTA: Algunos servidores o ciertas configuraciones de un servidor pueden no cumplir con el requisito de aire fresco. Consulte el manual del servidor específico para obtener detalles relacionados con el cumplimiento del requisito de aire fresco o póngase en contacto con Dell para obtener más detalles.

Para consultar el sistema para verificar el cumplimiento de aire fresco, realice lo siguiente:

1 En la interfaz web de iDRAC, vaya a **System (Sistema)** > **Overview (Descripción general)** > **Cooling (Refrigeración)** > **Temperature overview (Descripción general de temperaturas)**.

Aparecerá la página **Temperature overview (Descripción general de temperaturas)**.

2 Consulte la sección **Aire fresco** que indica si el servidor cumple o no con el requisito de aire fresco.

Visualización de los datos históricos de temperatura

Es posible supervisar el porcentaje de tiempo en que el sistema ha funcionado a una temperatura ambiente mayor que el umbral de temperatura de aire fresco admitido normalmente. La lectura del sensor de temperatura de la placa del sistema se obtiene al cabo de un período para supervisar la temperatura. La recopilación de datos comienza cuando el sistema se enciende por primera vez o después del envío de fábrica. Los datos se recopilan y muestran durante el tiempo en que el sistema está encendido. Se puede realizar un seguimiento y almacenar la temperatura que se supervisó en los últimos siete años.

NOTA: Puede realizar un seguimiento del historial de temperatura incluso para sistemas que no cumplen con el requisito de aire fresco. Sin embargo, los límites de umbral y las advertencias relacionadas con aire fresco que se generan se basan en los límites de aire fresco admitidos. Los límites son 42 °C para el umbral de advertencia y 47 °C para el umbral crítico. Estos valores corresponden a los límites de 40 °C y 45 °C para aire fresco con un margen de 2 °C para garantizar su precisión.

Se realiza un seguimiento de dos bandas de temperatura fijas asociadas a los límites de aire fresco:

- Banda de advertencia: consta de la duración en la que un sistema ha funcionado por encima del umbral de advertencia del sensor de temperatura (42 °C). El sistema puede funcionar en la banda de advertencia durante el 10 % del tiempo por 12 meses.
- Banda crítica: consta de la duración en la que un sistema ha funcionado por encima del umbral crítico del sensor de temperatura (47 °C). El sistema puede funcionar en la banda crítica durante el 1 % del tiempo por 12 meses, lo que también incrementa el tiempo en la banda de advertencia.

Los datos recopilados se representan en un gráfico para realizar un seguimiento de los niveles del 10 % y del 1 %. Los datos de temperatura registrados se pueden borrar solamente antes de que salga de fábrica.

Se genera un suceso si el sistema continúa funcionando por encima del umbral de temperatura normalmente admitido para un tiempo de funcionamiento especificado. Si la temperatura promedio durante el tiempo de funcionamiento especificado, es mayor o igual al nivel de aviso (> = 8 %) o al nivel crítico (> = 0,8 %), se registra un suceso en el registro de Lifecycle y se genera la correspondiente captura SNMP. Los sucesos son:

- Suceso de advertencia cuando la temperatura fue mayor que el umbral de advertencia por una duración del 8 % o más en los últimos 12 meses.
- Suceso crítico cuando la temperatura fue mayor que el umbral de advertencia por una duración del 10 % o más en los últimos 12 meses.
- Suceso de advertencia cuando la temperatura fue mayor que el umbral crítico por una duración del 0,8 % o más en los últimos 12 meses.
- Suceso crítico cuando la temperatura fue mayor que el umbral crítico por una duración del 1 % o más en los últimos 12 meses.

Además, puede configurar iDRAC para que genere sucesos adicionales. Para obtener más información, consulte la sección Configuración de suceso de periodicidad de alertas.

Visualización de los datos históricos de temperatura mediante la interfaz web de iDRAC

Para ver los datos históricos de temperatura:

1 En la interfaz web de iDRAC, vaya a **System (Sistema)** > **Overview (Descripción general)** > **Cooling (Refrigeración)** > **Temperature overview (Descripción general de temperaturas)**.

Aparecerá la página **Temperature overview (Descripción general de temperaturas)**.

2 Consulte la sección **Datos históricos de temperatura de la placa del sistema** donde se muestra un gráfico de la temperatura almacenada (valores promedio y pico) correspondientes al último día, a los últimos 30 días y al año anterior.

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

NOTA: Después de una actualización del firmware de iDRAC o de reiniciar iDRAC, es posible que algunos datos de temperatura no se muestren en el gráfico.

Visualización de datos históricos de temperatura mediante RACADM

Para ver los datos históricos mediante RACADM, utilice el comando **inlettemphistory**.

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

Configuración del umbral de advertencia para la temperatura de entrada

Es posible modificar los valores mínimo y máximo del umbral de advertencia para el sensor de temperatura de entrada de la placa del sistema. Si se realiza una acción para restablecer los valores predeterminados, los umbrales de temperatura se establecen en los valores predeterminados. Debe tener el privilegio de configuración de usuarios para establecer los valores de umbral de advertencia para el sensor de temperatura interna.

Configuración del umbral de advertencia para la temperatura de entrada mediante la interfaz web

Para configurar el umbral de advertencia para la temperatura de entrada:

1 En la interfaz web de iDRAC, vaya a **System (Sistema)** > **Overview (Descripción general)** > **Cooling (Refrigeración)** > **Temperature overview (Descripción general de temperaturas)**.

Aparecerá la página **Temperature overview (Descripción general de temperaturas)**.

2 En la sección **Temperature Probes (Sondas de temperatura)**, para la opción **System Board Inlet Temp (Temperatura de entrada de la placa del sistema)**, introduzca los valores mínimo y máximo para **Warning Threshold (Umbral de advertencia)** en grados Celsius o Fahrenheit. Si introduce el valor en grados Celsius, el sistema calculará y mostrará automáticamente el valor en grados Fahrenheit. De la misma manera, si introduce el valor en grados Fahrenheit, se mostrará el valor en grados Celsius.

3 Haga clic en **Aplicar**.

Se configuran los valores.

NOTA: Los cambios realizados en los umbrales predeterminados no se reflejan en el gráfico de datos históricos, ya que los límites en el gráfico corresponden solamente a valores de límite de aire fresco. Las advertencias por exceder los umbrales personalizados son diferentes a las advertencias relacionadas con exceder los umbrales de aire fresco.

Visualización de interfaces de red disponibles en el sistema operativo host

Puede ver información acerca de todas las interfaces de red que están disponibles en el sistema operativo host como, por ejemplo, las direcciones IP que están asignadas al servidor. El Módulo de servicio de iDRAC proporciona estos datos a iDRAC. La información de dirección IP del sistema operativo incluye las direcciones IPv4 e IPv6, la dirección MAC, la longitud del prefijo o la máscara de subred, el FQDD del dispositivo de red, el nombre de la interfaz de red interfaz, la descripción de la interfaz de red, el estado de la interfaz de red, el tipo interfaz de red (Ethernet, túnel, bucle invertido, etc.), dirección de puerta de enlace, dirección de servidor DNS y dirección de servidor DHCP.

NOTA: Esta función está disponible con las licencias iDRAC Express y Enterprise.

Para ver la información del sistema operativo, asegúrese de que:

- Tiene privilegios de inicio de sesión.
- El módulo de servicio de iDRAC se ha instalado y se ejecuta en el sistema operativo host.
- La opción OS Information (Información de sistema operativo) se encuentra activada en la página **iDRAC Settings (Configuración de iDRAC)** > **Overview (Descripción general)** > **iDRAC Service Module (Módulo de servicio de iDRAC)**.

iDRAC puede mostrar las direcciones IPv4 e IPv6 para todas las interfaces configuradas en el sistema operativo host.

Según la forma en que el sistema operativo host detecta el servidor de DHCP, es posible que las direcciones IPv4 o IPv6 del servidor DHCP correspondiente no aparezcan.

Visualización de interfaces de red disponibles en el sistema operativo host mediante la interfaz web

Para ver las interfaces de red disponibles en el sistema operativo host mediante la interfaz web:

1 Vaya a **System (Sistema)** > **Host OS (SO host)** > **Network Interfaces (Interfaces de red)**.

La página **Interfaces de red** muestra todas las interfaces de red que se encuentran disponibles en el sistema operativo host.

2 Para ver la lista de interfaces de red asociadas con un dispositivo de red, en el menú desplegable **FQDD de dispositivo de red**, seleccione un dispositivo de red y, a continuación, haga clic en **Aplicar**.

Los detalles de IP para el sistema operativo se mostrarán en la sección **Interfaces de red para sistema operativo host**.

3 En la columna **FQDD de dispositivo**, haga clic en el vínculo para el dispositivo de red.

Se mostrará la página para el dispositivo correspondiente en la sección **Hardware** > **Network Devices (Dispositivos de red)**, donde se pueden ver los detalles del dispositivo. Para obtener información sobre las propiedades, consulte *iDRAC Online Help (Ayuda en línea de iDRAC)*.

4 Haga clic en el icono  para mostrar más detalles.

De forma similar, se puede ver la información de interfaces de red para el sistema operativo host asociado con un dispositivo de red en la página **Hardware** > **Network Devices (Dispositivos de red)**. Haga clic en **View Host OS Network Interfaces (Ver interfaces de red del sistema operativo host)**.

NOTA: Para el sistema operativo host ESXi en el módulo de servicio de iDRAC v2.3.0 o posterior, la columna Descripción de la lista Detalles adicionales se muestra en el siguiente formato:

```
<List-of-Uplinks-Configured-on-the-vSwitch>/<Port-Group>/<Interface-name>
```

Visualización de interfaces de red disponibles en el sistema operativo host mediante RACADM

Utilice el comando **gethostnetworkinterfaces** para ver las interfaces de red disponibles en los sistemas operativos host con RACADM. Para obtener más información, consulte *iDRAC RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de iDRAC)* disponible en **dell.com/esmmanuals**.

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

En los servidores Blade, FlexAddress permite el uso de nombres de red mundial y direcciones MAC (WWN/MAC) persistentes con chasis asignado para cada conexión de puerto de servidor administrada.

Puede ver la información siguiente para cada puerto de tarjeta Ethernet incorporada y tarjeta mezzanine opcional instalada:

- Redes Fabric a las que están conectadas las tarjetas
- Tipo de red Fabric.
- Direcciones MAC asignadas por el servidor, asignadas por el chasis o asignadas de manera remota.

Para ver la información de la dirección flexible en iDRAC, configure y active la función Flex Address (Dirección flexible) en Chassis Management Controller (CMC). Para obtener más información, consulte *Dell Chassis Management Controller User Guide (Guía del usuario de Chassis Management Controller)*, disponible en **dell.com/support/manuals**. Cualquier sesión existente de la consola virtual o de los medios virtuales finalizará si se activa o desactiva la configuración de la dirección flexible.

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 Flex Address (Dirección flexible) reemplaza las direcciones MAC asignadas por el servidor por las direcciones MAC asignadas por el chasis y se implementa para iDRAC junto con LOM de servidores blade, tarjetas mezzanine y módulos de E/S. La función Flex Address (Dirección flexible) de iDRAC admite la conservación de una dirección MAC específica de ranura para iDRAC en un chasis. La dirección MAC asignada por el chasis se almacena en la memoria no volátil de CMC y se envía a iDRAC durante un inicio de iDRAC o cuando se activa la dirección flexible de CMC.

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

- **System (Sistema)** > **Details (Detalles)** > **iDRAC Details (Detalles de iDRAC)**.
- **System (Sistema)** > **Server (Servidor)** > **WWN/MAC**.
- **iDRAC Settings (Configuración de iDRAC)** > **Overview (Descripción general)** > **Current Network Settings (Configuración de red actual)**.

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

Visualización o terminación de sesiones iDRAC

Es posible ver el número de usuarios actualmente conectados en iDRAC y terminar las sesiones de usuario.

Terminación de las sesiones de iDRAC mediante la interfaz web

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

Para ver y terminar las sesiones iDRAC:

1 En la interfaz web de iDRAC, vaya a **iDRAC Settings (Configuración de iDRAC)** > **Users (Usuarios)** > **Sessions (Sesiones)**.

En la página **Sessions (Sesiones)**, se muestra la Id. de sesión, el nombre de usuario, la dirección IP y el tipo de sesión. Para obtener más información sobre estas propiedades, consulte *iDRAC Online Help (Ayuda en línea de iDRAC)*.

2 Para terminar la sesión, en la columna **Terminar**, haga clic en el icono de papelera de reciclaje de una sesión.

Terminación de las sesiones de iDRAC mediante RACADM

Es necesario disponer de privilegios de administrador para terminar las sesiones iDRAC mediante RACADM.

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

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

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

6

Configuración de la comunicación de iDRAC

Es posible comunicarse con iDRAC mediante cualquiera de los modos siguientes:

- Interfaz web del iDRAC
- Conexión serie mediante un cable DB9 (comunicación en serie RAC o comunicación en serie IPMI): solo para servidores tipo bastidor y torre
- Comunicación en serie IPMI en la LAN
- IPMI en la LAN
- RACADM remoto
- RACADM local
- Servicios remotos

NOTA: Para garantizar que los comandos de importación o exportación de RACADM local funcionen correctamente, asegúrese de que el host de almacenamiento masivo USB esté activado en el sistema operativo. Para obtener información acerca de cómo activar el host de almacenamiento USB, consulte la documentación de su sistema operativo.

La siguiente tabla proporciona una descripción general de los protocolos y de los comandos compatibles y de los requisitos previos:

Tabla 15. Modos de comunicación: resumen

Modos de comunicación	Protocolo compatible	Comandos admitidos	Requisito previo
Interfaz web del iDRAC	Protocolo de Internet (https)	N/A	Servidor web
Comunicación en serie mediante un cable DB9 de módem nulo	Protocolo de comunicación en serie	RACADM	Parte del firmware iDRAC
		SMCLP	Comunicación en serie RAC o IPMI activada
		IPMI	
Comunicación en serie IPMI en la LAN	Protocolo de bus de administración de plataforma inteligente	IPMI	IPMITool se instala y la Comunicación en serie IPMI en la LAN está activada
	SSH		
	Telnet		
IPMI en la LAN	Protocolo de bus de administración de plataforma inteligente	IPMI	IPMITool se instala y la configuración IPMI se activa
SMCLP	SSH	SMCLP	SSH o Telnet en iDRAC se activa
	Telnet		
RACADM remoto	HTTPS	RACADM remoto	RACADM remoto se instala y activa
Firmware RACADM	SSH	Firmware RACADM	Firmware RACADM se instala y se activa.
	Telnet		

Modos de comunicación	Protocolo compatible	Comandos admitidos	Requisito previo
RACADM local	IPMI	RACADM local	Local RACADM se instala
Servicios remotos [1]	WSMan	WinRM (Windows) OpenWSMan (Linux)	Se instala WinRM (Windows) o se instala OpenWSMan (Linux).
	Redfish	Diversos complementos del navegador, CURL (Windows y Linux), solicitud de Python y módulos de JSON	Los complementos, CURL, módulos de Python están instalados

[1] Para obtener más información, consulte *Lifecycle Controller Remote Services User's Guide* (Guía del usuario de Lifecycle Controller Remote Services) disponible en **dell.com/idracmanuals.**

Temas:

Comunicación con iDRAC a través de una conexión serie mediante un cable DB9

Puede utilizar cualquiera de los métodos de comunicación para realizar tareas de administración del sistema a través de una conexión serie a servidores tipo bastidor y torre:

- Comunicación en serie RAC
- Comunicación en serie IPMI: modo básico de conexión directa y modo de terminal de conexión directa

NOTA: En el caso de los servidores blade, la conexión en serie se establece a través del chasis. Para obtener más información, consulte *Chassis Management Controller User's Guide* (Guía del usuario de Chassis Management Controller) disponible en dell.com/support/manuals.

Para establecer una conexión serie:

1. Configure el BIOS para activar la conexión en 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.

   NOTA: Se requiere un ciclo de apagado y encendido del servidor desde vConsole o la GUI para cualquier cambio en la velocidad en baudios.
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 encuentre el sistema administrado en el proceso de inicio, aparecerá la pantalla de POST o la pantalla del sistema operativo. Eso depende de la configuración: SAC para Windows y pantallas de modo de texto de Linux para Linux.

4 Active las conexiones RAC serie o IPMI serie en iDRAC.

Configuración del BIOS para la conexión serie

Para configurar el BIOS para la conexión serie:

NOTA: Esto es aplicable solamente para iDRAC en servidores tipo bastidor y torre.

1 Encienda o reinicie el sistema.
2 Presione F2.
3 Vaya a **Configuración del BIOS del sistema** > **Comunicación en serie**.
4 Seleccione **Conector serie externo** en **Dispositivo de acceso remoto**.
5 Haga clic en **Atrás**, en **Terminar** y, a continuación, en **Sí**.
6 Presione Esc para cerrar la **configuración del sistema**.

Activación de la conexión serie RAC

Después de configurar la conexión serie en el BIOS, active la comunicación en serie RAC en iDRAC.

NOTA: Esto es aplicable solamente para iDRAC en servidores tipo bastidor y torre.

Activación de la conexión serie RAC mediante la interfaz web

Para activar la conexión serie RAC:

1 En la interfaz web de iDRAC, vaya a **iDRAC Settings (Configuración de iDRAC)** > **Network (Red)** > **Serial (Comunicación en serie)**.
Se mostrará la página **Comunicación en serie**.
2 En **Comunicación en serie RAC**, seleccione **Activado** y especifique los valores de los atributos.
3 Haga clic en **Aplicar**.
Se habrán configurado los valores de la comunicación en serie RAC.

Activación de la conexión serie RAC mediante RACADM

Para activar la conexión en serie de RAC mediante RACADM, utilice el comando **set** con el objeto en el conjunto **iDRAC.Serial**.

Activación de los modos básicos y de terminal de la conexión serie básica IPMI

Para activar el enrutamiento de comunicación en serie IPMI del BIOS en iDRAC, configure la comunicación en serie IPMI en cualquiera de los modos siguientes en iDRAC:

NOTA: Esto es aplicable solamente para iDRAC en servidores tipo bastidor y torre.

- Modo básico de IPMI: admite una interfaz binaria para el acceso al programa, como el shell de IPMI (ipmish) que se incluye con la utilidad de administración de la placa base (BMU). Por ejemplo, para imprimir el registro de sucesos del sistema mediante ipmish a través del modo básico de IPMI, ejecute el siguiente comando:

```
ipmish -com 1 -baud 57600 -flow cts -u <username> -p <password> sel get
```

NOTA: El nombre de usuario y la contraseña predeterminados para iDRAC se proporcionan en el distintivo del sistema.

- Modo de terminal de IPMI: admite comandos ASCII que se envían desde un terminal de comunicación en serie. Este modo admite un número limitado de comandos (incluido el control de alimentación) y comandos IPMI sin formato que se escriben como caracteres ASCII hexadecimales. Esto permite ver las secuencias de inicio del sistema operativo hasta el BIOS, cuando se inicia sesión en iDRAC a través de SSH o Telnet. Deberá desconectarse del terminal de IPMI mediante **[sys pwd -x]**. A continuación, se muestran ejemplo de los comandos del modo de terminal de IPMI.
  - **[sys tmode]**
  - **[sys pwd -u root calvin]**
  - **[sys health query -v]**
  - **[18 00 01]**
  - **[sys pwd -x]**

Activación de la conexión serie mediante la interfaz web

Asegúrese de desactivar la interfaz serie RAC para activar la comunicación en serie IPMI.

Para configurar los valores de la comunicación en serie IPMI:

1. En la interfaz web de iDRAC, vaya a **iDRAC Settings (Configuración de iDRAC)** > **Connectivity (Conectividad)** > **Serial (Comunicación en serie)**.
2. En **IPMI Serial (Comunicación en serie de IPMI)**, especifique los valores de los atributos. Para obtener más información acerca de estas opciones, consulte la *Ayuda en línea de iDRAC*.
3. Haga clic en **Aplicar**.

Activación del modo de comunicación en serie de IPMI mediante RACADM

Para configurar el modo de IPMI, desactive la interfaz de serie RAC y, a continuación, active el modo de IPMI.

```
racadm set iDRAC.Serial.Enable 0
racadm set iDRAC.IPMISerial.ConnectionMode <n>
```

n=0: Modo de terminal

n=1: Modo básico

Activación de la configuración de la comunicación en serie de IPMI mediante RACADM

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

   ```
   racadm set iDRAC.Serial.Enable 0
   ```

2. Establezca la velocidad en baudios en serie de IPMI mediante el comando.

   ```
   racadm set iDRAC.IPMISerial.BaudRate <baud_rate>
   ```

Parámetro	Valores permitidos (en bps)
<baud_rate>	9600, 19200, 57600 y 115200.

3. Habilite el control de flujo de hardware en serie de IPMI mediante el comando.

   ```
   racadm set iDRAC.IPMISerial.FlowContro 1
   ```

4. Establezca el nivel de privilegio mínimo del canal en serie de IPMI mediante el comando.

   ```
   racadm set iDRAC.IPMISerial.ChanPrivLimit <level>
   ```

Parámetro	Nivel de privilegio
<level> = 2	Usuario
<level> = 3	Operador
<level> = 4	Administrador

5 Asegúrese de que el MUX en serie (conector en serie externo) se haya establecido correctamente en el dispositivo de acceso remoto en el programa de configuración del BIOS para configurar el BIOS para la conexión en serie.

Para obtener más información sobre estas propiedades, consulte la especificación IPMI 2.0.

Configuración adicional para el modo de terminal de la comunicación en serie IPMI

En esta sección se proporcionan valores de configuración adicionales para el modo de terminal de la comunicación en serie IPMI.

Configuración de valores adicionales para el modo de terminal de comunicación en serie IPMI mediante la interfaz web

Para configurar los valores del modo de terminal:

1 En la interfaz web de iDRAC, vaya a **iDRAC Settings (Configuración de iDRAC)** > **Connectivity (Conectividad)** > **Serial (Comunicación en serie)**.

Aparecerá la página **Comunicación en serie**.

2 Active la comunicación en serie IPMI.

3 Haga clic en **Configuración del modo de terminal**.

Se muestra la página **Configuración del modo de terminal**.

4 Especifique los valores siguientes:

- Edición de línea
- Control de eliminación
- Control del eco
- Control del protocolo de enlace
- Nueva secuencia de línea
- Entrada de nuevas secuencias de línea

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

5 Haga clic en **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, utilice el comando **set** con los objetos en el grupo **idrac.ipmiserial**.

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

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

iDRAC admite secuencias de tecla de escape que permiten cambiar entre una comunicación de interfaz en serie RAC y una consola de comunicación en serie en servidores tipo bastidor y torre.

Cambio de una consola de comunicación en serie a la comunicación en serie RAC

Para cambiar al modo de comunicación de interfaz en serie del RAC desde el modo de consola en serie, presione Esc+Mayúsc., 9.

Esta secuencia de teclas lo dirige a la indicación `iDRAC Login` (si iDRAC está configurada en el modo de 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 conexión en serie directa de IPMI.

Cambio de una comunicación en serie RAC a consola de comunicación en serie

Para cambiar al modo de consola en serie desde el modo de comunicación de interfaz en serie del RAC, presione Esc+Mayúsc., Q.

En modo de terminal, para cambiar la conexión al modo de consola en serie, presione Esc+Mayúsc., Q.

Para volver al uso de modo de terminal, cuando esté conectado en el modo de consola en serie, presione Esc+Mayúsc.,9.

Comunicación con iDRAC mediante IPMI SOL

La comunicación en serie IPMI en la LAN (SOL) permite el redireccionamiento de los datos de comunicación en serie de la consola basada en texto de un sistema administrado a través de la red de administración Ethernet fuera de banda (dedicada o compartida) de iDRAC. Con SOL, usted puede:

- Acceder a los sistemas operativos de manera remota sin tiempo de espera.
- Realizar diagnósticos de sistemas host en servicios de administración de emergencia (EMS) o en la consola administrativa especial (SAC) para un shell de Windows o Linux.
- Ver el progreso de los servidores durante POST y reconfigurar el programa de configuración del BIOS.

Para configurar el modo de comunicación SOL:

1 Configure el BIOS para la conexión serie.
2 Configure iDRAC para utilizar SOL.
3 Active un protocolo compatible (SSH, Telnet, IPMItool).

Configuración del BIOS para la conexión serie

NOTA: Esto es aplicable solamente para iDRAC en servidores tipo bastidor y torre.

1 Encienda o reinicie el sistema.
2 Presione F2.
3 Vaya a **Configuración del BIOS del sistema** > **Comunicación en serie**.
4 Especifique los valores siguientes:
   - Comunicación en serie: con Redirección de consola
   - Dirección de puerto serie: COM2.

     NOTA: Se puede configurar el campo de comunicación serie en Activado con redirección serie a través de com1 si dispositivo serie2 en el campo de dirección del puerto serie también está configurado en com1.
   - Conector serie externo: dispositivo serie2
   - Velocidad en baudios a prueba de fallas: 115200
   - Tipo de terminal remota: VT100/VT220
   - Redirección después de inicio: activado
5 Haga clic en **Atrás** y luego en **Terminar**.
6 Haga clic en **Sí** para guardar los cambios.
7 Presione <Esc> para salir de **Configuración del sistema**.

NOTA: El BIOS envía los datos de comunicación en serie de la pantalla en el formato 25 x 80. La ventana SSH que se utiliza para invocar el comando `console com2` debe estar configurada en el formato 25 x 80. De esta manera, la pantalla redirigida se mostrará correctamente.

NOTA: Si el cargador de inicio o el sistema operativo proporciona redirección serie como GRUB o Linux, la configuración Redirection After Boot (Redirección después de inicio) del BIOS debe estar desactivada. Esto es para evitar una posible condición de problema por el acceso de varios componentes al puerto serie.

Configuración de iDRAC para usar SOL

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

Configuración de iDRAC para usar SOL mediante la interfaz web iDRAC

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

1 En la interfaz web de iDRAC, vaya a **iDRAC Settings (Configuración de iDRAC)** > **Connectivity (Conectividad)** > **Serial Over LAN (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 habrán configurado los valores avanzados de IPMI SOL. Estos valores ayudan a mejorar el rendimiento.

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

Configuración de iDRAC para usar SOL mediante RACADM

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

1 Active serie IPMI en LAN mediante el comando.

```
racadm set iDRAC.IPMISol.Enable 1
```

2 Actualice el nivel mínimo de privilegio de SOL de IPMI con el comando.

```
racadm set iDRAC.IPMISol.MinPrivilege <level>
```

Parámetro	Nivel de privilegio
<level> = 2	Usuario
<level> = 3	Operador
<level> = 4	Administrador

NOTA: El nivel de privilegio mínimo de SOL de IPMI determina el privilegio mínimo para activar SOL de IPMI. Para obtener más información, consulte la especificación de IPMI 2.0.

3 Actualice la velocidad en baudios de SOL de IPMI con el comando.

```
racadm set iDRAC.IPMISol.BaudRate <baud_rate>
```

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.

Parámetro	Valores permitidos (en bps)
<baud_rate>	9600, 19200, 57600 y 115200.

4 Active SOL para cada usuario mediante el comando.

```
racadm set iDRAC.Users.<id>.SolEnable 2
```

Parámetro	Descripción
<id>	Identificación única del usuario

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

Activación del protocolo compatible

Los protocolos admitidos son IPMI, SSH y Telnet.

Activación del protocolo admitido mediante la interfaz web

Para activar SSH o Telnet, vaya a **iDRAC Settings (Configuración de iDRAC)** > **Services Servicios)** y seleccione **Enabled (Activado)** para SSH o Telnet, respectivamente.

Para activar IPMI, vaya a **iDRAC Settings (Configuración de iDRAC)** > **Connectivity (Conectividad)** y seleccione **IPMI Settings (Configuración de IPMI)**. Asegúrese de que el valor **Encryption Key (Clave de cifrado)** tenga todos ceros o presione la tecla de retroceso para borrar y cambiar el valor a caracteres NULOS.

Activación del protocolo admitido mediante RACADM

Para activar SSH o telnet, utilice los comandos siguientes:

- Telnet

  ```
  racadm set iDRAC.Telnet.Enable 1
  ```
- SSH

  ```
  racadm set iDRAC.SSH.Enable 1
  ```

  Para cambiar el puerto de SSH

  ```
  racadm set iDRAC.SSH.Port <port number>
  ```

Puede utilizar las herramientas siguientes:

- IPMItool para utilizar el protocolo IPMI
- Putty/OpenSSH para utilizar el protocolo SSH o Telnet

SOL mediante el protocolo IPMI

La utilidad SOL basada en IPMI/IPMItool utiliza RMCP+ que se entrega mediante datagramas UDP al puerto 623. RMCP+ proporciona opciones mejoradas de autenticación, verificaciones de integridad de datos, cifrado y capacidad para transportar varios tipos de cargas cuando se utiliza IPMI 2.0. Para obtener más información, vaya a **http://ipmitool.sourceforge.net/manpage.html**.

RMCP+ utiliza una clave de cifrado de cadena hexadecimal de 40 caracteres (0-9, a-f y A-F) para la autenticación. El valor predeterminado de una cadena es 40 ceros.

Una conexión RMCP+ a iDRAC debe cifrarse mediante la clave de cifrado (clave del generador de claves [KG]). Se puede configurar la clave de cifrado mediante la interfaz web de iDRAC o la utilidad de configuración de iDRAC.

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

NOTA: Si fuera necesario, puede cambiar el tiempo de espera de SOL predeterminado en iDRAC Settings (Configuración de iDRAC) > Services (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 indicador de comandos (Windows o Linux), ejecute el siguiente comando para iniciar SOL a través del iDRAC:

```
ipmitool -H <iDRAC-ip-address> -I lanplus -U <login name> -P <login password> sol activate
```

Este comando conectó la estación de administración al puerto en serie del sistema administrado.

3 Para salir de una sesión de SOL desde IPMItool, presione ~ y, a continuación, . (punto).

NOTA: Si una sesión SOL no termina, restablezca iDRAC y deje pasar al menos dos minutos para completar el inicio.

SOL mediante el protocolo SSH o Telnet

Shell seguro (SSH) y Telnet son protocolos de red que se usan para establecer comunicaciones de línea de comandos a la iDRAC. Es posible analizar comandos remotos RACADM y SMCLP a través de cualquiera de estas interfaces.

SSH ahora es más seguro que Telnet. La iDRAC solo admite la versión 2 de SSH con autentificación de contraseña y está activada de forma predeterminada. La iDRAC admite hasta dos sesiones de SSH y dos sesiones de Telnet a la vez. Es recomendable utilizar SSH, ya que Telnet no es un protocolo seguro. Debe usar Telnet solo si no puede instalar un cliente de SSH o si la infraestructura de la red es segura.

Para conectarse a iDRAC, utilice programas de código abierto, tal como PuTTY u OpenSSH que admitan los protocolos de red SSH y Telnet en una estación de administración.

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

Antes de utilizar SSH o Telnet para comunicarse con iDRAC, asegúrese de realizar lo siguiente:

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

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

La comunicación SOL basada en IPMI que utiliza protocolo de SSH o Telnet elimina la necesidad de una utilidad adicional, ya que la traducción de comunicación en serie a la red se realiza dentro de la iDRAC. La consola de Telnet o SSH que se utilice debe poder interpretar y responder a los datos provenientes del puerto serie del sistema administrado. El puerto serie normalmente se conecta a un shell que emula un terminal ANSI o VT100/VT220. La consola de comunicación en serie se redirige automáticamente a la consola de Telnet o SSH.

Uso de SOL desde PuTTY en Windows

NOTA: Si fuera necesario, puede cambiar el tiempo de espera de SSH o Telnet predeterminado en iDRAC Settings (Configuración de iDRAC) > Services (Servicios).

Para iniciar IPMI SOL desde PuTTY en una estación de trabajo de Windows:

1 Ejecute el siguiente comando para conectarse a iDRAC:

```
putty.exe [-ssh | -telnet] <login name>@<iDRAC-ip-address> <port number>
```

NOTA: El número de puerto es opcional. Solo se requiere cuando se reasigna el número de puerto.

2 Ejecute el comando `console com2` o `connect` para iniciar SOL e iniciar el sistema administrado.

Se abre una sesión de SOL de la estación de administración al sistema administrado mediante el protocolo de SSH o Telnet. Para acceder a la consola de línea de comandos de iDRAC, siga la secuencia de teclas de ESC. Comportamiento de conexión de PuTTY y SOL:

- 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 emergencias (EMS) inmediatamente después de un reinicio del host, es posible que se dañe el terminal de la consola de administración especial (SAC). Cierre la sesión de SOL, cierre el terminal, abra otro terminal e inicie la sesión de SOL con el mismo comando.

Uso de SOL desde OpenSSH o Telnet en Linux

Para iniciar SOL desde OpenSSH o Telnet en una estación de trabajo de Linux:

NOTA: Si fuera necesario, puede cambiar el tiempo de espera predeterminado de la sesión de SSH o Telnet en iDRAC Settings (Configuración de iDRAC) > Services (Servicios).

1 Inicie una ventana de shell.
2 Conéctese a iDRAC mediante el comando siguiente:
   - Para SSH: ssh *<iDRAC-ip-address>* -l *<login name>*
   - Para Telnet: telnet *<iDRAC-ip-address>*

NOTA: Si cambió el número predeterminado de puerto del servicio de Telnet (puerto 23), agregue el número de puerto al final del comando Telnet.

3 Introduzca uno de los comandos siguientes en el símbolo del sistema para iniciar SOL:
   - `connect`
   - `console com2`

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

La secuencia de escape también se imprime en la pantalla tan pronto se conecta la sesión de SOL. Cuando el sistema administrado está desactivado, lleva bastante tiempo establecer la sesión de SOL.

NOTA: Puede utilizar console com1 o console com2 para iniciar SOL. Reinicie el servidor para establecer la conexión.

El comando `console -h com2` muestra el contenido del búfer de historial de la conexión serie antes de esperar información proveniente del teclado o nuevos caracteres provenientes del puerto serie.

El tamaño predeterminado (y máximo) del búfer de historial es 8192 caracteres. Puede establecer este número en un valor menor con el comando:

```
racadm set iDRAC.Serial.HistorySize <number>
```

4 Cierre la sesión SOL para cerrar la sesión SOL activa.

Uso de la consola virtual de Telnet

Es posible que algunos clientes de Telnet en sistemas operativos Microsoft no muestren correctamente la pantalla de configuración del BIOS cuando la consola virtual del BIOS está configurada para la emulación de VT100/VT220. En este caso, cambie la consola del BIOS al modo ANSI para actualizar la pantalla. Para llevar a cabo este procedimiento en el menú de configuración del BIOS, seleccione **Virtual Console (Consola virtual)** > **Remote Terminal Type (Tipo de terminal remoto)** > **ANSI**.

Al configurar la ventana de emulación de cliente VT100, defina la ventana o la aplicación que está mostrando la consola virtual redirigida en 25 filas x 80 columnas para garantizar que el texto se muestre correctamente. De lo contrario, es posible que algunas pantallas de texto aparezcan ilegibles.

Para utilizar la consola virtual Telnet:

1 Active **Telnet** en **Servicios de componentes de Windows**.

2 Conéctese a iDRAC mediante el comando

```
telnet <IP address>:<port number>
```

Parámetro	Descripción
`<IP address>`	Dirección IP del iDRAC
`<port number>`	Número de puerto de telnet (si se está usando un puerto nuevo)

Configuración de la tecla de retroceso para la sesión de Telnet

Según el cliente de Telnet, la utilización de la tecla de retroceso puede producir resultados inesperados. Por ejemplo: la sesión puede generar eco de `^h`. Sin embargo, la mayoría de los clientes de Microsoft y Linux se pueden configurar para usar la tecla de retroceso.

Para configurar que la sesión de Telnet de Linux utilice la tecla de retroceso, abra un símbolo del sistema y escriba `stty erase ^h`. Cuando se le solicite, escriba `telnet`.

Para configurar los clientes de 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 de Telnet, escriba `telnet`. Si está ejecutando una sesión de Telnet, presione Ctrl+].

3 Cuando se le solicite, escriba `set bsasdel`.

Aparecerá el mensaje `Backspace will be sent as delete`.

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

Los comandos para desconectar una sesión de SOL dependen de la utilidad. Puede salir de la utilidad solamente cuando la sesión de SOL se haya terminado por completo.

Para desconectar una sesión de SOL, finalice la sesión de SOL desde la consola de línea de comandos de iDRAC.

- Para cerrar la redirección de SOL, presione Entrar, Esc, T.

Se cierra la sesión de SOL.

- Para salir de una sesión de SOL por medio de Telnet en Linux, presione y mantenga presionadas las teclas Ctrl+].
  Aparece una petición de Telnet. Escriba `quit` para salir de Telnet.

Si una sesión de SOL no se termina por completo en la utilidad, es posible que no haya otras sesiones de SOL disponibles. Para solucionar este problema, cierre la consola de línea de comandos en la interfaz web en **iDRAC Settings (Configuración de iDRAC)** > **Connectivity (Conectividad)** > **Serial Over LAN (Comunicación en serie en la LAN)**.

Comunicación con iDRAC mediante IPMI en la LAN

Debe configurar IPMI en la LAN para iDRAC con el fin de activar o desactivar los comandos IPMI en los canales LAN hacia cualquier sistema externo. Si no se configura IPMI en la LAN, los sistemas externos no podrán comunicarse con el servidor de iDRAC mediante comandos de IPMI.

NOTA: IPMI también admite el protocolo de direcciones IPv6 para los sistemas operativos basados en Linux.

Configuración de IPMI en la LAN mediante la interfaz web

Para configurar IPMI en la LAN:

1. En la interfaz web de iDRAC, vaya a **iDRAC Settings (Configuración de iDRAC)** > **Connectivity (Conectividad)**.
   Aparecerá la página **Red**.
2. En **Configuración de IPMI**, especifique los valores de los atributos y haga clic en **Aplicar**.
   Para obtener más información acerca de estas opciones, consulte la *Ayuda en línea de iDRAC*.

   Se habrán configurado los valores de IPMI en la LAN.

Configuración de IPMI en la LAN mediante la utilidad de configuración de iDRAC

Para configurar IPMI en la LAN:

1. En **Utilidad de configuración de iDRAC**, vaya a **Red**.
   Aparece la pantalla **Red de configuración de iDRAC**.
2. Para **Configuración de IPMI**, especifique los valores.
   Para obtener información acerca de las opciones, consulte la *Ayuda en línea de la utilidad de configuración de iDRAC*.
3. Haga clic en **Atrás**, en **Terminar** y, a continuación, en **Sí**.
   Se habrán configurado los valores de IPMI en la LAN.

Configuración de IPMI en la LAN mediante RACADM

1. Activar IPMI en LAN

```
racadm set iDRAC.IPMILan.Enable 1
```

   NOTA: Este valor determina los comandos IPMI que se ejecutan mediante la interfaz IPMI en la LAN. Para obtener más información, consulte las especificaciones de IPMI 2.0 en intel.com.

2. Actualice los privilegios del canal de IPMI.

```
racadm set iDRAC.IPMILan.PrivLimit <level>
```

Parámetro	Nivel de privilegio
<level> = 2	Usuario
<level> = 3	Operador
<level> = 4	Administrador

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

```
racadm set iDRAC.IPMILan.EncryptionKey <key>
```

Parámetro	Descripción
<key>	Clave de cifrado de 20 caracteres en un formato hexadecimal válido.

NOTA: La IPMI de iDRAC admite el protocolo RMCP+. Para obtener más información, consulte las especificaciones de IPMI 2.0 en intel.com.

Activación o desactivación de RACADM remoto

Puede activar o desactivar la RACADM remota mediante la interfaz web de iDRAC o RACADM. Puede ejecutar hasta cinco sesiones de RACADM remota simultáneamente.

NOTA: RACADM remoto está habilitado de forma predeterminada.

Activación o desactivación de RACADM remoto mediante la interfaz web

1 En la interfaz web de iDRAC, vaya a **iDRAC Settings (Configuración de iDRAC)** > **Services (Servicios)**.

2 En **RACADM remoto**, seleccione la opción que desee y haga clic en **Aplicar**.

RACADM remoto se activa o desactiva según la opción seleccionada.

Activación o desactivación de RACADM remoto mediante RACADM

NOTA: Se recomienda ejecutar estos comandos por medio de RACADM local o RACADM de firmware.

- Para desactivar RACADM remoto:

```
racadm set iDRAC.Racadm.Enable 0
```

- Para activar RACADM remoto:

```
racadm set iDRAC.Racadm.Enable 1
```

Desactivación de RACADM local

La RACADM local está activada de forma predeterminada. Para desactivarla, consulte Desactivación del acceso para modificar los valores de configuración de iDRAC en el sistema host.

Activación de IPMI en Managed System

En un sistema administrado, utilice Dell Open Manage Server Administrator para activar o desactivar IPMI. Para obtener más información, consulte *Dell OpenManage Server Administrator's User Guide (Guía del usuario de Dell OpenManage Server Administrator)*, disponible en **dell.com/support/manuals**.

NOTA: Desde iDRAC v2.30.30.30 o posterior, IPMI admite el protocolo de direcciones IPv6 para los sistemas operativos basados en Linux.

Configuración de Linux para la consola en serie durante el inicio

Los siguientes pasos son específicos de 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, inserte un comentario en la línea que comienza con `splashimage`.

En el ejemplo siguiente se proporciona un archivo **/etc/grub.conf** que muestra los cambios que se describen en este procedimiento.

```
# grub.conf generated by anaconda
# Note that you do not have to rerun grub after making changes to this file
# NOTICE: You do not have a /boot partition. This means that all
# kernel and initrd paths are relative to /, e.g.
# root (hd0,0)
# kernel /boot/vmlinuz-version ro root=/dev/sda1
# initrd /boot/initrd-version.img
#boot=/dev/sda
default=0
timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz

serial --unit=1 --speed=57600
terminal --timeout=10 serial

title Red Hat Linux Advanced Server (2.4.9-e.3smp) root (hd0,0)
kernel /boot/vmlinuz-2.4.9-e.3smp ro root=/dev/sda1 hda=ide-scsi console=ttyS0
console=ttyS1,115200n8r
initrd /boot/initrd-2.4.9-e.3smp.img
title Red Hat Linux Advanced Server-up (2.4.9-e.3) root (hd0,00)
kernel /boot/vmlinuz-2.4.9-e.3 ro root=/dev/sda1 s
initrd /boot/initrd-2.4.9-e.3.im
```

4 Para activar varias opciones de GRUB para iniciar sesiones en la consola virtual mediante la conexión serie del RAC, agregue la siguiente línea a todas las opciones:

```
console=ttyS1,115200n8r console=tty1
```

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

NOTA: Si el cargador de inicio o el sistema operativo proporciona redirección serie como GRUB o Linux, la configuración Redirection After Boot (Redirección después de inicio) del BIOS debe estar desactivada. Esto es para evitar una posible condición de problema por el acceso de varios componentes al puerto serie.

Activación del inicio de sesión en la consola virtual después del inicio

En el archivo **/etc/inittab**, agregue una línea nueva para configurar `agetty` en el puerto serie COM2:

```
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
```

El siguiente ejemplo muestra un archivo con la nueva línea.

```
#inittab This file describes how the INIT process should set up
#the system in a certain run-level.
#Author:Miquel van Smoorenburg
#Modified for RHS Linux by Marc Ewing and Donnie Barnes
#Default runlevel. The runlevels used by RHS are:
#0 - halt (Do NOT set initdefault to this)
#1 - Single user mode
#2 - Multiuser, without NFS (The same as 3, if you do not have #networking)
#3 - Full multiuser mode
#4 - unused
#5 - X11
#6 - reboot (Do NOT set initdefault to this)
id:3:initdefault:
#System initialization.
si::sysinit:/etc/rc.d/rc.sysinit
l0:0:wait:/etc/rc.d/rc 0
l1:1:wait:/etc/rc.d/rc 1
l2:2:wait:/etc/rc.d/rc 2
l3:3:wait:/etc/rc.d/rc 3
l4:4:wait:/etc/rc.d/rc 4
l5:5:wait:/etc/rc.d/rc 5
l6:6:wait:/etc/rc.d/rc 6
#Things to run in every runlevel.
ud::once:/sbin/update
ud::once:/sbin/update
#Trap CTRL-ALT-DELETE
ca::ctrlaltdel:/sbin/shutdown -t3 -r now
#When our UPS tells us power has failed, assume we have a few
#minutes of power left. Schedule a shutdown for 2 minutes from now.
#This does, of course, assume you have power installed and your
#UPS is connected and working correctly.
pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure; System Shutting Down"
#If power was restored before the shutdown kicked in, cancel it.
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored; Shutdown Cancelled"
```

```
#Run gettys in standard runlevels
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6

#Run xdm in runlevel 5
#xdm is now a separate service
x:5:respawn:/etc/X11/prefdm -nodaemon
```

En el archivo **/etc/securetty**, agregue una línea nueva con el nombre de la conexión tty serie para COM2:

```
ttyS1
```

El siguiente ejemplo muestra un archivo con la nueva línea.

NOTA: Utilice la secuencia de teclas de interrupción (~B) para ejecutar los comandos clave de Linux Magic SysRq en la consola de comunicación en serie utilizando la herramienta IPMI.

```
vc/1
vc/2
vc/3
vc/4
vc/5
vc/6
vc/7
vc/8
vc/9
vc/10
vc/11
tty1
tty2
tty3
tty4
tty5
tty6
tty7
tty8
tty9
tty10
tty11
ttyS1
```

Esquemas de criptografía SSH compatibles

Para comunicarse con el sistema iDRAC mediante el protocolo SSH, se admiten varios esquemas de criptografía que se enumeran en la tabla siguiente.

Tabla 16. Esquemas de criptografía SSH

Tipo de esquema	Algoritmos
Criptografía asimétrica	
Clave pública	ssh-rsa
	ecdsa-sha2-nistp256
Criptografía simétrica	
Intercambio de claves	curve25519-sha256@libssh.org
	ecdh-sha2-nistp256
	ecdh-sha2-nistp384
	ecdh-sha2-nistp521
	diffie-hellman-group-exchange-sha256
	diffie-hellman-group14-sha1
Cifrado	chacha20-poly1305@openssh.com
	aes128-ctr
	aes192-ctr

Tipo de esquema	Algoritmos
	aes256-ctr
	aes128-gcm@openssh.com
	aes256-gcm@openssh.com
MAC	hmac-sha1
	hmac-ripemd160
	umac-64@openssh.com
Compression	Ninguno

NOTA: Si activa OpenSSH 7.0 o posterior, se desactiva la compatibilidad con claves públicas DSA. Para garantizar una mayor seguridad para iDRAC, Dell recomienda no activar la compatibilidad con claves públicas DSA.

Uso de la autentificación de clave pública para SSH

La iDRAC admite la autentificación de clave pública (PKA) para SSH. Esta es una función con licencia. Cuando la PKA para SSH se configura y se utiliza correctamente, debe introducir el nombre de usuario al iniciar sesión en iDRAC. Esto es de utilidad a la hora de configurar scripts automatizados que realizan distintas funciones. Las claves cargadas deben tener el formato OpenSSH o RFC 4716. De lo contrario, deberá convertir las claves a ese formato.

En cualquier escenario, se debe generar un par de claves privada y pública en la estación de administración. La clave pública se carga en el usuario local de iDRAC y la clave privada la utiliza el cliente de SSH para establecer la relación de confianza entre la estación de administración y la iDRAC.

Puede generar el par de claves pública o privada mediante los elementos siguientes:

- La aplicación *Generador de clave PuTTY* para clientes que ejecutan Windows
- La CLI *ssh-keygen* para clientes que ejecutan Linux.

PRECAUCIÓN: Este privilegio normalmente se reserva para usuarios que son miembros del grupo de usuarios administradores de iDRAC. No obstante, se puede asignar este privilegio a los usuarios del grupo de usuarios "Custom (Personalizado)". Un usuario con este privilegio puede modificar la configuración de cualquier usuario. Esto incluye la creación o la eliminación de cualquier usuario, la administración de la clave SSH para usuarios, etc. Por estos motivos, asigne este privilegio con cuidado.

PRECAUCIÓN: La capacidad para cargar, ver o eliminar las claves SSH se basa en el privilegio de configuración de usuarios que tenga el usuario. Este privilegio permite a los usuarios configurar la clave SSH de otro usuario. 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 RSA para el tipo de clave.
2 Introduzca la cantidad de bits para la clave. El número de bits debe estar entre 2048 y 4096.
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 2048 -C testing`.

donde:

- `-t` es *rsa*.
- `-b` especifica el tamaño de cifrado de bits entre 2048 y 4096.
- `-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 mediante ssh-keygen tienen un formato distinto de 4716. Convierta las claves al formato 4716 mediante . `ssh-keygen -e -f /root/.ssh/id_rsa.pub > std_rsa.pub`. No cambie los permisos del archivo de clave. La conversión debe realizarse con los permisos predeterminados.

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

Carga de claves SSH

Puede cargar hasta cuatro claves públicas *por usuario* para utilizar en una interfaz SSH. Antes de agregar las claves públicas, asegúrese de visualizarlas para comprobar que estén configuradas, de modo que no se sobrescriban accidentalmente.

Al agregar claves públicas nuevas, asegúrese de que las claves existentes no se encuentran en el índice en que se agregará una clave nueva. La iDRAC no realiza ninguna comprobación para asegurarse de que las claves anteriores se eliminen antes de que se agregue una clave nueva. Cuando se agrega una clave nueva, se puede utilizar si la interfaz SSH está activada.

Carga de claves SSH mediante la interfaz web

Para cargar las claves SSH:

1. En la interfaz web de iDRAC, vaya a **iDRAC Settings (Configuración de iDRAC)** > **Users (Usuarios)** > **Local Users (Usuarios locales)**.
   Aparecerá la página **Usuarios locales**.
2. En la columna **Identificación de usuario**, haga clic en un número de identificación de usuario.
   Aparece la página **Menú principal de usuarios**.
3. En **Configuración de claves SSH**, seleccione **Cargar claves SSH** y haga clic en **Siguiente**.
   Aparece la página **Cargar claves SSH**.
4. Cargue las claves SSH de una de las maneras siguientes:
   - Cargue el archivo clave.
   - Copie del contenido del archivo de claves en el cuadro de texto

   Para obtener más información, consulte la Ayuda en línea de iDRAC.
5. Haga clic en **Aplicar**.

Carga de claves SSH mediante RACADM

Para cargar las claves SSH, ejecute el siguiente comando:

NOTA: No es posible cargar y copiar una clave al mismo tiempo.

- Para RACADM local: `racadm sshpkauth -i <2 to 16> -k <1 to 4> -f <filename>`
- Para RACADM remota con Telnet o SSH: `racadm sshpkauth -i <2 to 16> -k <1 to 4> -t <key-text>`

Por ejemplo, para cargar una clave válida al ID 2 de usuario de iDRAC en el primer espacio de clave mediante un archivo, ejecute el comando siguiente:

```
$ racadm sshpkauth -i 2 -k 1 -f pkkey.key
```

NOTA: La opción `-f` no se admite en RACADM Telnet/SSH/serie.

Visualización de claves SSH

Es posible ver las claves cargadas en iDRAC.

Visualización de claves SSH mediante la interfaz web

Para ver las claves SSH:

1. En la interfaz web, vaya a **iDRAC Settings (Configuración de iDRAC)** > **Users (Usuarios)**.
   Aparecerá la página **Usuarios locales**.
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.

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 **iDRAC Settings (Configuración de iDRAC)** > **Users (Usuarios)**.
   Aparecerá la página **Usuarios locales**.
2. En la columna **ID (Id.)**, seleccione un número de id. de usuario y haga clic en **Edit (Editar)**.
   Se muestra la página **Edit User (Editar usuario)**.
3. En **SSH Key Configurations (Configuración de claves SSH)**, seleccione una clave SSH y haga clic en **Edit (Editar)**.
   En la página **SSH Key (Clave SSH)**, se muestran detalles de **Edit From (Editar desde)**.
4. Seleccione la opción **Remove (Quitar)** para las claves que desea eliminar y haga clic en **Apply (Aplicar)**.
   Se eliminan las claves seleccionadas.

Eliminación de claves SSH mediante RACADM

Para eliminar las claves SSH, ejecute los comandos siguientes:

- Clave específica: `racadm sshpkauth -i <2 to 16> -d -k <1 to 4>`
- Todas las claves: `racadm sshpkauth -i <2 to 16> -d -k all`

7

Configuración de cuentas de usuario y privilegios

Puede configurar las cuentas de usuario con privilegios específicos (*autoridad basada en roles*) para administrar el sistema mediante iDRAC y mantener la seguridad del sistema. De forma predeterminada, iDRAC está configurado con una cuenta de administrador local. El nombre de usuario y la contraseña predeterminados para iDRAC se proporcionan con el distintivo del sistema. Como administrador, puede configurar cuentas de usuario para permitir que otros usuarios accedan a iDRAC. Para obtener más información, consulte la documentación del servidor.

Puede configurar usuarios locales o utilizar servicios de directorio como Microsoft Active Directory o LDAP para configurar cuentas de usuario. El uso de un servicio de directorio proporciona una ubicación central para administrar las cuentas de usuario autorizadas.

iDRAC admite el acceso basado en roles para usuarios con un conjunto de privilegios asociados. Los roles son: administrador, operador, solo lectura o ninguno. El rol define los privilegios máximos disponibles.

Temas:

Caracteres recomendados para nombres de usuario y contraseñas

Esta sección proporciona información sobre los caracteres recomendados para la creación y el uso de nombres de usuario y contraseñas.

Utilice los siguientes caracteres al crear nombres de usuario y contraseñas:

Tabla 17. Caracteres recomendados para los nombres de usuario

Caracteres	Longitud
0-9	1-16
A-Z	
a-z	
- ! # $ % & ( ) * / ; ? @ [\ ] ^ _ ` { | } ~ + < = >	

Tabla 18. Caracteres recomendados para las contraseñas

Caracteres	Longitud
0-9	1-20
A-Z	

Caracteres	Longitud
a-z	
' - ! " # $ % & ( ) * , . / : ; ? @ [\ ] ^ _ ` { | } ~ + < = >	

NOTA: Es posible que pueda crear nombres de usuario y contraseñas que incluyan otros caracteres. Sin embargo, para garantizar la compatibilidad con todas las interfaces, Dell recomienda utilizar únicamente los caracteres que se indican aquí.

NOTA: Los caracteres permitidos en los nombres de usuario y las contraseñas para recursos compartidos de red son determinados por el tipo de recurso compartido de red. La iDRAC admite caracteres válidos para las credenciales de recurso compartido de red según lo definido por el tipo de recurso compartido, excepto <, > y , (coma).

NOTA: Para mejorar la seguridad, se recomienda utilizar contraseñas complejas que tengan ocho caracteres o más e incluir letras minúsculas, letras mayúsculas, números y caracteres especiales. Además, se recomienda cambiar periódicamente las contraseñas, de ser posible.

Configuración de usuarios locales

Puede configurar hasta 16 usuarios locales en iDRAC con permisos de acceso específicos. Antes de crear un usuario de iDRAC, compruebe si existen usuarios actuales. Puede configurar nombres de usuario, contraseñas y roles con los privilegios para estos usuarios. Los nombres de usuario y las contraseñas se pueden cambiar mediante cualquiera de las interfaces seguras de iDRAC (es decir, la interfaz web, RACADM o WSMan). También puede activar o desactivar la autentificación de SNMPv3 para cada usuario.

Configuración de usuarios locales mediante la interfaz web de iDRAC

Para agregar y configurar usuarios de iDRAC locales:

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

1 En la interfaz web de iDRAC, vaya a **iDRAC Settings (Configuración de iDRAC)** > **Users (Usuarios)**.
Aparecerá la página **Usuarios locales**.

2 En la columna **ID (Id.)** del usuario, seleccione un número de id. de usuario y haga clic en **Edit (Editar)**.

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

Se muestra la página **User Configuration (Configuración de usuario)**.

3 Agregue los detalles de **User Account Settings (Configuración de la cuenta de usuario)** y **Advanced Settings (Configuración avanzada)** para configurar la cuenta de usuario.

NOTA: Active la id. de usuario y especifique el nombre de usuario, la contraseña y el rol de usuario (privilegios de acceso) para el usuario. También puede activar nivel de privilegio de LAN, el nivel de privilegio de puerto serie, el estado de comunicación en serie en la LAN, la autentificación de SNMPv3, el tipo de autenticación y el tipo de privacidad para el usuario. Para obtener más información sobre las opciones, consulte la *Ayuda en línea de iDRAC*.

4 Haga clic en **Save** (Guardar). El usuario se crea con los privilegios necesarios.

Configuración de los usuarios locales mediante RACADM

NOTA: Se debe haber iniciado sesión como usuario root para ejecutar los comandos de RACADM en un sistema remoto con Linux.

Puede configurar uno o varios usuarios de iDRAC mediante RACADM.

Para configurar varios usuarios de iDRAC una configuración idéntica, siga estos procedimientos:

- Use los ejemplos de RACADM de esta sección como guía para crear un archivo por lotes de comandos RACADM y después ejecute el archivo por lotes en cada sistema administrado.
- Cree el archivo de configuración de iDRAC y ejecute el comando **racadm set** en cada sistema administrado con el mismo archivo de configuración.

Si está configurando una nueva iDRAC o si ha usado el comando **racadm racresetcfg**, compruebe el nombre de usuario y la contraseña predeterminados para iDRAC en el distintivo del sistema. El subcomando **racadm racresetcfg** restablece iDRAC a los valores predeterminados.

NOTA: Los usuarios se pueden activar o desactivar con el transcurso del tiempo. Por este motivo, un usuario puede tener un número de índice diferente en cada iDRAC.

Para verificar si existe un usuario, escriba el siguiente comando una vez para cada índice (de 1 a 16):

```
racadm get iDRAC.Users.<index>.UserName
```

Varios parámetros e ID de objeto se muestran con sus valores actuales. El campo de clave es `iDRAC.Users.UserName=`. Si se muestra un nombre de usuario después del signo =, se toma ese número de índice.

NOTA: Puede utilizar

```
racadm get -f <myfile.cfg>
```

y ver o editar el archivo

```
myfile.cfg
```

que incluye todos los parámetros de configuración de iDRAC.

Para activar la autentificación de SNMPv3 para un usuario, use objetos **SNMPv3AuthenticationType**, **SNMPv3Enable** y **SNMPv3PrivacyType**. Para obtener más información, consulte *RACADM Command Line Interface Guide (Guía de la interfaz de línea de comandos RACADM)*, disponible en **dell.com/idracmanuals**.

Si está utilizando el archivo XML de configuración, utilice los atributos **AuthenticationProtocol**, **ProtocolEnable** y **PrivacyProtocol** para activar la autentificación de SNMPv3.

Cómo agregar un usuario iDRAC mediante RACADM

1 Establecer el índice y el nombre de usuario.

```
racadm set idrac.users.<index>.username <user_name>
```

Parámetro	Descripción
`<index>`	Índice único del usuario
`<user_name>`	Nombre de usuario

2 Establezca la contraseña.

```
racadm set idrac.users.<index>.password <password>
```

3 Establezca los privilegios de usuario.

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

4 Active el usuario.

```
racadm set.idrac.users.<index>.enable 1
```

Para verificar, use el siguiente comando:

```
racadm get idrac.users.<index>
```

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

Activación del usuario iDRAC con permisos

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

1 Busque un índice de usuario disponible.

```
racadm get iDRAC.Users <index>
```

2 Escriba los comandos siguientes con el nombre de usuario y la contraseñas nuevos.

```
racadm set iDRAC.Users.<index>.Privilege <user privilege bit mask value>
```

NOTA: El valor de privilegio predeterminado es 0, lo que indica que el usuario no tiene activado ningún privilegio. Para obtener una lista de los valores de máscara de bits válidos para los privilegios de usuario específicos, consulte *iDRAC RACADM Command Line Interface Reference Guide (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC)*, disponible en dell.com/idracmanuals.

Configuración de usuarios de Active Directory

Si la empresa utiliza el software Microsoft Active Directory, puede configurarlo para proporcionar acceso a iDRAC, lo que permite agregar y controlar los privilegios de usuario iDRAC para los usuarios existentes en el servicio de directorio. Esta es una función con licencia.

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

Puede configurar la autenticación de usuario a través de Active Directory para iniciar sesión en iDRAC. Además, puede proporcionar autoridad basada en roles, que permite que un administrador configure privilegios específicos para cada usuario.

El rol de iDRAC y los nombres de privilegio han cambiado desde la generación anterior de los servidores. Los nombres de funciones son:

Tabla 19. Roles de iDRAC

Generación actual	Generación anterior	Privileges (Privilegios)
Administrador	Administrador	Inicio de sesión, Configurar, Configurar usuarios, Registros, Control del sistema, Acceder a la consola virtual, Acceder a medios virtuales, Operaciones del sistema, Depuración
Operador	Usuario avanzado	Inicio de sesión, Configurar, Control del sistema, Acceder a la consola virtual, Acceder a medios virtuales, Operaciones del sistema, Depuración
Solo lectura	Usuario invitado	Inicio de sesión
Ninguno	Ninguno	Ninguno

Tabla 20. Privilegios del usuario del iDRAC

Generación actual	Generación anterior	Descripción
Inicio de sesión	Inicio de sesión en iDRAC	Permite al usuario iniciar sesión en el iDRAC.
Configurar	Configurar iDRAC	Permite al usuario configurar el iDRAC.
Configurar usuarios	Configurar usuarios	Permite activar la capacidad del usuario de otorgar permisos de acceso al sistema a usuarios específicos.

Generación actual	Generación anterior	Descripción
Registros	Borrar registros	Permite al usuario borrar el registro de sucesos del sistema (SEL).
Control del sistema	Ejecutar comandos de control del servidor	Permite ejecutar un ciclo de energía en el sistema host.
Acceder a la consola virtual	Redirección de acceso a la consola virtual (para servidores Blade)	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.
Operaciones del sistema	Probar alertas	Permite sucesos iniciados y generados por usuario. La información se envía como una notificación asincrónica y registrada.
Depuración	Ejecutar comandos de diagnóstico	Permite al usuario ejecutar comandos de diagnóstico.

Prerrequisitos del uso de la autentificación de Active Directory para iDRAC

Para utilizar la función de autentificación de Active Directory de iDRAC, asegúrese de haber realizado lo siguiente:

- La implementación de una infraestructura de Active Directory. Consulte el sitio web de Microsoft para obtener más información.
- La integración de PKI en la infraestructura de Active Directory. La iDRAC utiliza el mecanismo estándar de infraestructura de clave pública (PKI) para la autenticación segura en Active Directory. Consulte el sitio web de Microsoft para obtener más información.
- Activado Capa de sockets seguros (SSL) en todas las controladoras de dominio a las que se conecta iDRAC para la autentificación en todas las controladoras de dominio.

Activación de SSL en una controladora de dominio

Cuando iDRAC autentica los usuarios con una controladora de dominio de Active Directory, inicia una sesión SSL en la controladora de dominio. En este momento, la controladora de dominio debe publicar un certificado firmado por la autoridad de certificados (CA), el certificado raíz que también se carga en iDRAC. Para que iDRAC autentique *cualquier* controladora de dominio (ya sea la controladora de dominio raíz o la secundaria), dicha controladora de dominio debe tener un certificado habilitado para SSL firmado por la CA del dominio.

Si utiliza la CA raíz empresarial de Microsoft para asignar *automáticamente* todas las controladoras de dominio a un certificado SSL, deberá realizar lo siguiente:

1 Instalar el certificado SSL en cada controladora de dominio.
2 Exportar el certificado de CA raíz de la controladora de dominio a iDRAC.
3 Importar el certificado SSL del firmware de iDRAC.

Instalación de un certificado SSL para cada controladora de dominio

Para instalar el certificado SSL para cada controladora:

1 Haga clic en **Start (Inicio)** > **Administrative Tools (Herramientas administrativas)** > **Domain Security Policy (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 **Next (Siguiente)** y, después, en **Finish (Terminar)**. Se instala el certificado SSL.

Exportación de un certificado de CA raíz de la controladora de dominio a iDRAC

NOTA: Si el sistema ejecuta Windows 2000 o si está utilizando una CA independiente, los siguientes pasos pueden variar.

Para exportar el certificado de CA raíz de la controladora de dominio a iDRAC.

1 Localice la controladora de dominio que ejecuta el servicio de CA de Microsoft Enterprise.

2 Haga clic en **Inicio** > **Ejecutar**.

3 Introduzca `mmc` y haga clic en **OK (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 **Equipo** y haga clic en **Siguiente**.

8 Seleccione **Equipo local**, haga clic en **Terminar**, y a continuación haga clic en **Aceptar**.

9 En la ventana **Console 1 (Consola 1)**, vaya a **Certificates (Certificados)**, la carpeta **Personal Certificates (Certificados personales)**.

10 Localice el certificado de CA raíz y haga clic con el botón derecho del mouse sobre ese elemento. Seleccione **Todas las tareas** y haga clic en **Exportar...**.

11 En el **Asistente de exportación de certificados**, haga clic en **Siguiente** y seleccione **No exportar la clave privada**.

12 Haga clic en **Siguiente** y seleccione **Codificado en base 64 X.509 (.cer)** como el formato.

13 Haga clic en **Siguiente** y guarde el certificado en un directorio del sistema.

14 Cargue el certificado guardado en el paso 13 en iDRAC.

Importación del certificado SSL de firmware de iDRAC

El certificado SSL de iDRAC es el certificado idéntico que se utiliza para el servidor web de iDRAC. Todas las controladoras de iDRAC se entregan con un certificado autofirmado predeterminado.

Si el servidor de Active Directory no se configura para autenticar el cliente durante la fase de inicialización de una sesión de SSL, deberá cargar el certificado del servidor de iDRAC en la controladora de dominio de Active Directory. Este paso adicional no es necesario si Active Directory no realiza la autenticación de clientes durante la fase de inicialización de una sesión de SSL.

NOTA: Si el sistema ejecuta Windows 2000, los siguientes pasos pueden variar.

NOTA: Si el certificado SSL del firmware de iDRAC es firmado por una CA y el certificado de esta ya se encuentra en la lista Entidades emisoras raíz de confianza de la controladora de dominio, no realice los pasos que se describen en esta sección.

Para importar el certificado SSL del firmware iDRAC en todas las listas de certificado seguras de la controladora de dominio:

1 Descargue el certificado SSL de iDRAC mediante el comando RACADM siguiente:
```
racadm sslcertdownload -t 0x1 -f <RAC SSL certificate>
```
2 En la controladora de dominio, abra una ventana **Consola de MMC** y seleccione **Certificados** > **Autoridades de certificación de raíz confiables**.
3 Haga clic con el botón derecho del mouse en **Certificados**, seleccione **Todas las tareas** y haga clic en **Importar**.
4 Haga clic en **Siguiente** y desplácese al archivo de certificado SSL.
5 Instale el certificado SSL de iDRAC en la lista **Autoridades de certificación raíz de confianza** de cada controladora de dominio.
Si ha instalado su propio certificado, asegúrese de que la CA que firma el certificado esté en la lista **Trusted Root Certification Authority (Autoridad de certificación de 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 **Finish (Finalizar)** y, a continuación, en **OK (Aceptar)**. El certificado SSL del firmware de iDRAC se importa en todas las listas de certificados de confianza de la controladora de dominio.

Mecanismos de autentificación compatibles de Active Directory

Es posible utilizar Active Directory para definir el acceso de usuario a iDRAC mediante dos métodos:

- La solución del *esquema estándar*, que solo utiliza objetos de grupo de Active Directory.
- La solución de *esquema extendido*, que contiene objetos de Active Directory personalizados. Todos los objetos de control de acceso se mantienen en Active Directory. Esto proporciona una flexibilidad máxima a la hora de configurar el acceso de los usuarios en diferentes iDRAC con niveles de privilegios variados.

Descripción general del esquema estándar de Active Directory

Como se muestra en la figura a continuación, el uso del esquema estándar para la integración de Active Directory requiere la configuración tanto en Active Directory como en el iDRAC.

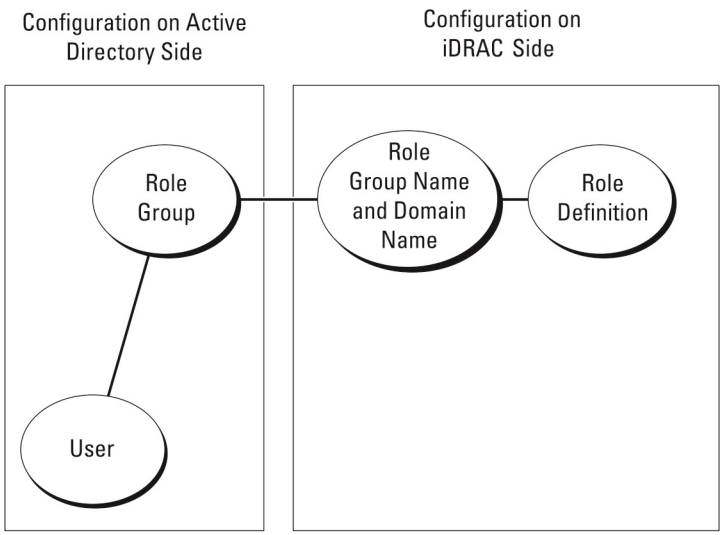


Ilustración 1. Configuración de iDRAC con el esquema estándar de Active Directory

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

Tabla 21. Privilegios predeterminados del grupo de roles

Grupos de funciones	Nivel predeterminado de privilegios	Permisos otorgados	Máscara de bits
Grupo de roles 1	Ninguno	Iniciar sesión en el iDRAC, Configurar el iDRAC, Configurar usuarios, Borrar registros, Ejecutar comandos de control del servidor, Acceder a la consola virtual, Acceder a los medios virtuales, Probar alertas, Ejecutar comandos de diagnóstico	0x000001ff
Grupo de roles 2	Ninguno	Iniciar sesión en el iDRAC, Configurar el iDRAC, Ejecutar comandos de control del servidor, Acceder a la consola virtual, Acceder a los medios virtuales, Probar alertas, Ejecutar comandos de diagnóstico	0x000000f9
Grupo de roles 3	Ninguno	Iniciar sesión en iDRAC	0x00000001
Grupo de roles 4	Ninguno	Sin permisos asignados	0x00000000
Grupo de roles 5	Ninguno	Sin permisos asignados	0x00000000

NOTA: Los valores de la máscara de bits se utilizan únicamente cuando se establece el esquema estándar con RACADM.

Casos de dominio único y dominio múltiple

Si todos los usuarios y grupos de roles de inicio de sesión, incluidos los grupos anidados, se encuentran en el mismo dominio, solamente es necesario configurar las direcciones de las controladoras de dominio en iDRAC. En este caso de dominio único, se admite cualquier tipo de grupo.

Si todos los grupos de roles o usuarios de inicio de sesión, o cualquiera de los grupos anidados, provienen de dominios múltiples, se deberán configurar las direcciones del servidor de catálogo global en iDRAC. En este caso de dominios múltiples, todos los grupos de roles y los grupos anidados, de existir, deben ser del tipo de grupo universal.

Configuración del esquema estándar de Active Directory

Para configurar iDRAC para un acceso de inicio de sesión de Active Directory:

1. En un servidor de Active Directory (controladora de dominio), abra el complemento Usuarios y equipos de Active Directory.
2. Cree un grupo o seleccione un grupo existente. Agregue el usuario de Active Directory como miembro del grupo de Active Directory para obtener acceso a iDRAC.
3. Configure el nombre del grupo, el nombre de dominio y los privilegios de rol en iDRAC mediante la interfaz web de iDRAC o RACADM.

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

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

1 En la interfaz web de iDRAC, vaya a **iDRAC Settings (Configuración de iDRAC)** > **Users (Usuarios)** > **Directory Services (Servicios de directorio)**.

Aparecerá la página **Servicios de directorio**.

2 Seleccione la opción **Microsoft Active Directory** y, a continuación, haga clic en **Edit (Editar)**.

Aparecerá la página **Configuración y administración de Active Directory**.

3 Haga clic en **Configurar Active Directory**.

Aparece la página **Paso 1 de 4 de Configuración y administración de Active Directory**.

4 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). Para ello, se deben especificar las controladoras de dominio y el FQDN de catálogo global. Esto se realiza en los próximos pasos. Además, el DNS debe estar correctamente configurado en la configuración de red.

5 Haga clic en **Next (Siguiente)**.

Aparece la página **Paso 2 de 4 de Configuración y administración de Active Directory**.

6 Active Active Directory y especifique la información de ubicación sobre los servidores de Active Directory y las cuentas de usuario. Además, especifique el tiempo que iDRAC debe esperar para las respuestas de Active Directory durante el inicio de sesión de iDRAC.

NOTA: Si está activada la validación de certificados, especifique las direcciones de servidor de controladora de dominio y el FQDN de catálogo global. Asegúrese de que el DNS esté configurado correctamente en iDRAC Settings (Configuración de iDRAC) > Network (Red).

7 Haga clic en **Next (Siguiente)**. Aparecerá la página **Active Directory Configuration and Management Step 3 of 4 (Paso 3 de 4 de Configuración y administración de Active Directory)**.

8 Seleccione **Esquema estándar** y haga clic en Siguiente.

Aparece la página **Paso 4a de 4 de Configuración y administración de Active Directory**.

9 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.

10 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**.

11 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**.

12 Haga clic en **Finalizar**. Se habrán configurado los valores de Active Directory para el esquema estándar.

Configuración de Active Directory con esquema estándar mediante RACADM

1 Use los siguientes comandos:

```
racadm set iDRAC.ActiveDirectory.Enable 1
racadm set iDRAC.ActiveDirectory.Schema 2
racadm set iDRAC.ADGroup.Name <common name of the role group>
racadm set iDRAC.ADGroup.Domain <fully qualified domain name>
racadm set iDRAC.ADGroup.Privilege <Bit-mask value for specific RoleGroup permissions>
racadm set iDRAC.ActiveDirectory.DomainController1 <fully qualified domain name or IP
address of the domain controller>
racadm set iDRAC.ActiveDirectory.DomainController2 <fully qualified domain name or IP
address of the domain controller>
racadm set iDRAC.ActiveDirectory.DomainController3 <fully qualified domain name or IP
```

```
address of the domain controller>
racadm set iDRAC.ActiveDirectory.GlobalCatalog1 <fully qualified domain name or IP address
of the domain controller>
racadm set iDRAC.ActiveDirectory.GlobalCatalog2 <fully qualified domain name or IP address
of the domain controller>
racadm set iDRAC.ActiveDirectory.GlobalCatalog3 <fully qualified domain name or IP address
of the domain controller>
```

- Introduzca el nombre de dominio completamente calificado (FQDN) de la controladora de dominio, no el FQDN del dominio. Por ejemplo, introduzca `servername.dell.com`, en lugar de `dell.com`.
- Para valores de máscara de bits para permisos de grupo de roles específicos, consulte Privilegios predeterminados del grupo de roles.
- Debe proporcionar al menos una de las tres direcciones de controladora de dominio. La iDRAC trata de conectarse con cada una de las direcciones configuradas, una a la vez, hasta establecer una conexión satisfactoriamente. Con el esquema estándar, son las direcciones de las controladoras de dominio donde se ubican las cuentas de usuario y los grupos de roles.
- El servidor de catálogo global solo es necesario para el esquema estándar cuando las cuentas de usuario y los grupos de roles se encuentran en dominios diferentes. En el caso de múltiples dominios, se puede usar solo el grupo universal.
- Si está activada la validación de certificados, el FQDN o la dirección IP que especifica en este campo deben coincidir con el campo Subject o Subject Alternative Name del certificado de controladora de dominio.
- Para desactivar la validación del certificado durante el protocolo de enlace de SSL, utilice el siguiente comando:

  ```
  racadm set iDRAC.ActiveDirectory.CertValidationEnable 0
  ```

  En este caso, no es necesario cargar ningún certificado de CA.
- Para aplicar la validación de certificado durante el protocolo de enlace de SSL (opcional), utilice el comando siguiente:

  ```
  racadm set iDRAC.ActiveDirectory.CertValidationEnable 1
  ```

  En este caso, deberá cargar el certificado de CA con el siguiente comando:

  ```
  racadm sslcertupload -t 0x2 -f <ADS root CA certificate>
  ```

  NOTA: Si está activada la validación de certificados, especifique las direcciones de servidor de controladora de dominio y el FQDN de catálogo global. Asegúrese de que el DNS esté configurado correctamente en Overview (Descripción general) > iDRAC Settings (Configuración de iDRAC) > Network (Red).

  El siguiente comando de RACADM es opcional.

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

2 Si DHCP está activado en el iDRAC y desea utilizar el DNS proporcionado por el servidor DHCP, introduzca el siguiente comando:

```
racadm set iDRAC.IPv4.DNSFromDHCP 1
```

3 Si DHCP está desactivado en iDRAC o si desea introducir manualmente la dirección IP de DNS, introduzca el siguiente comando de RACADM:

```
racadm set iDRAC.IPv4.DNSFromDHCP 0
racadm set iDRAC.IPv4.DNSFromDHCP.DNS1 <primary DNS IP address>
racadm set iDRAC.IPv4.DNSFromDHCP.DNS2 <secondary DNS IP address>
```

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

```
racadm set iDRAC.UserDomain.<index>.Name <fully qualified domain name or IP Address of the
domain controller>
```

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

Descripción general del esquema extendido de Active Directory

El uso del esquema extendido requiere la extensión del esquema de Active Directory.

Prácticas recomendadas para el esquema extendido

El esquema extendido utiliza objetos de asociación de Dell para unirse a iDRAC y el permiso. Esto le permite a usted usar iDRAC en función de los permisos otorgados en general. El valor predeterminado de la lista de control de acceso (ACL) de los objetos de asociación de Dell permite a los administradores autónomos y de dominio administrar los permisos y el alcance de los objetos de iDRAC.

De manera predeterminada, los objetos de asociación de Dell no heredan todos los permisos de los objetos principales de Active Directory. Si activa la herencia para el objeto de asociación de Dell, los permisos heredados para ese objeto de asociación se otorgarán a los usuarios y grupos seleccionados. Esto puede ocasionar que se proporcionen privilegios imprevistos a la iDRAC.

Para utilizar el esquema extendido manera segura, Dell recomienda no activar la herencia en objetos de asociación de Dell dentro de la implementación del esquema extendido.

Extensiones de esquema de Active Directory

Los datos de Active Directory son una base de datos distribuida de *atributos* y *clases*. El esquema de Active Directory incluye las reglas que determinan los tipos de datos que se pueden agregar o incluir en la base de datos. La clase de usuario es un ejemplo de una *clase* que se almacena en la base de datos. Algunos ejemplos de atributos de clase de usuario pueden incluir el nombre, el apellido, el número de teléfono y otros datos del usuario. Puede ampliar la base de datos de Active Directory al agregar sus propios y exclusivos *atributos* y *clases* para requisitos específicos. Dell ha extendido el esquema para incluir los cambios necesarios para admitir la autorización y la autenticación de administración remota mediante Active Directory.

Cada *atributo* o *clase* que se agrega a un esquema existente de Active Directory debe definirse con una Id. única. Para mantener Id. únicas en todo el sector, Microsoft mantiene una base de datos de identificadores de objetos de Active Directory (OID) para que cuando las empresas agreguen extensiones al esquema, puedan tener la garantía de que serán únicas y no entrarán en conflicto entre sí. Para extender el esquema en Active Directory de Microsoft, Dell recibe OID únicos, extensiones de nombre únicas e Id. de atributo con vínculo únicas para los atributos y las clases que se agregan al servicio de directorio:

- La extensión es: `dell`.
- El OID de base es: `1.2.840.113556.1.8000.1280`.
- El rango de Id. de vínculo de RAC es: `12070 to 12079`.

Descripción general sobre las extensiones de esquema de iDRAC

Dell ha extendido el esquema para incluir una propiedad *Association (Asociación)*, *Device (Dispositivo)* y *Privilege (Privilegio)*. La propiedad *Association (Asociación)* se utiliza para vincular usuarios o grupos con un conjunto específico de privilegios para uno o varios dispositivos iDRAC. Este modelo le proporciona a un administrador la flexibilidad máxima sobre las distintas combinaciones de usuarios, privilegios de iDRAC y dispositivos iDRAC en la red sin mucha complexidad.

Para cada dispositivo iDRAC físico en la red que desee integrar con Active Directory para la autenticación y autorización, cree al menos un objeto de asociación y un objeto de dispositivo iDRAC. Puede crear varios objetos de asociación y cada uno de ellos se puede vincular con varios usuarios, grupos de usuarios u objetos de dispositivo iDRAC, según sea necesario. Los usuarios y los grupos de usuarios de iDRAC pueden ser miembros de cualquier dominio en la empresa.

No obstante, cada objeto de asociación puede vincularse (o puede vincular usuarios, grupos de usuarios u objetos de dispositivo iDRAC) con un solo objeto de privilegio. En este ejemplo, se le permite al administrador controlar los privilegios de cada usuario en dispositivos iDRAC específicos.

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

En la figura siguiente se muestra que el objeto de asociación proporciona la conexión necesaria para la autentificación y la autorización.

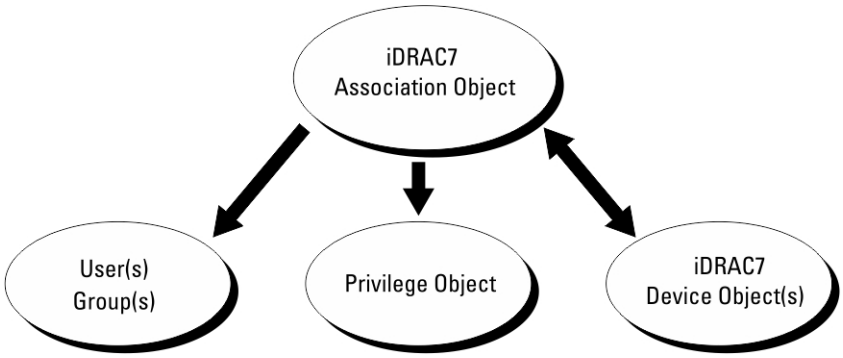


Ilustración 2. Configuración típica de los objetos de active directory

Puede crear el número de objetos de asociación que sea necesario. Sin embargo, debe crear al menos un objeto de asociación y debe tener al menos un objeto de dispositivo iDRAC para cada dispositivo iDRAC en la red que desee integrar con Active Directory para la autenticación y autorización con iDRAC.

El objeto de asociación permite el número de usuarios o grupos que sea necesario, así como objetos de dispositivo iDRAC. No obstante, el objeto de asociación solo incluye un solo objeto de privilegio por objeto de asociación. El objeto de asociación conecta los usuarios que tienen los privilegios en los dispositivos iDRAC.

La extensión de Dell al complemento ADUC MMC solo permite asociar el objeto de privilegio y objetos de iDRAC desde el mismo dominio con el objeto de asociación. La extensión de Dell no permite que un grupo o un objeto de iDRAC de otros dominios se agreguen como miembro de producto del objeto de asociación.

Cuando agregue 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 funcionan con grupos universales de otros dominios.

Los usuarios, los grupos de usuarios o los grupos de usuarios anidados de otros dominios se pueden agregar al objeto de asociación. Las soluciones de esquema extendido admiten cualquier tipo de grupo de usuarios y cualquier anidamiento de grupos de usuarios en varios dominios admitidos por Microsoft Active Directory.

Acumulación de privilegios con el esquema extendido

El mecanismo de autentificación del esquema extendido admite la acumulación de privilegios de distintos objetos de privilegio asociados con el mismo usuario a través de distintos objetos de asociación. En otras palabras, la autentificación del esquema extendido acumula privilegios para permitir que el usuario tenga el súper conjunto de todos los privilegios asignados correspondientes a los distintos 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.

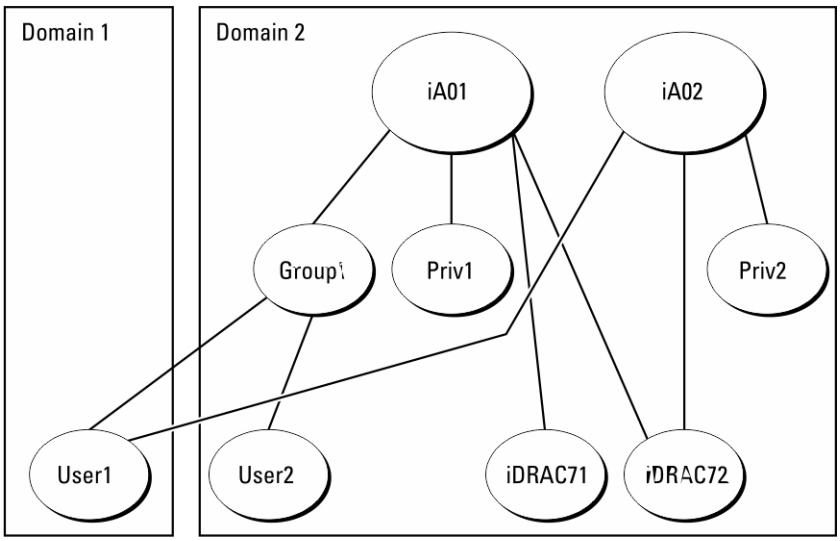


Ilustración 3. Acumulación de privilegios para un usuario

En la figura, se muestran dos objetos de asociación: A01 y A02. Usuario1 está asociado a iDRAC2 a través de ambos objetos de asociación.

La autentificación del esquema extendido acumula privilegios para permitir que el usuario tenga el conjunto máximo de privilegios según los privilegios asignados de los distintos objetos de privilegio asociados al mismo usuario.

En este ejemplo, Usuario1 tiene los privilegios Priv1 y Priv2 en iDRAC2. Usuario1 tiene privilegios Priv1 en iDRAC1 solamente. Usuario2 tiene privilegios Priv1 tanto en iDRAC1 como en iDRAC2. Asimismo, en esta figura, se muestra que Usuario1 puede estar en un dominio diferente y puede ser miembro de un grupo.

Configuración del esquema extendido de Active Directory

Si desea configurar Active Directory para acceder a iDRAC:

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

Extensión del esquema de Active Directory

La extensión del esquema de Active Directory agrega una unidad organizacional de Dell, clases y atributos de esquema, y ejemplos de privilegios y objetos de asociación al esquema de Active Directory. Antes de extender el esquema, asegúrese de tener privilegios de administrador de esquema en el propietario de roles de operaciones de maestro único flexible (FSMO) de maestro de esquema en el bosque de dominio.

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 están en el DVD *Dell Systems Management Tools and Documentation* (Documentación y herramientas de Dell Systems Management) en los siguientes directorios respectivamente:

- Unidad DVD: **\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\LDIF_Files**
- <Unidad DVD>: **\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\Schema Extender**

Para usar los archivos LDIF, consulte las instrucciones en el archivo léame que se incluye en el directorio **LDIF_Files**.

Puede copiar y ejecutar Schema Extender o los archivos LDIF desde cualquier ubicación.

Uso de Dell Schema Extender

PRECAUCIÓN: Dell Schema Extender utiliza el archivo SchemaExtenderOem.ini. Para asegurarse de que la utilidad Dell Schema Extender funcione correctamente, no modifique el nombre de este archivo.

1. En la pantalla de **Bienvenida**, haga clic en **Siguiente.**
2. Lea y comprenda la advertencia y haga clic en **Siguiente**.
3. Seleccione **Usar las credenciales de inicio de sesión actuales** o introduzca un nombre de usuario y una contraseña con derechos de administrador de esquema.
4. Haga clic en **Siguiente** para ejecutar Dell Schema Extender.
5. Haga clic en **Finalizar**.

   El esquema se ha extendido. Para comprobar la extensión del esquema, utilice MMC y el complemento de esquema de Active Directory para verificar que Clases y atributos existe. 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 22. Definiciones de clases para las clases agregadas al esquema de Active Directory

Nombre de la clase	Número de identificación de objeto asignado (OID)
delliDRACDevice	1.2.840.113556.1.8000.1280.1.7.1.1
delliDRACAssociation	1.2.840.113556.1.8000.1280.1.7.1.2
dellRAC4Privileges	1.2.840.113556.1.8000.1280.1.1.1.3
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5

Tabla 23. Clase DelliDRACdevice

OID	1.2.840.113556.1.8000.1280.1.7.1.1
Descripción	Representa el dispositivo de iDRAC de Dell. iDRAC debe configurarse como delliDRACDevice en Active Directory. Esta configuración permite a iDRAC enviar solicitudes de protocolo ligero de acceso a directorios (LDAP) a Active Directory.
Tipo de clase	Clase estructural
SuperClasses	dellProduct

OID	1.2.840.113556.1.8000.1280.1.7.1.1
Atributos	dellSchemaVersion
	dellRacType

Tabla 24. Clase delliDRACAssociationObject

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

Tabla 25. Clase dellRAC4Privileges

OID	1.2.840.113556.1.8000.1280.1.1.1.3
Descripción	Define los privilegios (derechos de autorización) para iDRAC
Tipo de clase	Clase auxiliar
SuperClasses	Ninguno
Atributos	dellIsLoginUser
	dellIsCardConfigAdmin
	dellIsUserConfigAdmin
	dellIsLogClearAdmin
	dellIsServerResetUser
	dellIsConsoleRedirectUser
	dellIsVirtualMediaUser
	dellIsTestAlertUser
	dellIsDebugCommandAdmin

Tabla 26. 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

OID	1.2.840.113556.1.8000.1280.1.1.1.4
SuperClasses	Usuario
Atributos	dellRAC4Privileges

Tabla 27. Clase dellProduct

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

Tabla 28. Lista de atributos agregados al esquema de Active Directory

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

Nombre del atributo/Descripción	OID asignado/Identificador de objeto de sintaxis	Con un solo valor
TRUE si el usuario tiene derechos de restablecimiento de servidor en el dispositivo.	Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellIsConsoleRedirectUser TRUE si el usuario tiene derechos de consola virtual en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.8 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	VERDADERO
dellIsVirtualMediaUser TRUE si el usuario tiene derechos de medios virtuales en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.9 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	VERDADERO
dellIsTestAlertUser TRUE si el usuario tiene derechos de usuario de alertas de prueba en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.10 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	VERDADERO
dellIsDebugCommandAdmin TRUE si el usuario tiene derechos de administrador de comando de depuración en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.11 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	VERDADERO
dellSchemaVersion La versión del esquema actual se usa para actualizar el esquema.	1.2.840.113556.1.8000.1280.1.1.2.12 Cadena de no distinguir mayúsculas de minúsculas (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	VERDADERO
dellRacType Este atributo es el tipo de RAC actual para el objeto delliDRACDevice y el vínculo de retroceso al vínculo de avance de dellAssociationObjectMembers.	1.2.840.113556.1.8000.1280.1.1.2.13 Cadena de no distinguir mayúsculas de minúsculas (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	VERDADERO
dellAssociationMembers Lista de los objetos dellAssociationObjectMembers que pertenecen a este producto. Este atributo es el vínculo de retroceso al atributo vinculado dellProductMembers. Identificación de vínculo: 12071	1.2.840.113556.1.8000.1280.1.1.2.14 Nombre distintivo (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSO

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

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

Cuando instale el software Systems Management con el DVD *Dell Systems Management Tools and Documentation (Herramientas y documentación de Dell Systems Management)*, puede extender el complemento si selecciona la opción **Active Directory Users and Computers Snap-in (Complemento Usuarios y equipos de Active Directory)**. Consulte Dell OpenManage Software Quick Installation Guide (Guía de instalación rápida del software Dell OpenManage) para obtener instrucciones adicionales acerca de la instalación del software Systems Management. Para los sistemas operativos Windows de 64 bits, el instalador del complemento se encuentra en:

<Unidad DVD>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_SnapIn64

Para obtener más información acerca del complemento Usuarios y equipos de Active Directory, consulte la documentación de Microsoft.

Cómo agregar usuarios y privilegios de iDRAC a Active Directory

Con el complemento Usuarios y equipos de Active Directory extendido de Dell, puede agregar usuarios y privilegios de iDRAC mediante la creación de objetos de dispositivo, asociación y privilegios. Para agregar cada objeto, siga estos pasos:

- Cree un objeto de dispositivo iDRAC
- Cree un objeto de privilegio
- Cree un objeto de asociación
- Agregue los objetos a un objeto de asociación

Creación de un objeto de dispositivo de iDRAC

Para crear un objeto de dispositivo de iDRAC:

1 En la ventana **Raíz de consola** de MMC, haga clic con el botón derecho del mouse en un contenedor.
2 Seleccione **Nuevo** > **Opciones avanzadas del objeto Dell Remote Management**.
Se abre la ventana **Nuevo objeto**.
3 Introduzca un nombre para el nuevo objeto. El nombre debe ser idéntico al nombre de iDRAC que se introduce al configurar las propiedades de Active Directory mediante la interfaz web de iDRAC.
4 Seleccione **Objeto de dispositivo de iDRAC** y haga clic en Aceptar.

Creación de un objeto de privilegio

Para crear un objeto de privilegio:

NOTA: Debe crear un objeto de privilegio en el mismo dominio que el objeto de asociación relacionado.

1 En la ventana **Raíz de consola** (MMC), haga clic con el botón derecho del mouse en un contenedor.
2 Seleccione **Nuevo** > **Opciones avanzadas del objeto Dell Remote Management**.
Se abre la ventana **Nuevo objeto**.
3 Introduzca un nombre para el nuevo objeto.
4 Seleccione **Objeto de privilegio** y haga clic en Aceptar.
5 Haga clic con el botón derecho del mouse en el objeto de privilegio que creó y seleccione **Propiedades**.
6 Haga clic en la ficha **Privilegios de administración remota** y asigne los privilegios para el usuario o grupo.

Creación de un objeto de asociación

Para crear un objeto de asociación:

NOTA: El objeto de asociación de iDRAC se deriva de un grupo y su alcance está configurado como Local de dominio.

1 En la ventana **Raíz de consola** (MMC), haga clic con el botón derecho del mouse en un contenedor.
2 Seleccione **Nuevo** > **Opciones avanzadas del objeto Dell Remote Management**.
Se abre la ventana **Nuevo objeto**.

3 Introduzca un nombre para el nuevo objeto y seleccione **Objeto de asociación**.
4 Seleccione el ámbito para el **Objeto de asociación** y haga clic en Aceptar.
5 Proporcione privilegios de acceso a los usuarios autentificados para acceder al objeto de asociación creado.

Concesión de privilegios de acceso a los usuarios para los objetos de asociación

Para proporciona privilegios de acceso a los usuarios autentificados para acceder al objeto de asociación creado:

1 Vaya a **Administrative Tools (Herramientas administrativas)** > **ADSI Edit (Editor ADSI)**. Aparece la ventana **ADSI Edit (Editor ADSI)**.
2 En el panel derecho, navegue al objeto de asociación creado, haga clic con el botón derecho del mouse y seleccione **Propiedades.**
3 En la ficha **Seguridad**, haga clic en **Agregar**.
4 Escriba `Authenticated Users` y haga clic **Check Names (Verificar nombres)** y en **OK (Aceptar)**. Los usuarios autenticados se agregan a la lista **Groups and user names (Grupos y nombres de usuario)**.
5 Haga clic en **OK** (Aceptar).

Adición de objetos a un objeto de asociación

En la ventana **Propiedades de objeto de asociación**, puede asociar usuarios o grupos de usuarios, objetos de privilegio y dispositivos iDRAC o grupos de dispositivos iDRAC.

Puede agregar grupos de usuarios y dispositivos de iDRAC.

Adición de usuarios o grupos de usuarios

Para agregar usuarios o grupos de usuarios:

1 Haga clic con el botón derecho del mouse en **Objeto de asociación** y seleccione **Propiedades**.
2 Seleccione la ficha **Usuarios** y haga clic en **Agregar**.
3 Introduzca el nombre del grupo de usuarios o del usuario y haga clic en **Aceptar**.

Adición de privilegios

Para agregar privilegios:
Haga clic en la ficha **Objeto de privilegio** para agregar el objeto de privilegio a la asociación que define los privilegios del usuario o del grupo de usuarios al autentificar un dispositivo iDRAC. Solo se puede agregar un objeto de privilegio a un objeto de asociación.

1 Seleccione la ficha **Objeto de privilegios** y haga clic en **Agregar**.
2 Introduzca el nombre del objeto de privilegio y haga clic en **Aceptar**.
3 Haga clic en la ficha **Objeto de privilegio** para agregar el objeto de privilegio a la asociación que define los privilegios del usuario o del grupo de usuarios al autentificar un dispositivo iDRAC. Solo se puede agregar un objeto de privilegio a un objeto de asociación.

Cómo agregar dispositivos iDRAC o grupos de dispositivos iDRAC

Para agregar dispositivos iDRAC o grupos de dispositivos iDRAC:

1 Seleccione la ficha **Productos** y haga clic en **Agregar**.
2 Introduzca el nombre de los dispositivos iDRAC o de los grupos de dispositivos iDRAC y haga clic en **Aceptar**.
3 En la ventana **Propiedades**, haga clic en **Aplicar** y en **Aceptar**.
4 Haga clic en la ficha **Products (Productos)** para agregar un dispositivo iDRAC conectado a la red que está disponible para los usuarios o los grupos de usuarios definidos. Puede agregar varios dispositivos iDRAC a un objeto de asociación.

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

Para configurar Active Directory con esquema extendido mediante la interfaz web:

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

1 En la interfaz web de iDRAC, vaya a **iDRAC Settings (Configuración de iDRAC)** > **Users (Usuarios)** > **Directory Services (Servicios de directorio)** > **Microsoft Active Directory**. Haga clic en **Edit (Editar)**.

Aparece la página **Paso 1 de 4 de Configuración y administración de Active Directory**.

2 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).

3 Haga clic en **Next (Siguiente)**.

Aparece la página **Paso 2 de 4 de Configuración y administración de Active Directory**.

4 Especifique la información de ubicación sobre las cuentas de usuario y los servidores de Active Directory (AD). Además, especifique el tiempo que iDRAC debe esperar para las respuestas de AD durante el proceso de inicio de sesión.

NOTA:

- Si está activada la validación de certificados, especifique las direcciones de servidor de controladora de dominio y el FQDN. Asegúrese de que el DNS esté configurado correctamente en **iDRAC Settings (Configuración de iDRAC)** > **Network (Red)**.
- Si el usuario y los objetos de iDRAC se encuentran en dominios diferentes, no seleccione la opción **User Domain from Login (Dominio de usuario desde inicio de sesión)**. En su lugar, seleccione la opción **Specify a Domain (Especificar un dominio)** e introduzca el nombre de dominio donde el objeto de iDRAC está disponible.

5 Haga clic en **Next (Siguiente)**. Aparecerá la página **Active Directory Configuration and Management Step 3 of 4 (Paso 3 de 4 de Configuración y administración de Active Directory)**.

6 Seleccione **Esquema extendido** y haga clic en **Siguiente**.

Aparece la página **Paso 4 de 4 de Configuración y administración de Active Directory**.

7 Introduzca el nombre y la ubicación del objeto de dispositivo de iDRAC en Active Directory (AD) y haga clic en **Terminar**.

Se habrán configurado los valores de Active Directory para el modo de esquema extendido.

Configuración de Active Directory con esquema extendido mediante RACADM

Para configurar Active Directory con esquema estándar a través de RACADM:

1 Use los siguientes comandos:

```
racadm set iDRAC.ActiveDirectory.Enable 1
racadm set iDRAC.ActiveDirectory.Schema 2
racadm set iDRAC.ActiveDirectory.RacName <RAC common name>
racadm set iDRAC.ActiveDirectory.RacDomain <fully qualified rac domain name>
racadm set iDRAC.ActiveDirectory.DomainController1 <fully qualified domain name or IP
address of the domain controller>
racadm set iDRAC.ActiveDirectory.DomainController2 <fully qualified domain name or IP
address of the domain controller>
racadm set iDRAC.ActiveDirectory.DomainController3 <fully qualified domain name or IP
address of the domain controller>
```

- Introduzca el nombre de dominio completamente calificado (FQDN) de la controladora de dominio, no el FQDN del dominio. Por ejemplo, introduzca `servername.dell.com`, en lugar de `dell.com`.
- Debe proporcionar al menos una de las tres direcciones. La iDRAC trata de conectarse con cada una de las direcciones configuradas, una a la vez, hasta establecer una conexión satisfactoriamente. Con el esquema extendido, son las direcciones IP o FQDN de las controladoras de dominio donde se encuentra este dispositivo iDRAC.

- Para desactivar la validación del certificado durante el protocolo de enlace de SSL, utilice el siguiente comando:

  ```
  racadm set iDRAC.ActiveDirectory.CertValidationEnable 0
  ```

  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 set iDRAC.ActiveDirectory.CertValidationEnable 1
  ```

  En este caso, deberá cargar un certificado de la entidad emisora con el siguiente comando:

  ```
  racadm sslcertupload -t 0x2 -f <ADS root CA certificate>
  ```

  NOTA: Si está activada la validación de certificados, especifique las direcciones de servidor de controladora de dominio y el FQDN. Asegúrese de que el DNS está configurado correctamente en iDRAC Settings (Configuración de iDRAC) > Network (Red).

  El siguiente comando de RACADM es opcional:

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

2 Si DHCP está activado en el iDRAC y desea utilizar el DNS proporcionado por el servidor DHCP, introduzca el siguiente comando:

```
racadm set iDRAC.IPv4.DNSFromDHCP 1
```

3 Si DHCP está desactivado en iDRAC o si desea introducir manualmente la dirección IP de DNS, introduzca el siguiente comando:

```
racadm set iDRAC.IPv4.DNSFromDHCP 0
racadm set iDRAC.IPv4.DNSFromDHCP.DNS1 <primary DNS IP address>
racadm set iDRAC.IPv4.DNSFromDHCP.DNS2 <secondary DNS IP address>
```

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

```
racadm set iDRAC.UserDomain.<index>.Name <fully qualified domain name or IP Address of the
domain controller>
```

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

Prueba de la configuración de Active Directory

Puede probar la configuración de Active Director para comprobar si es correcta o para diagnosticar el problema con un inicio de sesión de Active Directory fallido.

Prueba de la configuración de Active Directory mediante una interfaz web de iDRAC

Para probar la configuración de Active Directory:

1 En la interfaz web de iDRAC, vaya a **iDRAC Settings (Configuración de iDRAC)** > **Users (Usuarios)** > **Directory Services (Servicios de directorio)** > **Microsoft Active Directory** y haga clic en **Test (Prueba)**.

Aparece la página **Test Active Directory Settings (Probar configuración de Active Directory)**.

2 Haga clic en **Prueba**.

3 Introduzca el nombre de usuario de prueba (por ejemplo, **nombredeusuario@dominio.com**) y la contraseña, y haga clic en **Start Test (Iniciar prueba)**. Aparecerán los resultados de la prueba y el registro de la misma.

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 Enable Certificate Validation (Activar validación de certificados) seleccionada, la iDRAC requiere que el servidor de Active Directory se identifique por el FQDN, y no una dirección IP. Si el servidor de Active Directory se identifica por una dirección IP, fallará la validación de certificados porque la iDRAC no puede comunicarse con el servidor de 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 *iDRAC RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM de iDRAC), disponible en **dell.com/idracmanuals**.

Configuración de los usuarios LDAP genéricos

iDRAC ofrece una solución genérica para admitir la autentificación basada en el Protocolo liviano de acceso a directorios (LDAP). Esta función no requiere ninguna extensión del esquema en sus servicios de directorio.

Para hacer que la implementación LDAP de iDRAC sea genérica, los elementos comunes entre los distintos servicios de directorio se utilizan para agrupar usuarios y asignar la relación usuario-grupo. La acción específica del servicio de directorio es el esquema. Por ejemplo, pueden tener nombres de atributo diferentes para el grupo, el usuario y el vínculo entre el usuario y el grupo. Estas acciones se pueden configurar en iDRAC.

NOTA: Los inicios de sesión de autentificación 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.

Configuración del servicio de directorio de LDAP genérico mediante la interfaz basada en web de iDRAC

Para configurar el del servicio de directorio de LDAP genérico mediante la interfaz web:

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

1. En la interfaz web de iDRAC, vaya a **Configuración de iDRAC** > **Usuario** > **Servicios de directorio** > **Servicios de directorio LDAP genérico**, y haga clic en **Editar**.
   La página **Pasos 1 y 3 de la Configuración y administración de LDAP genérico** muestra la configuración actual del LDAP genérico.
2. 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 perteneciente a SSL. Sólo se admite el LDAP a través de SSL.
3. Haga clic en **Next (Siguiente)**.
   Aparece la página **Paso 2 de 3 de Configuración y administración de LDAP genérico**.
4. Active la autentificación 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 haya configurado correctamente en 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 admite un único dominio. No se admiten dominios cruzados.
5. Haga clic en **Next (Siguiente)**.
   Aparece la página **Paso 3a de 3 de Configuración y administración de LDAP genérico**.
6. Haga clic en **Grupo de roles**.
   Aparece la página **Paso 3b de 3 de Configuración y administración de LDAP genérico**.
7. 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 guarda la configuración del grupo de roles. La página **Paso 3a de 3 de la Configuración y administración de LDAP genérico** muestra la configuración del grupo de roles.

8 Si desea configurar grupos de roles adicionales, repita los pasos 7 y 8.

9 Haga clic en **Finalizar**. Se habrá configurado el servicio de directorio LDAP.

Configuración del servicio de directorio LDAP genérico mediante RACADM

Para configurar el servicio de directorio LDAP, utilice los objetos de los grupos iDRAC.LDAP e iDRAC.LDAPRole.

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

Prueba de la configuración del servicio de directorio de LDAP

Puede probar la configuración del servicio de directorio de LDAP para comprobar si es correcta o para diagnosticar la falla de la sesión de inicio de LDAP.

Prueba de la configuración del servicio de directorio de LDAP mediante una interfaz web de iDRAC

Para probar la configuración del servicio de directorio LDAP:

1 En la interfaz web de iDRAC, vaya a **Configuración de iDRAC** > **Usuarios** > **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 **Prueba**.

3 Introduzca el nombre de usuario y la contraseña de un usuario de directorio elegido para probar la configuración de LDAP. El formato depende del *Atributo de inicio de sesión del usuario* utilizado y el nombre de usuario introducido debe coincidir con el valor del atributo elegido.

NOTA: Al realizar la prueba de la configuración de LDAP con Activar validación de certificados seleccionada, iDRAC requiere que el servidor de LDAP sea identificado por FQDN y no una dirección IP. Si una dirección IP identifica el servidor de LDAP, fallará la validación del certificado porque iDRAC no puede comunicarse con el servidor LDAP.

NOTA: Cuando está habilitado el LDAP genérico, iDRAC primero intenta iniciar la sesión del usuario como un usuario de directorio. Si falla, se activa la búsqueda de usuario local.

Aparecen los resultados de la prueba y el registro de la misma.

Prueba de la configuración del servicio de directorio LDAP mediante RACADM

Para probar la configuración del servicio de directorio LDAP, utilice el comando `testfeature`. Para obtener más información, consulte *iDRAC RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM de iDRAC), disponible en **dell.com/idracmanuals**.

8

Modo de bloqueo del sistema

El modo de bloqueo del sistema es compatible con el iDRAC 9 y versiones posteriores. Esta función le permite asegurarse de que una vez que un sistema se aprovisiona según sea necesario, no debería cambiar la configuración específica. Esta función puede protegerlo de modificaciones no intencionadas o malintencionadas. El modo de bloqueo puede aplicarse a las actualizaciones de configuración y firmware. En el estado de bloqueo todas las herramientas Dell se asegurarán de bloquear cualquier intento de cambiar la configuración del sistema. Se mostrará un mensaje de error en caso de que exista dicho intento.

NOTA: Una vez que el modo de bloqueo del sistema está activado, los usuarios no podrán cambiar los valores de configuración. Los campos de configuración del sistema permanecen desactivados.

El modo de bloqueo se puede activar o desactivar de las siguientes interfaces:

- UI de iDRAC
- Racadm de iDRAC
- WSMan de iDRAC
- IDRAC SCP (Perfil de configuración del sistema)
- Redfish de IDRAC
- Uso de F2 durante la configuración de iDRAC

NOTA: Para permitir el modo de bloqueo el usuario debe tener la licencia de iDRAC Enterprise y privilegios de control del sistema.

Existen algunas tareas esenciales que se pueden realizar incluso si el sistema se encuentra en el modo de bloqueo. Las siguientes operaciones están permitidas cuando el sistema está en modo de bloqueo:

- Configuración del límite de alimentación
- Operaciones de encendido del sistema (encendido/apagado, restablecer)
- Identificar operaciones (chasis o PERC)
- Sustitución de piezas
- Ejecución de diagnósticos
- Las operaciones modulares (configuración de Vlan, dirección flex)
- Código de acceso de Group Manager

La siguiente tabla enumera las características funcionales y no funcionales, las interfaces y las utilidades que se ven afectadas por el modo de bloqueo:

Tabla 29. Elementos afectados por el modo de bloqueo

Desactivado	Permanece funcional

• OMSA/OMSS
• IPMI
• DRAC/LC
• RACADM
• WSMan
• DTK-Syscfg
• Redfish
• OpenManage Essentials
	• Todas las herramientas de proveedores que tengan acceso directo al dispositivo
	• PERC
	  • PERC CLI
	  • DTK-RAIDCFG
	  • F2/Ctrl+R
	• NVMe
	  • DTK-RAIDCFG

Desactivado	Permanece funcional

• BIOS (la configuración F2 se vuelve de sólo lectura)	• F2/Ctrl+R
	• BOSS
	  • Marvell CLI
	  • F2/Ctrl+R
	• Sustitución de piezas, Restauración sencilla y sustitución de la placa base
	• Límites de alimentación
	• Operaciones de encendido del sistema (encendido, apagado, restablecer)
	• Identifique los dispositivos (chasis y PERC)
	• Configuración de ISM/OMSA (activar SO/BMC, comando ping guardián, nombre del sistema operativo, versión del sistema operativo)
	• Las operaciones modulares (configuración de VLAN, direccionamiento flex)
	• Código de acceso de Group Manager

9

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

En esta sección se proporciona información para configurar iDRAC con el inicio de sesión mediante tarjeta inteligente (para usuarios locales y usuarios de Active Directory) y el inicio de sesión único (SSO) (para usuarios de Active Directory). SSO y el inicio de sesión único son funciones con licencia.

iDRAC admite la autentificación de Active Directory basada en Kerberos para admitir inicios de sesión mediante tarjeta inteligente y SSO. Para obtener información sobre Kerberos, consulte el sitio web de Microsoft.

Temas:

Prerrequisitos para el inicio de sesión único de Active Directory o el inicio de sesión mediante tarjeta inteligente

A continuación se indican los prerrequisitos de inicios de sesión SSO y mediante tarjeta inteligente basados en Active Directory:

- Sincronice la hora de iDRAC con la hora de la controladora de dominio de Active Directory. Si no es así, fallará la autenticación de Kerberos en el iDRAC. Es posible usar la zona horaria y la función de NTP para sincronizar la hora. Para ello, consulte Configuración de zona horaria y NTP.
- Registre el iDRAC como equipo en el dominio raíz de Active Directory.
- Genere un archivo keytab mediante la herramienta ktpass.
- Para activar el inicio de sesión único para el esquema extendido, asegúrese de que la opción **Confiar en este usuario para la delegación a cualquier servicio (solo Kerberos)** está seleccionada en la pestaña **Delegación** del usuario Keytab. Esta pestaña solo está disponible después de crear el archivo Keytab mediante la utilidad ktpass.
- Configure el explorador para activar el inicio de sesión SSO.
- Cree los objetos de Active Directory y proporcione los privilegios necesarios.
- Para SSO, configure la zona de búsqueda invertida en los servidores DNS para la subred en la que reside iDRAC.

  NOTA: Si el nombre del host no coincide con la búsqueda de DNS invertida, fallará la autentificación de Kerberos.
- Configure el explorador para admitir el inicio de sesión SSO. Para obtener más información, consulte Inicio de sesión único .

  NOTA: Google Chrome y Safari no admiten Active Directory para realizar el inicio de sesión SSO.

Registro de iDRAC como equipo en el dominio raíz de Active Directory

Para registrar iDRAC en el dominio raíz de Active Directory:

1 Haga clic en **Configuración de iDRAC** > **Conectividad** > **Red**.

Aparecerá la página **Red**.

2 Puede seleccionar **Configuración de IPv4** o **Configuración de IPv6** en función de la configuración de IP.

3 Introduzca una dirección IP válida **para el Servidor DNS preferido/alternativo**. Este valor es una dirección IP válida del servidor DNS que forma parte del dominio raíz.

4 Seleccione **Registrar el iDRAC en DNS**.

5 Indique un **nombre de dominio DNS** válido.

6 Verifique que la configuración de DNS de la red coincida con la información de DNS de Active Directory.

Para obtener más información sobre las opciones, consulte la *Ayuda en línea de iDRAC*.

Generación del archivo Keytab de Kerberos

Para admitir la autenticación de inicio de sesión mediante SSO y tarjeta inteligente, iDRAC permite que la configuración se active como un servicio protegido en una red de Windows Kerberos. La configuración de Kerberos en iDRAC implica los mismos pasos que la configuración de un servicio que no sea de Windows Server Kerberos como elemento principal de seguridad en Windows Server Active Directory.

La Herramienta *ktpass* (disponible en Microsoft como parte de los CD/DVD de instalación de servidores) se utiliza para crear enlaces de Nombre principal del servicio (SPN) a una cuenta de usuario y exportar la información de confianza a un archivo Keytab de Kerberos de tipo MIT, el cual 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 autentificación de Kerberos para utilizar las funciones de interoperabilidad que proporciona un servicio Windows Server Kerberos KDC. Para obtener más información sobre la utilidad **ktpass**, consulte el sitio web de Microsoft en: **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 usar con la opción **-mapuser** del comando. `ktpass` Asimismo, debe tener el mismo nombre que el nombre DNS de iDRAC al que cargará el archivo Keytab generado.

Para generar un archivo keytab mediante la herramienta ktpass:

1 Ejecute la utilidad *ktpass* en la controladora de dominio (servidor de Active Directory) donde desee asignar el iDRAC a una cuenta de usuario en Active Directory.

2 Utilice el comando ktpass siguiente para crear el archivo keytab de Kerberos:

```
C:\> ktpass.exe -princ HTTP/idrac7name.domainname.com@DOMAINNAME.COM -mapuser DOMAINNAME
\username -mapOp set -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass [password] -out c:
\krbkeytab
```

El tipo de cifrado es AES256-SHA1. El tipo principal es KRB5_NT_PRINCIPAL. Las propiedades de la cuenta de usuario a la que se asigna el Nombre principal del servicio deben tener activada la propiedad **Utilizar tipos de cifrado AES 256 para esta cuenta**.

> **NOTA: Utilice letras en minúsculas para el iDRACname y el Nombre principal del servicio. Utilice letras en mayúsculas para el nombre de dominio, tal como se muestra en el ejemplo.**

3 Ejecute el comando siguiente:

```
C:\>setspn -a HTTP/iDRACname.domainname.com username
```

Se genera un nuevo archivo keytab.

NOTA: Si encuentra problemas con el usuario de iDRAC para el que se crea el archivo Keytab, cree un nuevo usuario y un nuevo archivo Keytab. Si se vuelve a ejecutar el mismo archivo Keytab que se había creado en un principio, 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. Se recomienda 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 autentificados* para acceder al objeto de asociación creado.

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

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

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

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

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

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

1 Verifique si el nombre DNS de iDRAC coincide con el nombre de dominio completamente calificado de iDRAC. Para ello, en la interfaz web de iDRAC, vaya a **Configuración de iDRAC** > **Red** > **Valores comunes** y consulte la propiedad **Nombre DNS de iDRAC**.
2 Al configurar Active Directory para configurar una cuenta de usuario basada en el esquema estándar o el esquema extendido, realice los dos pasos adicionales siguientes para configurar SSO:
   - Cargue el archivo keytab en la página **Paso 1 de 4 de Configuración y administración de Active Directory**.
   - Seleccione **Activar inicio de sesión único** en la página **Paso 2 de 4 de Configuración y administración de Active Directory**.

Configuración del inicio de sesión SSO de iDRAC para usuarios de Active Directory mediante RACADM

Para activar el inicio de sesión único (SSO), complete los pasos para configurar Active Directory y ejecute el comando siguiente:

```
racadm set iDRAC.ActiveDirectory.SSOEnable 1
```

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

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

1 Cargue el certificado de usuario de tarjeta inteligente y el certificado de CA de confianza en iDRAC.
2 Active el inicio de sesión mediante tarjeta inteligente.

Carga del certificado de usuario de tarjeta inteligente

Antes de cargar el certificado de usuario, asegúrese de que el certificado de usuario del proveedor de la tarjeta inteligente se ha exportado en el formato Base64. También se admiten los certificados SHA-2.

Carga del certificado de usuario de tarjeta inteligente mediante la interfaz web

Para cargar el certificado de usuario de tarjeta inteligente:

1 En la interfaz web de iDRAC, vaya a **Configuración de iDRAC** > **Usuarios** > **Tarjeta Inteligente**.

> **NOTA: La función de inicio de sesión de tarjeta inteligente requiere la configuración del certificado de usuario local y/o de Active Directory.**

2 En **Configurar Inicio de sesión de tarjeta inteligente**, seleccione **Activado con RACADM remota** para permitir la configuración.
3 Active la **Verificación CRL para el Inicio de sesión de tarjeta inteligente**
4 Haga clic en **Aplicar**.

Carga del certificado de usuario de tarjeta inteligente mediante RACADM

Para cargar el certificado de usuario de tarjeta inteligente, utilice el objeto **usercertupload**. Para obtener más información, consulte *iDRACRACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos iDRACRACADM) disponible en **dell.com/idracmanuals**.

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.

Carga del certificado de CA de confianza para tarjeta inteligente mediante la interfaz web

Para cargar el certificado de CA de confianza para el inicio de sesión mediante tarjeta inteligente:

1 En la interfaz web de iDRAC, vaya a **Configuración de iDRAC** > **Red** > **Autenticación de usuario** > **Usuarios locales**.
Se muestra la página **Users (Usuarios)**.
2 En la columna **Identificación de usuario**, haga clic en un número de identificación de usuario.

Aparece la página **Menú principal de usuarios**.

3 En **Configuraciones de tarjeta inteligente**, seleccione **Cargar certificado de CA de confianza** y haga clic en **Siguiente**.

Aparece la página **Carga del certificado de CA de confianza**.

4 Busque y seleccione el certificado de CA de confianza y haga clic en **Aplicar**.

Carga del certificado de CA de confianza para tarjeta inteligente mediante RACADM

Para cargar el certificado de CA de confianza para el inicio de sesión mediante tarjeta inteligente, utilice el objeto **usercertupload**. Para obtener más información, consulte *iDRAC RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM de iDRAC), disponible en **dell.com/idracmanuals**.

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

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

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

1 En la interfaz web de iDRAC, al configurar Active Directory para establecer una cuenta de usuario basada en el esquema estándar o el esquema extendido, en la página **Paso 1 de 4 de Configuración y administración de Active Directory** realice lo siguiente:

- Active la validación de certificados.
- Cargue un certificado firmado por la CA de confianza.
- Cargue el archivo keytab.

2 Active el inicio de sesión mediante tarjeta inteligente. Para obtener más información acerca de estas opciones, consulte la *Ayuda en línea de iDRAC*.

Activación o desactivación del inicio de sesión mediante tarjeta inteligente

Antes de activar o desactivar el inicio de sesión mediante tarjeta inteligente para iDRAC, asegúrese de haber realizado lo siguiente:

- Configurar los permisos iDRAC.
- Completar la configuración de usuario local de iDRAC o la configuración de usuario de Active Directory con los certificados adecuados.

NOTA: Si el inicio de sesión mediante tarjeta inteligente está activado, SSH, Telnet, IPMI por LAN, Comunicación en serie por LAN y RACADM remoto quedan desactivados. Si desactiva el inicio de sesión mediante tarjeta inteligente, las interfaces no se activan automáticamente.

Activación o desactivación del inicio de sesión mediante tarjeta inteligente utilizando la interfaz web

Para activar o desactivar la función de inicio de sesión mediante tarjeta inteligente:

1 En la interfaz web de iDRAC, vaya a **Configuración de iDRAC** > **Usuarios** > **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 sobre las opciones, consulte la *Ayuda en línea de iDRAC*.

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

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

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

Para activar el inicio de sesión mediante tarjeta inteligente, utilice el comando **set** con objetos en el grupo **iDRAC.SmartCard**.

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

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 **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**.

La función de inicio de sesión mediante tarjeta inteligente se activa o desactiva según la opción seleccionada.

10

Configuración de iDRAC para enviar alertas

Es posible configurar alertas y acciones para ciertos sucesos que se producen en el sistema administrado. Un suceso se produce cuando el estado de un componente del sistema es mayor que la condición definida previamente. Si un suceso coincide con un filtro de sucesos y ha configurado este filtro para que genere una alerta (correo electrónico, captura SNMP, alerta IPMI, registros del sistema remoto, suceso de Redfish o sucesos de WS), se envía una alerta a uno o más destinos configurados. Si el mismo filtro de sucesos también está configurado para ejecutar una acción (como reiniciar, ciclo de encendido o apagar el sistema), la acción se ejecuta. Puede establecer solamente una acción para cada suceso.

Si desea configurar iDRAC para enviar alertas:

1 Active las alertas.
2 De manera opcional, puede filtrar las alertas en función de la categoría o la gravedad.
3 Configure los valores de alerta por correo electrónico, alerta IPMI, captura SNMP, registro del sistema remoto, suceso de Redfish, registro del sistema operativo y/o sucesos de WS.
4 Active las alertas y las acciones de suceso, como por ejemplo:
   - Envíe una alerta por correo electrónico, alerta IPMI, capturas SNMP, registros del sistema remoto, suceso de Redfish, registro del sistema operativo o sucesos de WS a los destinos configurados.
   - Realice un reinicio, un apagado o un ciclo de encendido del sistema administrado.

Temas:

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.

Activación o desactivación de alertas mediante la interfaz web

Para activar o desactivar la generación de alertas:

1 En la interfaz web de iDRAC, vaya a **Configuración** > **Configuración del sistema** > **Configuración de alerta**.
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

Utilice el comando siguiente:

```
racadm set iDRAC.IPMILan.AlertEnable <n>
```

n=0: Inhabilitado

n=1: Habilitado

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 **Platform Events (Sucesos de plataforma)**, seleccione **Enabled (Activado)** para activar la generación de alertas o las acciones de suceso. De lo contrario, seleccione **Desactivado**. Para obtener más información acerca de las opciones, consulte *iDRAC Settings Utility Online Help (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.

Filtrado de alertas mediante la interfaz web de iDRAC

Para filtrar alertas en función de la categoría o la gravedad:

NOTA: Es posible filtrar alertas incluso con privilegios de solo lectura.

1 En la interfaz web de iDRAC, vaya a **Configuración** > **Configuración del sistema** > **Configuración de alertas y registro del sistema remoto**.

2 En la sección **Configuración de alertas y registro del sistema remoto**, seleccione **Filtro**:

- Estado del sistema: la categoría Estado del sistema representa todas las alertas relacionadas con el hardware dentro del chasis del sistema. Algunos ejemplos incluyen errores de temperatura, errores de voltaje, errores de dispositivo.
- Estado del almacenamiento: la categoría Estado del almacenamiento representa las alertas que se relacionan con el subsistema de almacenamiento. Los ejemplos incluyen, errores de controladora, errores de discos físicos, errores de discos virtuales.
- Configuración: la categoría Configuración representa alertas relacionadas con los cambios de configuración del hardware, el firmware y el software. Algunos ejemplos incluyen, tarjeta PCI-e agregada/extraída, configuración de RAID modificada, licencia de iDRAC modificada.
- Auditoría: la categoría Auditoría representa el registro de auditoría. Los ejemplos incluyen, información de inicio/cierre de sesión del usuario, fallas de autenticación de la contraseña, información de la sesión, estados de la alimentación.
- Actualizaciones: la categoría Actualización representa alertas que se generan debido a actualizaciones/regresos a versiones anteriores de firmware/controladores.

NOTA: Esto no representa el inventario de firmware.

- Notas de trabajo

3 Seleccione uno o más de los niveles de gravedad siguientes:
   - Informativo
   - 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 *iDRAC RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM de iDRAC), disponible en **dell.com/idracmanuals**.

Configuración de alertas de suceso

Puede configurar alertas de sucesos como alertas por correo electrónico, alertas IPMI, capturas SNMP, registros del sistemas remoto, registros del sistema operativo y sucesos WS para que se envíen a los destinos configurados.

Configuración de alertas de suceso mediante la interfaz web

Para establecer una alerta de suceso mediante la interfaz web:

1 Asegúrese de tener configuradas las alertas por correo electrónico, las alertas IPMI, las capturas SNMP y/o los parámetros de registro del sistema remoto.
2 En la interfaz web de iDRAC, vaya a **Configuración** > **Configuración del sistema** > **Configuración de alertas y registro del sistema remoto**.
3 En **Categoría**, seleccione una o todas las siguientes alertas para los sucesos necesarios:
   - Correo electrónico
   - Captura SNMP
   - Alerta IPMI
   - Registro del sistema remoto
   - Sucesos de WS
   - Registro del sistema operativo
   - Suceso de Redfish
4 Seleccione **Acción**.

   La configuración se guarda.
5 De manera opcional, puede enviar un suceso de prueba. En el campo **ID de mensaje para suceso de prueba**, introduzca la identificación de mensajes para probar si la alerta está generada y haga clic en **Probar**. Para la lista de identificaciones de mensajes, consulte la *Guía de mensajes de eventos* disponible en **dell.com/support/manuals**.

Configuración de alertas de suceso mediante RACADM

Para establecer alertas de suceso, utilice el comando **eventfilters**. Para obtener más información, consulte *iDRAC RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM de iDRAC), disponible en **dell.com/idracmanuals**.

Configuración de suceso de periodicidad de alertas

Puede configurar iDRAC para generar sucesos adicionales en intervalos específicos si el sistema continúa funcionando a una temperatura mayor que el límite de umbral de temperatura de entrada. El intervalo predeterminado es de 30 días. El rango válido es de 0 a 366 días. Un valor de 0 indica que la periodicidad de sucesos no está activada.

NOTA: Debe tener privilegio para configurar iDRAC para que establezca el valor de periodicidad de alertas.

Configuración de sucesos de periodicidad de alertas mediante RACADM

Para configurar el suceso de periodicidad de alertas mediante RACADM, utilice el comando **eventfilters**. Para obtener más información, consulte *iDRAC RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM de iDRAC), disponible en **dell.com/idracmanuals**.

Configuración de sucesos de periodicidad de alertas mediante la interfaz web de iDRAC

Para configurar el valor de periodicidad de alertas:

1 En la interfaz web de iDRAC, vaya a **Configuración** > **Configuración del sistema** > **Periodicidad de alertas**.
2 En la columna **Periodicidad**, introduzca el valor de frecuencia de alertas para la categoría, alerta y tipos de gravedad requeridos.
Para obtener más información, consulte la *Ayuda en línea de iDRAC*.
3 Haga clic en **Aplicar**.
Se guarda la configuración de periodicidad de alertas.

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.

Configuración de acciones del suceso mediante la interfaz web

Para configurar una acción de suceso:

1 En la interfaz web de iDRAC, vaya a **Configuración** > **Configuración del sistema** > **Configuración de alertas y registro del sistema remoto**.
2 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 medida de suceso, utilice el comando **eventfilters**. Para obtener más información, consulte *iDRAC RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM de iDRAC), disponible en **dell.com/idracmanuals**.

Configuración de alertas por correo electrónico, capturas SNMP o capturas IPMI

La estación de alimentación utiliza capturas de Protocolo simple de administración de red (SNMP) y de Interfaz de administración de plataforma inteligente (IPMI) para recibir datos de iDRAC. Para los sistemas con un gran número de nodos, es posible que no sea eficiente que una estación de administración sondee cada iDRAC para cada condición que pueda producirse. Por ejemplo, las capturas de suceso pueden ayudar a una estación de administración con el equilibrio de carga entre nodos o emitiendo una alerta si se produce un fallo de autentificación. Se admiten los formatos v1, v2 y v3 de SNMP.

Es posible configurar destinos de alerta IPv4 e IPv6, valores de correo electrónico y valores del servidor SMTP y después probar la configuración. También puede especificar el usuario SNMP v3 al que desea enviar las capturas SNMP.

Antes de configurar los valores de correo electrónico o capturas SNMP/IPMI, asegúrese de lo siguiente:

- Dispone de permisos Configurar el RAC.
- Ha configurado los filtros de sucesos.

Configuración de destinos de alerta IP

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

Para obtener más información sobre los MIB de iDRAC necesarios para supervisar los servidores por medio de SNMP, consulte la *Guía de referencia de SNMP* disponible en **dell.com/support/manuals**.

Configuración de destinos de alerta IP mediante la interfaz web

Para configurar destinos de alerta mediante la interfaz web:

1 En la interfaz web de iDRAC, vaya a **Configuración** > **Configuración del sistema** > **Configuración de SNMP y correo electrónico** .

2 Seleccione la opción **Estado** para activar un destino de alerta [dirección IPv4, dirección IPv6 o nombre de dominio completo (FQDN)] para recibir las capturas.

Es posible especificar hasta ocho direcciones de destino. Para obtener más información sobre las opciones, consulte la *Ayuda en línea de iDRAC*.

3 Seleccione el usuario SNMP v3 al que desea enviar la captura SNMP.

4 Introduzca la cadena de comunidad SNMP de iDRAC (solo se aplica a SNMPv1 y SNMPv2) y el número de puerto de la alerta SNMP.

Para obtener más información sobre las opciones, consulte la *Ayuda en línea de iDRAC*.

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

5 Para comprobar que la dirección IP está recibiendo las capturas IPMI o SNMP, haga clic en **Enviar** bajo **Probar captura IPMI** y **Probar captura SNMP**, respectivamente.

6 Haga clic en **Aplicar**.

Se configurarán los destinos de alerta.

7 En la sección **Formato de captura SNMP**, seleccione la versión de protocolo que se utilizará para enviar las capturas en los destinos de captura: **SNMP v1**, **SNMP v2** o **SNMP v3**, y haga clic en **Aplicar**.

NOTA: La opción Formato de captura SNMP se aplica solo a capturas SNMP y no a capturas IPMI. Las capturas IPMI siempre se envían en formato SNMP v1 y no se basan en la opción Formato de captura SNMP configurada.

Se configurará el formato de captura SNMP.

Configuración de destinos de alerta IP mediante RACADM

Para configurar los valores de alerta de captura, siga los pasos siguientes:

1 Para activar capturas:

```
racadm set idrac.SNMP.Alert.<index>.Enable <n>
```

Parámetro	Descripción
<index>	Índice del destino. Los valores permitidos son del 1 al 8.
<n>=0	Desactivar la captura
<n>=1	Activar la captura

2 Para configurar la dirección de destino de la captura, siga los pasos siguientes:

```
racadm set idrac.SNMP.Alert.<index>.DestAddr <Address>
```

Parámetro	Descripción
<index>	Índice del destino. Los valores permitidos son del 1 al 8.
<Address>	Una dirección IPv4, IPv6 o FQDN válida

3 Configure la cadena de nombre de comunidad SNMP:

```
racadm set idrac.ipmilan.communityname <community_name>
```

Parámetro	Descripción
<community_name>	El nombre de la comunidad SNMP.

4 Para configurar un destino de SNMP:

- Configure el destino de la captura de SNMP para SNMPv3:

  ```
  racadm set idrac.SNMP.Alert.<index>.DestAddr <IP address>
  ```

- Configure los usuarios de SNMPv3 para los destinos de captura:

  ```
  racadm set idrac.SNMP.Alert.<index>.SNMPv3Username <user_name>
  ```

- Active SNMPv3 para un usuario:

  ```
  racadm set idrac.users.<index>.SNMPv3Enable Enabled
  ```

5 Para probar la captura, si fuera necesario:

```
racadm testtrap -i <index>
```

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

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

Es posible configurar destinos de alerta (IPv4, IPv6 o FQDN) mediante la utilidad de configuración de iDRAC. Para hacerlo:

1 En la **utilidad de configuración de iDRAC**, vaya a **Alertas**.

Aparece la pantalla **Alertas de configuración de iDRAC**.

2 En **Valores de captura**, active las direcciones IP para recibir las capturas e introduzca las direcciones de destino IPv4, IPv6 o FQDN. Puede especificar hasta ocho direcciones.

3 Introduzca el nombre de la cadena de comunidad.

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

4 Haga clic en **Atrás**, en **Terminar** y, a continuación, en **Sí**.

Se configurarán los destinos de alerta.

Configuración de los valores de alertas por correo electrónico

Puede configurar la dirección de correo electrónico en la cual recibir alertas por correo electrónico. Asimismo, puede configurar los valores de la dirección del servidor SMTP.

NOTA: Si el servidor de correo es Microsoft Exchange Server 2007, compruebe que el nombre de dominio de iDRAC está configurado para que el servidor de correo reciba alertas por correo electrónico desde iDRAC.

NOTA: Las alertas por correo electrónico admiten las direcciones IPv4 e IPv6. Al utilizar IPv6, se debe especificar el Nombre de dominio DNS de DRAC.

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 En la interfaz web de iDRAC, vaya a **Configuración** > **Configuración del sistema** > **Configuración de SMTP (correo electrónico)**.

2 Introduzca una dirección de correo electrónico válida.

3 Haga clic en **Enviar** en **Probar correo electrónico** para probar los valores de alerta por correo electrónico configurados.

4 Haga clic en **Aplicar**.

5 Para la configuración del servidor SMTP (correo electrónico) proporcione los siguientes detalles:

- Dirección IP de servidores de correo electrónico SMTP o nombre de FQDN o DNS
- Número de puerto SMTP
- Autentificación
- Nombre de usuario

6 Haga clic en **Aplicar**. Para obtener más información sobre las opciones, consulte la *Ayuda en línea de iDRAC*.

Configuración de los valores de alerta por correo electrónico mediante RACADM

1 Para activar alertas por correo electrónico:

```
racadm set iDRAC.EmailAlert.Enable.[index] [n]
```

Parámetro	Descripción
`index`	Índice de destino del correo electrónico. Los valores permitidos son del 1 al 14.
`n=0`	Inhabilita las alertas de correo electrónico.
`n=1`	Habilita las alertas de correo electrónico.

2 Para configurar los valores de correo electrónico:

```
racadm set iDRAC.EmailAlert.Address.[index] [email-address]
```

Parámetro	Descripción
index	Índice de destino del correo electrónico. Los valores permitidos son del 1 al 14.
email-address	Dirección de correo electrónico de destino que recibe las alertas de eventos de la plataforma.

3 Para configurar un mensaje personalizado:

```
racadm set iDRAC.EmailAlert.CustomMsg.[index] [custom-message]
```

Parámetro	Descripción
index	Índice de destino del correo electrónico. Los valores permitidos son del 1 al 14.
custom-message	Mensaje personalizado

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

```
racadm testemail -i [index]
```

Parámetro	Descripción
index	Índice de destino del correo electrónico que se debe probar. Los valores permitidos son del 1 al 14.

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

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

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

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

Para configurar la dirección del servidor SMTP:

1 En la interfaz web de iDRAC, vaya a **Configuración** > **Configuración del sistema** > **Configuración de alertas** > **SNMP (Configuración de correo electrónico)**.

2 Introduzca la dirección IP válida o el nombre de dominio completamente calificado (FQDN) del servidor SMTP que se va a usar en la configuración.

3 Seleccione la opción **Activar autenticación** y, a continuación, proporcione el nombre de usuario y la contraseña (de un usuario que tenga acceso al servidor SMTP).

4 Introduzca el número de puerto SMTP.

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

5 Haga clic en **Aplicar**.

Se habrán configurado los valores de SMTP.

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

Para configurar el servidor de correo electrónico SMTP:

```
racadm set iDRAC.RemoteHosts.SMTPServerIPAddress <SMTP E-mail Server IP Address>
```

Configuración de sucesos de WS

El protocolo de Sucesos de WS se utiliza para que un servicio de cliente (suscriptor) registre el interés (suscripción) en un servidor (fuente de sucesos) para recibir mensajes que contienen los sucesos del servidor (notificaciones o mensajes de sucesos). Los clientes interesados en recibir los mensajes de sucesos de WS pueden suscribirse en iDRAC y recibir sucesos relacionados con trabajos de Lifecycle Controller.

Los pasos necesarios para configurar la función de sucesos de WS para recibir mensajes de sucesos de WS para cambios relacionados con trabajos de Lifecycle Controller se describen en el documento con especificaciones de Soporte de sucesos de servicios web para iDRAC 1.30.30 . Además de esta especificación, consulte el documento DSP0226 (Especificación de administración de WS DMTF), sección 10 Notificaciones (Sucesos), para obtener la información completa sobre el protocolo de sucesos de WS. Los trabajos relacionados con Lifecycle Controller se describen en el documento de Perfil de control de trabajos de DCIM.

Configuración de sucesos de Redfish

El protocolo de sucesos de Redfish se utiliza para que un servicio cliente (suscriptor) registre el interés (suscripción) en un servidor (fuente de sucesos) para recibir mensajes con los eventos de Redfish (notificaciones o mensajes de sucesos). Los clientes interesados en recibir los mensajes de sucesos de Redfish pueden suscribirse en iDRAC y recibir sucesos relacionados con trabajos de Lifecycle Controller.

Supervisión de sucesos del chasis

En el chasis PowerEdge FX2/FX2s, puede activar la configuración **Administración y supervisión del chasis** en el iDRAC para realizar las tareas de administración y supervisión del chasis, como la supervisión de componentes del chasis, la configuración de alertas, el uso de RACADM de iDRAC para pasar comandos de RACADM de la CMC y la actualización del firmware de administración del chasis. Esta configuración le permite administrar los servidores en el chasis, incluso si la CMC no se encuentra en la red. Puede definir el valor como **Desactivado** para reenviar los sucesos del chasis. De manera predeterminada, este valor se establece como **Habilitado**.

NOTA: Para que esta configuración surta efecto, debe asegurarse de que en la CMC, el valor Administración de chasis en el servidor está establecido en Supervisar o Administrar y supervisar.

Cuando la opción **Administración y supervisión del chasis** se establece como **Activada**, iDRAC genera y registra sucesos del chasis. Los sucesos generados se integran en el subsistema de sucesos de iDRAC y se generan alertas de manera similar al resto de los sucesos.

La CMC también reenvía los sucesos generados a iDRAC. Si el iDRAC del servidor no funciona, la CMC deja en cola los primeros 16 sucesos y registra el resto en el registro de CMC. Estos 16 sucesos se envían a iDRAC tan pronto como la **Supervisión del chasis** se establezca como habilitada.

En instancias donde iDRAC detecta que una funcionalidad requerida de la CMC está ausente, aparece un mensaje de advertencia que informa que ciertas funciones podrían no estar en funcionamiento sin una actualización de firmware de la CMC.

Supervisión de sucesos del chasis mediante la interfaz web de iDRAC

Para supervisar los sucesos del chasis mediante la interfaz web de iDRAC, realice los pasos siguientes:

NOTA: Esta sección aparece solo para chasis PowerEdge FX2/FX2s y si Administración de chasis en el servidor está establecida en Supervisar o Administrar y supervisar en la CMC.

1. En la interfaz de la CMC, haga clic en **Descripción general del chasis** > **Configuración** > **General**.
2. En el menú desplegable **Modo administración de chasis en modo de servidor**, seleccione **Administrar y supervisar** y haga clic en **Aplicar**.
3. Inicie la interfaz web de iDRAC, haga clic en **Descripción general** > **Configuración de iDRAC** > **CMC**.
4. En la sección **Administración de chasis en el servidor**, asegúrese de que el cuadro desplegable **Capacidad de iDRAC** está configurado en **Activado**.

Supervisión de sucesos del chasis mediante RACADM

Esta configuración solo se aplica a los servidores PowerEdge FX2/FX2s y si **Administración de chasis en el servidor** está establecida en **Supervisar** o **Administrar y supervisar** en la CMC.

Para supervisar los eventos del chasis mediante RACADM de iDRAC:

```
racadm get system.chassiscontrol.chassismanagementmonitoring
```

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

Id. de mensaje de alertas

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

Tabla 30. Id. de mensaje de alertas

Id. de mensaje	Descripción
AMP	Amperage
ASR	Restablecimiento automático del sistema
BAR	Copia de seguridad/restauración
BAT	Suceso de la batería
BIOS	Administración del BIOS
BOOT	Control BOOT
CBL	Cable
CPU	Procesador
CPUA	Procesador ausente
CTL	Controladora de almacenamiento
DH	Administración de certificados
DIS	Descubrimiento automático
ENC	Gabinete de almacenamiento
FAN	Suceso de ventilador
FSD	Depuración
HWC	Configuración de hardware
IPA	Cambio de IP de DRAC
ITR	Intrusión
JCP	Control de trabajos
LC	Lifecycle Controller
LIC	Licencias

Id. de mensaje	Descripción
LNK	Estado de vínculo
LOG	Suceso del registro
MEM	Memoria
NDR	Controlador de SO de NIC
NIC	Configuración de NIC
OSD	Implementación de SO
OSE	Suceso del sistema operativo
PCI	Dispositivo PCI
PDR	Disco físico
PR	Intercambio de piezas
PST	POST del BIOS
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
Registro de sucesos del sistema	Registro de sucesos del sistema
SRD	RAID de software
SSD	SSD PCIe
STOR	En almacenamiento
SUP	Trabajo de actualización del firmware

Id. de mensaje	Descripción
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	Soportes virtuales
VRM	Consola virtual
WRK	Nota de trabajo

11

Group Manager de iDRAC 9

La función Group Manager de iDRAC está disponible para servidores Dell de la 14ª generación para ofrecer una administración básica simplificada de los iDRAC y servidores asociados en los servidores asociados en la red local mediante la GUI del iDRAC. Group Manager permite una experiencia de consola 1XMany sin implicar una aplicación independiente. Permite a los usuarios ver los detalles de un conjunto de servidores, permitiendo una administración más sólida que por medio de la inspección visual de los servidores en busca de fallas y demás métodos manuales.

Group Manager es una función con licencia y forma parte de la licencia Enterprise. Solo los usuarios administrativos de iDRAC pueden acceder a la función Group Manager.

NOTA: Para obtener una mejor experiencia del usuario, Group Manager admite hasta 100 nodos de servidor.

Temas:

Group Manager

Para utilizar la función **Group Manager**, necesita activar el **Group Manager** desde la página de índice de iDRAC o en la pantalla de Bienvenida de Group Manager. La pantalla de bienvenida de Group Manager ofrece opciones enumeradas en la tabla siguiente.

Opción	Descripción
Unirse a un grupo existente	Le permite unirse a un grupo existente. Debe conocer el **GroupName** y el **Código de acceso** para unirse a un grupo específico. **NOTA: Las contraseñas están asociadas a las credenciales de usuario de iDRAC. Mientras que un código de acceso se asocia a un grupo para establecer comunicación con los dispositivos autenticados entre los diferentes iDRAC en el mismo grupo.**
Crear grupo nuevo	Le permite crear un nuevo grupo. El iDRAC específico que ha creado el grupo debería ser el maestro (controladora principal) del grupo.

Opción	Descripción
Desactivar Group Manager para este sistema	Puede seleccionar esta opción en caso de que no desee unirse a ningún grupo desde un sistema específico. Sin embargo, puede acceder a Group Manager en cualquier momento seleccionando Abrir Group Manager desde la página de índice de iDRAC. Una vez que desactiva el Group Manager, el usuario debe esperar 60 segundos para realizar más operaciones de Group Manager.

Una vez que la función Group Manager está activada, el iDRAC le permite crear, o unirse a, un grupo local de iDRAC. En la red local se puede configurar más de un grupo de iDRAC, pero un iDRAC individual solo puede ser miembro de un grupo por vez. Para cambiar de grupo (unirse a un grupo nuevo), el iDRAC debe primero salir de su grupo actual, y luego, unirse al grupo nuevo. El iDRAC desde el cual se creó el grupo se elige como la controladora principal del grupo de manera predeterminada. El usuario no define una controladora principal de Group Manager dedicado para controlar ese grupo. La controladora principal aloja la interfaz web del Group Manager y proporciona los flujos de trabajo basados en la GUI. Los miembros de iDRAC seleccionan por su cuenta una nueva controladora primaria para el grupo si la controladora principal actual queda fuera de línea durante un tiempo prolongado, pero no causa ningún impacto en el usuario final. Generalmente, puede acceder al Group Manager desde todos los miembros de iDRAC haciendo clic en Group Manager desde la página de índice de iDRAC.

Vista de resumen

Debe tener privilegios de administrador para acceder a las páginas del Group Manager. Si un usuario que no sea administrador inicia sesión en el iDRAC, la sección de Group Manager no aparece con sus credenciales. La página de inicio del Group Manager (vista de resumen) se clasifica generalmente en tres secciones. La primera sección muestra el resumen de consolidación con detalles de resumen adicionales.

- El número total de servidores del grupo local.
- Gráfico que muestra el número de servidores por modelo de servidor.
- Gráfico de anillos que muestra los servidores según su estado (al hacer clic en una sección de gráfico se filtra la lista de servidores para mostrar solo los servidores en buen estado seleccionados).
- Aparece un cuadro de aviso si se detectó un grupo duplicado en la red local. Generalmente, el grupo duplicado es el grupo con el mismo nombre pero con diferente código de acceso. Este cuadro de aviso no aparece si no hay un grupo duplicado.
- Muestra los iDRAC que están controlando el grupo (controladora primaria y secundaria).

La segunda sección proporciona botones para las medidas que se toman en el grupo en su conjunto y la tercera sección muestra la lista de todos los iDRAC en el grupo.

Muestra todos los sistemas del grupo y su estado actual, y permite que el usuario tome las medidas correctivas oportunas según sea necesario. En la siguiente tabla se describen los atributos específicos de un servidor.

Atributo de servidor	Descripción
Condición	Indica el estado de condición de ese servidor específico.
Nombre del host	Muestra el nombre del servidor.
Dirección IP del iDRAC	Muestra las direcciones IPV4 e IPV6 exactas.
Service Tag	Muestra la información de la etiqueta de servicio.
Modelo	Muestra el número de modelo del servidor Dell.
iDRAC	Muestra la versión del iDRAC.
Última actualización de estado	Muestra la marca de tiempo en que el estado del servidor se actualizó por última vez.

El panel de información del sistema proporciona más detalles sobre el servidor como el estado de conectividad de red de iDRAC, el estado de energía del host del servidor, el código de servicio rápido, el sistema operativo, la etiqueta de propiedad, el ID de nodo, el nombre de DNS del IDRAC, la versión del BIOS del servidor, la información de CPU del servidor, la memoria del sistema y la información de la ubicación. Puede hacer doble clic en una fila o hacer clic en el botón de inicio de iDRAC para realizar un único redireccionamiento de inicio de sesión a

la página del índice de iDRAC seleccionado. En el servidor seleccionado, se puede acceder a la consola virtual o se pueden tomar medidas de energía del servidor de la lista desplegable Más acciones.

Las acciones de grupo admitidas son Administrar los inicios de sesión de los usuarios de iDRAC, la Configuración de alertas y la Exportación del inventario de grupos.

Administrar los inicios de sesión

Use esta sección para **Agregar nuevo usuario**, **Cambiar contraseña del usuario** y **Eliminar usuario** del grupo.

Los trabajos de grupo, incluida la Administración de inicios de sesión son configuraciones únicas de los servidores. El Administrador de grupo utiliza SCP y trabajos para realizar los cambios necesarios. Cada iDRAC de grupo posee un trabajo individual en su cola de trabajos para cada trabajo del Administrador de grupo. El Administrador de grupo no detecta cambios en los iDRAC de miembros o las configuraciones de bloqueo de miembros.

NOTA: Los trabajos de grupo no configuran ni anulan el modo de bloqueo para ningún iDRAC específico.

Dejar un grupo no cambia la configuración de alteración de usuario local o correo electrónico en un miembro de iDRAC.

Agregar un nuevo usuario

Use esta sección para crear y agregar un nuevo perfil de usuario en todos los servidores de dicho grupo. Se crearía un trabajo de grupo para agregar el usuario a todos los servidores de ese grupo. El estado del trabajo de grupo se puede encontrar en la página de > **Trabajos del administrador de grupo**.

NOTA: De manera predeterminada, iDRAC está configurado con una cuenta de administrador local. Puede acceder a información adicional sobre cada parámetro con la cuenta de administrador local.

Para obtener más información, consulte Configuración de cuentas y privilegios del usuario.

Opción	Descripción
Información de nuevo usuario	Le permite proporcionar información del nuevo usuario.
Permisos de iDRAC	Le permite definir el rol del usuario para uso futuro.
Configuración avanzada de usuarios	Permite establecer (IPMI) los privilegios de usuario y ayuda a activar SNMP.

NOTA: Cualquier iDRAC de miembro con bloqueo de sistema activado que forma parte del mismo grupo arroja el error de que la contraseña del usuario no se ha actualizado.

Cambiar contraseña de usuario

Use esta sección para cambiar la información de contraseña para el usuario. Puede ver la información de **Nombre de usuario**, **Rol** y **Dominio** de cada **Usuario** individual. Se crearía un trabajo de grupo para cambiar la contraseña del usuario en todos los servidores de ese grupo. El estado del trabajo de grupo se puede encontrar en la página de > **Trabajos del administrador de grupo**.

Si el usuario ya existe, la contraseña se puede actualizar. Cualquier iDRAC de miembro con bloqueo de sistema activado que forma parte del grupo arroja el error de que la contraseña del usuario no se ha actualizado. Si el usuario no existe, se informa un error al administrador de grupo que indica que el usuario no existe en el sistema. La lista de usuarios que se muestra en la GUI del Administrador de grupo está basada en la lista de usuarios actuales en el iDRAC que está actuando como controlador principal. No muestra todos los usuarios para todos los iDRAC.

Eliminar usuario

Use esta sección para eliminar usuarios de todos los servidores de grupo. Se crearía un trabajo de grupo para eliminar usuarios de todos los servidores de grupo. El estado del trabajo de grupo se puede encontrar en la página de > **Trabajos del administrador de grupos**.

Si el usuario ya existe en un iDRAC de miembro, se puede eliminar el usuario. Cualquier iDRAC de miembro con bloqueo de sistema activado que forma parte del grupo arroja el error de que el usuario no fue eliminado. Si el usuario no existe, se muestra una correcta eliminación para ese iDRAC. La lista de usuarios que se muestra en la GUI del Administrador de grupo está basada en la lista de usuarios actuales en el iDRAC que está actuando como controlador principal. No muestra todos los usuarios para todos los iDRAC.

Configuración de alertas

Use esta sección para configurar alertas por correo electrónico. Las alertas están desactivadas de manera predeterminada. Sin embargo, puede habilitarlas en cualquier momento. Se crea un grupo de trabajo para aplicar la configuración de alerta por correo electrónico a todos los servidores del grupo. El estado del trabajo de grupo se puede monitorear en la página **GroupManager** > **Trabajos** . La alerta por correo electrónico del administrador de grupo configura las alertas por correo electrónico en todos los miembros. Configura los valores del servidor SMTP en todos los miembros en el mismo grupo. Cada iDRAC está configurado por separado. La configuración por correo electrónico no está guardada globalmente. Los valores actuales se basan en el iDRAC que está actuando como controladora primaria. Al dejar un grupo, no se vuelven a configurar las alertas por correo electrónico.

Para obtener más información sobre la configuración de las alertas, consulte Configuración de iDRAC para enviar alertas.

Opción	Descripción
Configuración de la dirección del servidor SMTP (correo electrónico)	Le permite configurar la Dirección IP del servidor y el número de puerto de SMTP, como también activar la autenticación. En caso de estar habilitando la autenticación, debe proporcionar el nombre de usuario y la contraseña.
Direcciones de correo electrónico	Le permite configurar varias ID de correo electrónico para recibir notificaciones por correo electrónico sobre la modificación del estado del sistema. Puede enviar un correo electrónico de prueba a la cuenta configurada del sistema.
Categorías de alertas	Le permite seleccionar varias categorías de alertas para recibir notificaciones por correo electrónico.

NOTA: Cualquier miembro de iDRAC con bloqueo del sistema activado, el cual forma parte del mismo grupo, arroja un error de que la contraseña del usuario no se ha actualizado.

Exportar

Use esta sección para exportar el Resumen del grupo en el sistema local. La información se puede exportar a un formato de archivo csv. Este contiene datos relacionados con cada sistema en particular en el grupo. La exportación incluye la siguiente información en formato csv. Detalles del servidor:

- Condición
- Nombre del host
- Dirección IPV4 del iDRAC
- Dirección IPV6 del iDRAC
- Asset Tag
- Modelo
- Versión del firmware del iDRAC

- Última actualización de estado
- Código de servicio rápido
- Conectividad de iDRAC
- Estado de la alimentación
- Sistema operativo
- Service Tag
- ID del nodo
- Nombre DNS de iDRAC
- Versión del BIOS
- Detalles de CPU
- Memoria del sistema (MB)
- Detalles de la ubicación

NOTA: En caso de utilizar Internet Explorer, se debe desactivar la configuración de seguridad mejorada para descargar correctamente el archivo csv.

Vista de servidores detectados

Después de crear el grupo local, el Group Manager de iDRAC notifica a los demás iDRAC en la red local de que se ha creado un nuevo grupo. Para que los iDRAC aparezcan en servidores detectados, la función del Group Manager debe estar habilitada en cada iDRAC. La vista de servidores detectados muestra la lista de los iDRAC detectados en la misma red, que pueden formar parte de cualquier grupo. Si el iDRAC no aparece en la lista de sistemas detectados, el usuario debe iniciar sesión en el iDRAC específico y unirse al grupo. El iDRAC que creó el grupo aparecerá como el único miembro de la vista Essentials hasta que más iDRAC se unan al grupo.

NOTA: La vista de servidores detectados en la consola del Group Manager le permite incorporar uno o más servidores mostrados en la vista de ese grupo. Se puede realizar un seguimiento del progreso de la actividad de GroupManager > Trabajos. De manera alternativa, puede iniciar sesión en el iDRAC y seleccionar el grupo que desea integrar de la lista desplegable para unirse a ese grupo. Puede acceder a la pantalla de bienvenida del GroupManager desde la página de índice de iDRAC.

Opción	Descripción
Incorporación y cambio de inicio de sesión	Seleccione una fila específica y seleccione la opción de Incorporación y cambio de inicio de sesión para enviar los sistemas descubiertos recientemente al grupo. Debe proporcionar las credenciales de inicio de sesión del administrador para que los nuevos sistemas se unan al grupo. Si el sistema tiene la contraseña predeterminada, necesita cambiarlo al tiempo que lo incorpora a un grupo. La incorporación de grupos le permite aplicar la misma configuración de alertas de grupo a los nuevos sistemas.
Ignorar	Permite ignorar los sistemas de la lista de servidores detectados, en caso de que no desee agregarlos a ningún grupo.
Cancelar ignorar	Permite seleccionar los sistemas que desea reactivar en la lista de servidores detectados.
Volver a explorar	Permite explorar y generar la lista de servidores detectados en cualquier momento.

Vista Jobs (Trabajos)

Vista Jobs (Trabajos) le permite al usuario realizar el seguimiento del progreso de un grupo trabajo y lo ayuda con la recuperación simple para corregir los errores inducidos por la conectividad. También muestra el historial de las últimas acciones de grupos que se han realizado como registro de auditoría. El usuario puede utilizar la Vista Jobs (Trabajos) para realizar un seguimiento del progreso de la acción en el

grupo o para cancelar una acción programada para llevarse a cabo en el futuro. La vista Trabajos permite al usuario ver el estado de los últimos 50 trabajos que se han ejecutado y de las acciones correctas e incorrectas que se han producido.

Opción	Descripción
Estado	Muestra el estado del trabajo y el estado del trabajo en curso.
Trabajo	Muestra el nombre del trabajo.
ID	Muestra la ID del trabajo.
Hora de inicio	Muestra la hora de inicio.
Hora de finalización	Muestra la hora de finalización.
Acciones	• Cancelar: un trabajo programado se puede cancelar antes de que pase al estado de ejecución. Un trabajo en ejecución se puede detener mediante el uso del botón Stop (Detener). • Volver a ejecutar: permite al usuario volver a ejecutar el trabajo si este se encuentra en estado de falla. • Quitar: permite al usuario quitar los trabajos anteriores completados.
Exportar	Puede exportar la información del trabajo del grupo al sistema local para futuras referencias. La lista de trabajos se puede exportar a un formato de archivo csv. Este contiene datos relacionados con el trabajo individual.

NOTA: Para cada entrada de trabajo, la lista de sistemas proporciona detalles de hasta 100 sistemas. Cada entrada de los sistemas contiene Nombre de host, Etiqueta de servicio, Estado del trabajo del miembro y Mensaje, en caso de que fallara el trabajo.

Todas las acciones de grupos que crean trabajos se llevan en todos los miembros del grupo con efecto inmediato. Es posible puede realizar las siguientes tareas:

- Agregar/Editar/Eliminar usuarios
- Configure notificaciones por correo electrónico.
- Cambie el código de acceso y el nombre del grupo

NOTA: Los trabajos del grupo se completan rápidamente, siempre y cuando todos los miembros estén en línea y accesibles. Puede que se transcurran 10 minutos desde el inicio del trabajo hasta su finalización. Un trabajo esperará y volverá a intentar durante un máximo de 10 horas para los sistemas que no estén accesibles.

NOTA: Mientras se está ejecutando una incorporación, no se puede programar ningún otro trabajo. Los trabajos incluyen:

- Agregar un nuevo usuario
- Cambiar contraseña de usuario
- Eliminar usuario
- Configuración de alertas
- Incorporar sistemas adicionales
- Cambiar el código de acceso del grupo
- Cambiar el nombre del grupo

Intentar invocar otro trabajo mientras está activa una tarea de incorporación, dará como resultado el código de error GMGR0039. Una vez que la tarea de incorporación haya realizado su primer intento de incorporar todos los nuevos sistemas, se podrán crear trabajos en cualquier momento.

Exportación de trabajos

El registro se puede exportar en el sistema local para obtener más referencias. La lista de trabajos se puede exportar a un formato de archivo csv. Contiene todos los datos relacionados con cada trabajo.

NOTA: Los archivos CSV exportados están disponibles solo en inglés.

Panel Información de grupo

El Panel Información de grupo en la parte superior derecha de la vista de resumen de Group Manager muestra un resumen de grupo consolidado. La configuración de grupo actual puede editarse desde la página de Configuración del grupo, a la que se puede acceder haciendo clic en el botón Configuración de grupo. Muestra cuántos sistemas posee el grupo. Además, ofrece información acerca de las controladoras principal y secundaria del grupo.

Configuración de grupo

En la página Group settings (Configuración de grupo), se proporciona un listado de los atributos de grupo seleccionados.

Atributo de grupo	Descripción
Nombre de grupo	Muestra el nombre del grupo.
Número de sistemas	Muestra el número total de sistemas en ese grupo.
Creada el	Muestra los detalles de la fecha y la hora.
Creado por	Muestra los detalles de la administración de grupos.
Sistema de control	Muestra la etiqueta de servicio del sistema, que actúa como el sistema de control y coordina las tareas de administración de grupos.
Sistema de copia de seguridad	Muestra la etiqueta de servicio del sistema, que actúa como el sistema de copia de seguridad. Si el sistema de control no está disponible, puede asumir los roles del sistema de control.

Permite al usuario llevar a cabo las acciones que se enumeran en la siguiente tabla en el grupo. Se podría crear un trabajo de configuración del grupo para estas acciones (cambiar nombre de grupo, modificar contraseña de grupo, eliminar miembros y eliminar el grupo). El estado del trabajo del grupo se puede ver o modificar desde **Group Manager (Administrador de grupos)** > **Jobs (Trabajos)**.

Acciones	Descripción
Cambiar el nombre	Permite cambiar el valor de **Current Group Name (Nombre de grupo actual)** por el de **New Group Name (Nuevo nombre de grupo)**.
Change Passcode (Cambiar contraseña)	Permite cambiar la contraseña de grupo existente introduciendo un valor en **New Group Passcode (Nueva contraseña de grupo)** y validándola con **Reenter New Group Passcode (Vuelva a introducir la nueva contraseña de grupo)**.
Eliminar sistemas	Permite eliminar varios sistemas del grupo a la vez.
Eliminar grupo	Permite eliminar el grupo. Para utilizar cualquier función de administrador de grupos, el usuario debe tener privilegios de administrador. Cualquier trabajo pendiente se detendrá en caso de que se elimine el grupo.

Acciones en un servidor seleccionado

En la página Summary (Resumen), puede hacer doble clic en una fila para iniciar el iDRAC para ese servidor a través de un único redireccionamiento de inicio de sesión. Asegúrese de desactivar el bloqueo de ventanas emergentes en la configuración del explorador. Puede realizar las siguientes acciones en el servidor seleccionado. Para ello, haga clic en el elemento apropiado en la lista desplegable **Más acciones**.

Opción	Descripción
Apagado ordenado	Cierra el sistema operativo y apaga el sistema.
Reinicio mediante suministro de energía	Apaga y reinicia el sistema.
Consola virtual	Inicia la consola virtual con un inicio de sesión de individual en una ventana de explorador. **NOTA: Desactive el bloqueo de ventanas emergentes desde el explorador para utilizar esta función.**

Inicio de sesión único de Group Manager

Todos los iDRAC del grupo confían entre sí en función del código de acceso secreto compartido y el nombre de grupo compartido. Como resultado, un usuario administrador en un iDRAC de miembro del grupo puede otorgar privilegios de nivel de administrador en cualquier iDRAC de miembro del grupo cuando se accede a través del inicio de sesión único de la interfaz web de Group Manager. iDRAC registra <user>-<SVCTAG> como el usuario que inició sesión en los miembros del mismo nivel. <SVCTAG> es la etiqueta de servicio del iDRAC, donde el usuario inició sesión por primera vez.

Conceptos de Group Manager: Sistema de control

- Selecciona automáticamente y de manera predeterminada el primer iDRAC configurado para el Group Manager.
- Brinda flujo de trabajo de la GUI de Group Manager.
- Realiza el seguimiento de todos los miembros.
- Coordina tareas.
- Si un usuario inicia sesión en cualquier miembro y hace clic en Abrir Group Manager, el explorador será redirigido a la controladora principal.

Conceptos de Group Manager: Sistema de copia de seguridad

- La controladora principal selecciona automáticamente una controladora secundaria para tomar el control si la principal queda fuera de línea por un largo período de tiempo (10 minutos o más).
- Si tanto el primario como el secundario quedan fuera de línea por un período prolongado (durante más de 14 minutos), se elige un nuevo controlador primario y secundario.
- Conserva una copia de la caché de Group Manager de todos los miembros de grupos y tareas.
- El sistema de control y el sistema de copia de seguridad se determinan en forma automática por el Group Manager.
- No es necesario la configuración o participación del usuario.

12

Administración de registros

El iDRAC proporciona un registro de Lifecycle que contiene los sucesos relacionados con el sistema, los dispositivos de almacenamiento, los dispositivos de red, las actualizaciones de firmware, los cambios de configuración, los mensajes de licencia, etc. Sin embargo, los sucesos del sistema también están disponibles como registro distinto denominado Registro de sucesos del sistema (SEL). Se puede acceder al registro de Lifecycle a través de la interfaz web de iDRAC, RACADM y la interfaz de WSMan.

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 los mismos. Para ver los registros archivados, deberá exportarlos a una ubicación de su sistema.

Temas:

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 de SEL también está disponible en el registro de LC.

Visualización del registro de sucesos del sistema mediante la interfaz web

Para ver el registro de sucesos del sistema (SEL), en la interfaz web de iDRAC, vaya a **Maintenance (Mantenimiento)** > **System Event Log (Registro de sucesos del sistema)**.

En la página **System Event Log (Registro de sucesos del sistema)**, se muestra un indicador de la condición del sistema, una marca de hora y fecha, y una descripción de cada suceso registrado. Para obtener más información, consulte la *Ayuda en línea de iDRAC*.

Haga clic en **Guardar como** para guardar el **SEL** en una ubicación de su elección.

NOTA: Si está utilizando Internet Explorer y hay un problema al guardar, descargue la actualización de seguridad acumulada para Internet Explorer. Se puede descargar desde el sitio web de asistencia de Microsoft en support.microsoft.com.

Para borrar los registros, haga clic en **Borrar registro**.

NOTA: Borrar registro sólo aparece si tiene permiso de Borrar registros.

Después de vaciar el SEL, se registra una anotación en el registro de Lifecycle Controller. La anotación del registro incluye el nombre de usuario y la dirección IP de la ubicación desde donde se borró el SEL.

Visualización del registro de sucesos del sistema mediante RACADM

Para ver el SEL:

```
racadm getsel <options>
```

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

Para mostrar el número de entradas de SEL: `racadm getsel -i`

Para borrar las entradas de SEL: `racadm clrsel`

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

Visualización del registro de sucesos del sistema mediante la utilidad de configuración de iDRAC

Es posible ver la cantidad total de registros del registro de sucesos del sistema (SEL) mediante la utilidad de configuración de iDRAC. Además es posible borrar los registros. Para hacerlo:

1. En la utilidad de configuración de iDRAC, vaya a **Registro de sucesos del sistema**.
   La página **Configuración de iDRAC - Registro de sucesos del sistema** muestra la **cantidad total de registros**.
2. Para borrar los registros, seleccione **Sí**. De lo contrario, seleccione **No**.
3. Para ver los sucesos del sistema, haga clic en **Mostrar registro de sucesos del sistema**.
4. Haga clic en **Atrás**, en **Terminar** y, a continuación, en **Sí**.

Visualización del registro de Lifecycle

Los registros de Lifecycle Controller proporcionan un historial de los cambios relacionados con los componentes instalados en un sistema administrado. También puede agregar notas de trabajo en cada entrada del registro.

Los eventos y las actividades siguientes se registran:

- Todos
- Estado del sistema: la categoría Estado del sistema representa todas las alertas relacionadas con el hardware dentro del chasis del sistema.
- Estado: la categoría Estado del almacenamiento representa las alertas que se relacionan con el subsistema de almacenamiento.
- Actualizaciones: la categoría Actualización representa alertas que se generan debido a actualizaciones/regresos a versiones anteriores de firmware/controladores.
- Auditoría: la categoría Auditoría representa el registro de auditoría.
- Configuración: la categoría Configuración representa alertas relacionadas con los cambios de configuración del hardware, el firmware y el software.
- Notas de trabajo

Cuando inicia o cierra sesión en iDRAC mediante alguna de las siguientes interfaces, los sucesos de error en el inicio de sesión, el cierre de sesión o el acceso se registran en los registros de Lifecycle:

- Telnet

- SSH
- Interfaz web
- RACADM
- Redfish
- SM-CLP
- IPMI en la LAN
- Serie
- Consola virtual
- Medios virtuales

Puede ver y filtrar los registros en función de la categoría y el nivel de gravedad. También puede exportar y agregar una nota de trabajo a un evento de registro.

NOTA: Los registros de Lifecycle para cambiar el modo de personalidad solo se generan durante el reinicio desde el sistema operativo.

Si inicia trabajos e configuración con la interfaz web RACADM CLI o iDRAC, el registro de Lifecycle contiene información sobre el usuario, la interfaz utilizada y la dirección IP del sistema desde el cual se inicia el trabajo.

Visualización del registro de Lifecycle mediante la interfaz web

Para ver los registros de Lifecycle, haga clic en **Maintenance (Mantenimiento)** > **Lifecycle Log (Registro de Lifecycle)**. Aparecerá la página **Lifecycle Log (Registro de Lifecycle)**. Para obtener más información sobre las opciones, consulte la *Ayuda en línea de iDRAC*.

Filtrado de los registros de Lifecycle

Puede filtrar los registros según la categoría, la gravedad, una palabra clave o un intervalo de fechas.

Para filtrar los registros de lifecycle:

1 En la página **Registro de ciclos de vida**, bajo **Filtro del registro**, realice una o todas las acciones siguientes:
   - Seleccione **Tipo de registro** de la lista desplegable.
   - Seleccione el nivel de gravedad de la lista desplegable **Gravedad**.
   - Introduzca una palabra clave.
   - Especifique el intervalo de fechas.

2 Haga clic en **Aplicar**.
   Las entradas del registro con filtro se muestran en **Resultados del registro**.

Adición de comentarios a los registros de Lifecycle.

Para agregar comentarios a los registros de lifecycle:

1 En la página **Registro de Lifecycle**, haga clic en el icono de la anotación de registro deseada.
   Se muestran los detalles del ID de mensaje.

2 Introduzca los comentarios para la anotación de registro en el cuadro **Comentario**.
   Los comentarios se muestran en el cuadro **Comentario**.

Visualización del registro de Lifecycle mediante RACADM

Para ver los registros de Lifecycle, utilice el comando `lclog`.

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

Exportación de los registros de Lifecycle Controller

Puede exportar todo el registro de Lifecycle Controller (anotaciones activas y archivadas) en un archivo XML comprimido individual a un recurso compartido de red o al sistema local. La extensión del archivo XML comprimido es **.xml.gz**. Las anotaciones de archivo se ordenan en forma de secuencia según sus números de secuencia, desde el menor hasta el mayor.

Exportación de los registros de Lifecycle Controller mediante la interfaz web

Para exportar los registros de Lifecycle Controller mediante la interfaz web:

1 En la página **Registro de Lifecycle**, haga clic en **Exportar**.
2 Seleccione cualquiera de las opciones siguientes:
- **Red**: exporte los registros de Lifecycle Controller a una ubicación compartida de la red.
- **Local**: exporte los registros de Lifecycle Controller a una ubicación del sistema local.

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

Para obtener información acerca de los campos, consulte la *Ayuda en línea de iDRAC7*.
3 Haga clic en **Exportar** para exportar el registro a la ubicación especificada.

Exportación de los registros de Lifecycle Controller mediante RACADM

Para exportar los registros de Lifecycle Controller, utilice el comando `lclog export`.

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

Adición de notas de trabajo

Cada usuario que inicie sesión en iDRAC puede agregar notas de trabajo y estas se almacenan como un suceso en el registro de ciclos de vida. Es necesario tener un privilegio de registro en iDRAC para agregar notas de trabajo. Se admite un máximo de 255 caracteres para cada nota de trabajo nueva.

NOTA: No es posible eliminar notas de trabajo.

Para agregar una nota de trabajo:

1 En la interfaz web de iDRAC, vaya a **Panel** > **Notas** > **agregar nota**.
Aparecerá la página **Notas de trabajo**.
2 En **Notas de trabajo**, introduzca el texto en el cuadro de texto vacío.

NOTA: Se recomienda no utilizar demasiados caracteres especiales.

3 Haga clic en **Save** (Guardar).
La nota de trabajo se agregará al registro. Para obtener más información, consulte la *Ayuda en línea de iDRAC*.

Configuración del registro del sistema remoto

Puede enviar registros de Lifecycle a un sistema remoto. Antes de ello, asegúrese de que:

- Hay conectividad de red entre iDRAC y el sistema remoto.
- El sistema remoto e iDRAC se encuentran en la misma red.

Configuración del registro del sistema remoto mediante la interfaz web

Para configurar los valores del servidor de registro del sistema remoto:

1 En la interfaz web de iDRAC, vaya a **Configuración** > **Configuración del sistema** > **Configuración del registro del sistema remoto**.
Aparece la pantalla **Configuración del registro del sistema remoto**.

2 Active el registro del sistema remoto y especifique la dirección del servidor y el número de puerto. Para obtener más información acerca de estas opciones, consulte la *Ayuda en línea de iDRAC*.

3 Haga clic en **Aplicar**.
La configuración se guarda. 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 establecer la configuración de registro del sistema remoto, utilice el comando **set** con los objetos en el grupo **iDRAC.SysLog**.

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

13

Supervisión y administración de la alimentación

Puede utilizar iDRAC para supervisar y administrar los requisitos de alimentación del sistema administrado. Esto ayuda a proteger el sistema de cortes en el suministro eléctrico al distribuir y regular correctamente el consumo de energía 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 posible consumo de energía mínimo y máximo. Esta es una función con licencia.
- **Control de alimentación**: permite realizar operaciones de control de alimentación de manera remota (tal como encendido, apagado, restablecimiento del sistema, ciclo de encendido y apagado ordenado) en el sistema administrado.
- **Opciones de suministro de energía**: permiten configurar las opciones de suministro de energía, tal como la política de redundancia, el repuesto dinámico y la corrección del factor de alimentación.

Temas:

Supervisión de la alimentación

iDRAC supervisa el consumo de alimentación del sistema continuamente y muestra los siguientes valores de alimentación:

- Umbrales de advertencia y críticos del consumo de alimentación
- Valores acumulados de alimentación, alimentación pico y amperaje pico.
- Consumo de alimentación de la última hora, el último día o la última semana
- Consumo de alimentación promedio, mínimo y máximo
- Valores pico históricos y marcas de tiempo picos
- Valores espacio pico y de espacio instantáneo (para los servidores de tipo bastidor y torre).

NOTA: El histograma de la tendencia de consumo de energía del sistema (cada hora, diariamente, semanalmente) se mantiene solo mientras se ejecuta iDRAC. Si se reinicia iDRAC, los datos de consumo de energía existentes se pierden y el histograma se reinicia.

Supervisión del índice de rendimiento de CPU, memoria y módulos de E/S mediante la interfaz web

Para supervisar el índice de rendimiento de CPU, memoria y módulos de E/S, en la interfaz web de iDRAC, vaya a **System (Sistema)** > **Performance (Rendimiento)**.

- Sección **Rendimiento del sistema**: se muestra la lectura actual y la lectura de advertencia para el índice de utilización de la CPU, la memoria y los módulos de E/S, así como el índice CUPS en el nivel del sistema en una vista gráfica.
- Sección **Datos históricos de rendimiento del sistema**:
  - Proporciona las estadísticas para CPU, memoria, utilización de E/S e índice CUPS de nivel del sistema. Si el sistema host está apagado, en el gráfico, se muestra la línea de apagado por debajo del 0 %.
  - Es posible restablecer la utilización pico para un determinado sensor. Haga clic en **Reset Historical Peak (Restablecer pico histórico)**. Debe tener el privilegio de configuración para restablecer el valor pico.
- Sección **Métricas de rendimiento**:
  - Muestra el estado y la lectura presente.
  - Muestra o especifica el límite de utilización del umbral de aviso. Debe tener el privilegio de configuración de servidores para establecer los valores de umbral.

Para obtener información acerca de las propiedades que se muestran, consulte la *Ayuda en línea de iDRAC*.

Supervisión del índice de rendimiento de CPU, memoria y módulos de E/S mediante RACADM

Utilice el subcomando **SystemPerfStatistics** para supervisar el índice de rendimiento de la CPU, la memoria y los módulos de E/S. Para obtener más información, consulte *iDRAC RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de iDRAC)* disponible en **dell.com/esmmanuals**.

Configuración del umbral de advertencia para consumo de alimentación

Es posible establecer el valor de umbral de advertencia para el sensor de consumo de alimentación en los sistemas tipo bastidor y torre. El umbral de alimentación de advertencia/crítico para los sistemas de torre y bastidor puede cambiar en un ciclo de encendido del sistema según la capacidad de la unidad de suministro de energía y la política de redundancia. Sin embargo, el umbral de advertencia no debe exceder el umbral crítico aunque cambie la capacidad de la unidad de suministro de energía de la política de redundancia.

El umbral de alimentación de advertencia para los sistemas de tipo bastidor se establece según la asignación de alimentación para CMC.

Si se realiza una acción para restablecer los valores predeterminados, los umbrales de alimentación se establecerán en los valores predeterminados.

Es necesario tener el privilegio de usuario de configuración para establecer el valor del umbral de advertencia para el sensor de consumo de alimentación.

NOTA: El valor del umbral de advertencia se restablece al valor predeterminado después de realizar un racreset o una actualización del iDRAC.

Configuración del umbral de advertencia para consumo de alimentación mediante la interfaz web

1 En la interfaz web de iDRAC, vaya a **System (Sistema)** > **Overview (Descripción general)** > **Present Power Reading and Thresholds (Presentar lectura de alimentación y umbrales)**.

2 En la sección **Present Power Reading and Thresholds (Presentar lectura de alimentación y umbrales)**, haga clic en **Edit Warning Threshold (Editar umbral de advertencia)**.

Aparecerá la página **Edit Warning Threshold (Editar umbral de advertencia)**.

3 En la columna **Warning Threshold (Umbral de advertencia)**, introduzca el valor en **Watts (Vatios)** o **BTU/hr (BTU/h)**.

Los valores deben ser inferiores a los valores de **Umbral de falla**. Los valores se redondean hacia al valor más cercano que sea divisible por 14. Si introduce **Watts (Vatios)**, el sistema calcula y muestra automáticamente el valor en **BTU/hr (BTU/h)**. De la misma manera, si introduce BTU/hr (BTU/h), se muestra el valor en **Watts (Vatios)**.

4 Haga clic en **Save** (Guardar). Se configuran los valores.

Ejecución de las operaciones de control de alimentación

iDRAC permite encender, apagar, restablecer, apagar de manera ordenada, realizar una interrupción sin máscara (NMI) o un ciclo de encendido del sistema de manera remota mediante la interfaz web o RACADM.

Estas operaciones también se pueden realizar mediante los Servicios remotos de Lifecycle Controller o WSMan. Para obtener más información, consulte la *Guía de inicio rápido de servicios remotos de Lifecycle Controller,* disponible en **dell.com/idracmanuals** y el documento de perfil *Dell Power State Management* disponible en **delltechcenter.com**.

Las operaciones de control de alimentación del servidor iniciadas desde iDRAC son independientes del comportamiento del botón de encendido configurado en el BIOS. Puede utilizar la función PushPowerButton para apagar o encender el sistema en forma correcta, incluso si el BIOS está configurado para no hacer nada cuando se presiona el botón de alimentación física.

Ejecución de las operaciones de control de alimentación mediante la interfaz web

Para realizar las operaciones de control de alimentación:

1 En la interfaz web de iDRAC, vaya a **Configuración** > **Control de alimentación**. Aparecerán las opciones **Control de alimentación**.

2 Seleccione la operación de alimentación necesaria:

- Encender el sistema
- Apagar el sistema
- NMI (Interrupción no enmascarable)
- Apagado ordenado
- Restablecer el sistema (reinicio mediante sistema operativo)
- Realizar ciclo de encendido del sistema (reinicio mediante suministro de energía)

3 Haga clic en **Aplicar**. Para obtener más información, consulte la *Ayuda en línea de iDRAC*.

Ejecución de las operaciones de control de alimentación mediante RACADM

Para realizar acciones relacionadas con la alimentación, utilice el comando **serveraction**.

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

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 es una función con licencia.

Límites de alimentación en servidores Blade

Antes de que un servidor blade en un chasis PowerEdge M1000e o PowerEdge VRTX se encienda, el iDRAC proporciona a CMC sus requisitos de alimentación. Es mayor que la alimentación real que puede consumir el servidor blade y se calcula según la información del inventario de hardware limitado. Podrá solicitar un rango menor de alimentación después de que el servidor se enciende, de acuerdo con la energía real consumida por el servidor. Si el consumo de energía aumenta con el tiempo y si el servidor consume una alimentación cercana a su asignación máxima, es posible que iDRAC solicite un aumento del consumo de alimentación potencial máximo, por lo que aumentará la envolvente de alimentación. El iDRAC sólo aumenta su requerimiento de consumo de alimentación potencial máximo a CMC. No requiere una menor alimentación potencial mínima si el consumo disminuye. iDRAC sigue requiriendo más alimentación si el consumo de alimentación supera la alimentación asignada por la CMC.

Una vez encendido e inicializado el sistema, iDRAC calcula un nuevo requisito de alimentación basado en la configuración real del servidor blade. Este último permanece encendido incluso si CMC no consigue asignar una nueva solicitud de alimentación.

La CMC recupera toda alimentación sin utilizar de los servidores de menor prioridad y luego la asigna a un servidor o módulo de infraestructura de mayor prioridad.

Si no existe suficiente alimentación asignada, el servidor blade no se enciende. Si se ha asignado alimentación suficiente al servidor blade, iDRAC enciende el sistema.

Visualización y configuración de la política de límites de alimentación

Cuando la política de límite de alimentación está activada, aplica límites de alimentación definidos por el usuario para el sistema. De no ser así, utiliza la política de protección de alimentación del 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 en forma dinámica para mantener el consumo de alimentación cercano al umbral especificado.

El consumo de alimentación real puede ser inferior para las cargas de trabajo livianas y puede exceder momentáneamente el umbral hasta que se completen los ajustes de rendimiento. Por ejemplo, para una configuración determinada del sistema, el consumo de alimentación potencial máximo del sistema es de 700 vatios y el consumo mínimo es de 500 vatios. Puede especificar y activar un umbral de presupuesto de alimentación para reducir el consumo de los 650 vatios actuales a 525 vatios. A partir de ese punto, el rendimiento del sistema se ajusta en forma dinámica para mantener el consumo de alimentación de modo que no supere el umbral especificado por el usuario de 525 vatios.

Si el valor de límite de alimentación se establece a un valor inferior al umbral mínimo recomendado, es posible que iDRAC no pueda mantener el límite deseado.

El valor se puede especificar en vatios, BTU/hora o como un porcentaje (%) del límite de alimentación máximo recomendado.

Al establecer el umbral del límite de alimentación en BTU/h, la conversión a vatios se redondea al número entero más cercano. Al volver a leer el umbral del límite de alimentación, la conversión de vatios a BTU/h se vuelve a redondear del mismo modo. Como resultado, el valor escrito podría ser nominalmente diferente al valor leído; por ejemplo, un umbral establecido en 600 BTU/h se volverá a leer como 601 BTU/h.

Configuración de la política de límites de alimentación mediante la interfaz web

Para ver y configurar las políticas de alimentación:

1 En la interfaz web de iDRAC, vaya a **Configuration (Configuración)** > **Power Management (Administración de energía)** > **Power Cap Policy (Política de límite de alimentación)**.

El límite de la política de alimentación actual se muestra en la sección **Power Cap Limits (Límites de alimentación)**.

2 Seleccione **Enable (Activar)** en **Power Cap (Límite de alimentación)**.

3 En la sección **Power Cap Limits (Límites de alimentación)**, introduzca el límite de alimentación máximo en vatios y BTU/hora o el porcentaje (%) máximo del límite del 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 energía actuales, utilice los siguientes objetos con el comando `set`:

- System.Power.Cap.Enable
- System.Power.Cap.Watts
- System.Power.Cap.Btuhr
- System.Power.Cap.Percent

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

Configuración de la política de límites de alimentación mediante la utilidad de configuración de iDRAC

Para ver y configurar las políticas de alimentación:

1 En la utilidad de configuración de iDRAC, vaya a **Configuración de la alimentación**.

NOTA: El vínculo Configuración de alimentación está disponible solo si la unidad de suministro de energía del servidor admite la supervisión de alimentación.

Se muestra la página **Configuración de alimentación de la configuración de iDRAC**.

2 Seleccione **Activado** para activar la opción **Política de límites de alimentación**. De lo contrario, seleccione **Desactivado**.

3 Utilice los valores recomendados o, en **Política de límites de alimentación definida por el usuario**, introduzca los límites necesarios.

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

4 Haga clic en **Atrás**, en **Terminar** y, a continuación, en **Sí**.

Se habrán configurado los valores de límites de alimentación.

Configuración de las opciones de suministro de energía

Puede configurar las opciones de suministro de energía, tal como la política de redundancia, repuesto dinámico y corrección del factor de alimentación.

El repuesto dinámico es una función de suministro de energía que configura las unidades de suministro de energía (PSU) redundantes para que se apeguen en función de la carga del servidor. Esto permite a las PSU restantes funcionar con una mayor carga y eficacia. Esto requiere PSU que admitan esta función de modo que se pueda encender rápidamente si fuera necesario.

En un sistema de dos PSU, es posible configurar PSU1 o PSU2 como la PSU principal.

Después de activar el repuesto dinámico, las unidades de suministro de energía pueden activarse o suspenderse en función de la carga. Si Repuesto dinámico está activado, se activa la corriente eléctrica asimétrica que se comparte entre las dos unidades de suministro de energía. Una unidad de suministro de energía está *activa* y proporciona la mayoría de la corriente mientras que la otra se encuentra suspendida y proporciona una pequeña cantidad de corriente. Esto suele denominarse 1+0 con dos unidades de suministro de energía y repuesto dinámico activado. Si todas las unidades de suministro de energía 1 están en el circuito A y las unidades de suministro de energía 2 en el circuito B, con el repuesto dinámico activado (configuración de repuesto dinámico de fábrica predeterminada), el circuito B tiene mucho menos carga y dispara los avisos. Si se desactiva el repuesto dinámico, la corriente eléctrica se comparte en partes iguales (50-50) por las dos unidades de suministro de energía y los circuitos A y B generalmente tienen la misma carga.

El factor de potencia es la tasa de potencia real consumida en la potencia aparente. Cuando se activa la corrección del factor de energía, el servidor consume una pequeña cantidad de alimentación cuando el host está APAGADO. De manera predeterminada, la corrección del factor de energía está activada cuando el servidor se envía de fábrica.

Configuración de las opciones de suministro de energía mediante la interfaz web

Para configurar las opciones de suministro de energía:

1 En la interfaz web de iDRAC, vaya a **Configuración** > **Administración de la alimentación** > **Configuración de la alimentación**.
2 En **Política de redundancia de alimentación**, seleccione las opciones necesarias. Para obtener más información, consulte la *Ayuda en línea de iDRAC*.
3 Haga clic en **Aplicar**. Se habrán configurado los valores de suministro de energía.

Configuración de las opciones de suministro de energía mediante RACADM

Para configurar las opciones de suministro de energía, utilice los siguientes objetos con el comando `set`:

- System.Power.RedundancyPolicy
- System.Power.Hotspare.Enable
- System.Power.Hotspare.PrimaryPSU
- System.Power.PFC.Enable

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

Configuración de las opciones de suministro de energía mediante la utilidad de configuración de iDRAC

Para configurar las opciones de suministro de energía:

1 En la utilidad de configuración de iDRAC, vaya a **Configuración de la alimentación**.

> **NOTA: El vínculo Configuración de alimentación está disponible solo si la unidad de suministro de energía del servidor admite la supervisión de alimentación.**

Se muestra la página **Configuración de la alimentación de la configuración de iDRAC**.

2 En **Opciones de suministro de energía**:

- Activa o desactive la redundancia del suministro de energía.
- Active o desactive el repuesto dinámico.
- Establezca la unidad principal de suministro de energía.
- Activar o desactivadar la corrección del factor de alimentación. Para obtener más información acerca de las opciones, consulte la *Ayuda en línea de la utilidad de configuración de iDRAC*.

3 Haga clic en **Atrás**, en **Terminar** y, a continuación, en **Sí**.

Se habrán configurado los valores de suministro de energía.

Activación o desactivación del botón de encendido

Para activar o desactivar el botón de encendido del sistema administrado:

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

Se mostrará la página **Configuración de iDRAC - Seguridad del panel frontal**.

2 Seleccione **Activado** para activar el botón de encendido o **Desactivado** para desactivarlo.

3 Haga clic en **Atrás**, en **Terminar** y, a continuación, en **Sí**.

La configuración se guarda.

Refrigeración de múltiples vectores

La refrigeración de múltiples vectores implementa un enfoque de varias clavijas para controles térmicos en plataformas de servidores Dell EMC. Esto incluye (pero sin limitarse a):

- Un amplio conjunto de sensores (térmicos, de alimentación, de inventario, etc.) que permite la interpretación precisa del estado térmico del sistema en tiempo real en varias ubicaciones dentro del servidor. Se mostrará solamente un pequeño subconjunto de sensores que son relevantes para los usuarios, necesarios según la configuración.
- Un algoritmo inteligente y adaptable de control de bucle cerrado optimiza la respuesta del ventilador para mantener las temperaturas de los componentes. También permite conservar la alimentación del ventilador, el consumo de flujo de aire y la acústica.
- Mediante la asignación de zonas de ventiladores, el enfriamiento puede iniciarse para los componentes cuando se requiera. Por lo tanto, se produce un máximo rendimiento sin comprometer la eficacia de la utilización de alimentación.
- Representación exacta del flujo de aire de PCIe ranura por ranura en términos de métrica LFM (pies lineales por minuto: un estándar aceptado por el sector sobre cómo se especifica el requisito de flujo de aire de la tarjeta PCIe). La visualización de esta métrica en diversas interfaces de iDRAC le permite al usuario:
  - a Conocer la capacidad máxima LFM de cada ranura dentro del servidor.
  - b Conocer qué enfoque se está tomando para la refrigeración de PCIe para cada ranura (controlada por flujo de aire o controlada por temperatura).
  - c Conocer el mínimo LFM que se entregan a una ranura, si la tarjeta es de otros fabricantes (tarjeta personalizada definida por el usuario).

d Marcar un valor LFM mínimo personalizado para la tarjeta de otros fabricantes, lo que permite una definición más precisa de las necesidades de refrigeración de la tarjeta de las cuales el usuario tiene mejor conocimiento a través de las especificaciones de la tarjeta personalizada.

- Muestra una métrica de flujo de aire del sistema en tiempo real (CFM, pies cúbicos por minuto) en diversas interfaces de iDRAC al usuario para activar un equilibrio del flujo de aire del centro de datos basado en la agregación de consumo CFM por servidor.
- Permite una configuración térmica personalizada como perfiles térmicos (rendimiento máximo frente a rendimiento máximo por vatio, límite de sonido, etc.), opciones de velocidad de ventilador personalizadas (velocidad mínima del ventilador, desplazamientos de velocidad del ventilador, etc.) y configuración de temperatura de salida personalizada.

a La mayoría de estos ajustes permiten una refrigeración adicional sobre la línea de base de la refrigeración generada por algoritmos térmicos, y no permiten que las velocidades de los ventiladores excedan los requisitos de refrigeración del sistema.

> **NOTA: Una excepción a la declaración anterior es para las velocidades de los ventiladores que se agregan para tarjetas PCIe de otros fabricantes. El flujo de aire de aprovisionamiento del algoritmo térmico para tarjetas de otros fabricantes puede ser mayor o menor a las necesidades reales de enfriamiento de la tarjeta y el cliente puede ajustar la respuesta para la tarjeta al introducir el valor LFM correspondiente a la tarjeta de otros fabricantes.**

b La opción de temperatura de salida personalizada limita la temperatura de salida a la configuración deseada por el cliente.

> **NOTA: Es importante tener en cuenta que con ciertas configuraciones y cargas de trabajo, quizás no sea físicamente posible reducir la salida por debajo de un punto de ajuste deseado (por ejemplo, la configuración de salida personalizada de 45 °C con una alta temperatura de entrada [por ejemplo, 30 °C] y una configuración cargada [alto consumo de energía del sistema, bajo flujo de aire]).**

c La opción de límite de sonido es nueva en el servidor PowerEdge de 14.ª generación. Limita el consumo de energía de la CPU y controla la velocidad de los ventiladores y el techo acústico. Esto es exclusivo para las implementaciones acústicas y puede generar un menor rendimiento del sistema.

- El diseño y la disposición del sistema permiten una mayor capacidad de flujo de aire (con la posibilidad de alta potencia) y configuraciones de sistemas densos. También proporciona menos restricciones del sistema y mayor densidad de la función.

a El flujo de aire mejorado permite una eficiente relación de flujo de aire-consumo de energía del ventilador.

- Los ventiladores personalizados están diseñados para una mayor eficiencia, un mejor rendimiento, una duración más prolongada y menos vibración. También ofrece un mejor resultado de acústica.

a Los ventiladores pueden tener una larga duración (en general, pueden funcionar durante más de 5 años), incluso si funcionan a máxima velocidad todo el tiempo.

- Los disipadores de calor personalizados están diseñados para optimizar la refrigeración de los componentes al flujo de aire mínimo (obligatorio), pero que es compatible con CPU de alto rendimiento.

14

Inventario, supervisión y configuración de dispositivos de red

Es posible crear un inventario, supervisar y configurar los siguientes dispositivos de red:

- Tarjetas de interfaz de red (NIC)
- Adaptadores de red convergentes (CNA)
- LAN de la placa base (LOM)
- Tarjetas secundarias de interfaz de red (NIC)
- Tarjetas mezzanine (solo para servidores Blade)

Antes de deshabilitar NPAR o una partición individual en dispositivos CNA, asegúrese de borrar todos los atributos de la identidad de E/S (por ejemplo: dirección IP, direcciones virtuales, iniciador y destinos de almacenamiento) y los atributos de nivel de partición (por ejemplo: asignación de ancho de banda). Puede desactivar una partición mediante el cambio del valor del atributo VirtualizationMode a NPAR o deshabilitando todas las personalidades de una partición.

Según el tipo de dispositivo CNA instalado, la configuración de atributos de una partición no se puede conservar desde la última vez que la partición estuvo activa. Establezca todos los atributos de identidad de E/S y los atributos relacionados con la partición cuando se la activa. Puede activar una partición mediante el cambio del valor del atributo VirtualizationMode a NPAR o habilitando una personalidad (Ejemplo: NicMode) de la partición.

Temas:

Inventario y supervisión de dispositivos de red

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

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

- Estado de vínculo
- Propiedades
- Configuración y capacidades
- Estadísticas de recepción y transmisión
- iSCSI, iniciador de FCoE e información de destino

Supervisión de dispositivos de red mediante la interfaz web

Para ver la información del dispositivo de red mediante la interfaz web, vaya a **Sistema** > **Descripción general** > **Dispositivos de red**. Se mostrará la página **Dispositivos de red**. Para obtener más información acerca de las propiedades que se muestran, consulte la *Ayuda en línea de iDRAC*.

Supervisión de dispositivos de red mediante RACADM

Para ver información sobre los dispositivos de red, utilice los comandos **hwinventory** y **nicstatistics**.

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

Pueden mostrarse propiedades adicionales cuando se utiliza RACADM o WSMan, además de las propiedades que se muestran en la interfaz web de iDRAC.

Vista Conexión

Revisar y solucionar problemas de las conexiones de red de los servidores en forma manual es imposible de controlar en un entorno de centro de datos. IDRAC9 optimiza el trabajo con la vista Conexión de iDRAC. Esta función le permite verificar y solucionar problemas de conexiones de red de manera remota desde la misma GUI centralizada que está utilizando para implementar, actualizar, monitorear y mantener los servidores. La Vista Conexión en iDRAC9 proporciona detalles de la asignación física de puertos del conmutador a los puertos de red del servidor y conexiones de puerto iDRAC (integrated Dell Remote Access Controller) dedicadas. Todas las tarjetas de red admitidas están visibles en la Vista Conexión, independientemente de la marca.

En lugar de verificar y solucionar en forma manual las conexiones de red del servidor, puede ver y administrar las conexiones de los cables de red en forma remota.

La Vista Conexión proporciona la información de los puertos del conmutador conectados a los puertos del servidor y el puerto de iDRAC dedicado. Los puertos de red en el servidor PowerEdge incluyen los LOM, NDC, tarjetas Mezz y las tarjetas de complementos de PCIe

Para ver la Vista Conexión los dispositivos de red, vaya a **Sistema** > **Dispositivo de red** > **FQDD de Dispositivo de red** > **Puertos y puertos con particiones** .

Puede hacer clic en **Configuración de iDRAC** > **Descripción general** > **Vista Conexión** para ver la Vista Conexión.

Además, puede hacer clic en **Configuración de iDRAC** > **Conectividad** > > **Vista Conexión del conmutador** para activar o desactivar la Vista Conexión.

La Vista Conexión se puede explorar con el comando racadm `SwitchConnection View` y también se puede ver con el comando `winrm` .

Campo u opción	Descripción
Activado	Seleccione **Activado** para activar la configuración de la comunicación en serie en la LAN. La opción **Enable (Activar)** está seleccionada de manera predeterminada.
Estado	Muestra **Activado**, si se activa la conexión de la opción vista **Vista Conexión** de configuración de iDRAC.
Conexión del conmutador	Muestra el ID. del chasis LLDP del conmutador a través de la cual el puerto de dispositivo está conectado.

Campo u opción	Descripción
Conexión del puerto del conmutador	Muestra el Id. de puerto LLDP del puerto del conmutador al que el puerto de dispositivo está conectado.

NOTA: Conexión del conmutador y el puerto de conmutación ID. ID. de conexión están disponibles una vez que la conexión Ver está activado y el vínculo está conectado. La tarjeta de red asociado debe ser compatible con la vista conexión. Solo los usuarios con privilegios de configuración de iDRAC pueden modificar la configuración de la Vista Conexión del puerto del conmutador.

Vista Conexión del conmutador

Utilice **Actualizar vista Conexión** a fin de ver la información más reciente de Conexión del conmutador y del puerto del conmutador ID. ID. de conexión.

NOTA: Si el iDRAC contiene conexión del conmutador y el puerto de conmutación información de conexión para puerto de red o servidor y puerto de red iDRAC debido a alguna razón, el puerto del conmutador y conexión del conmutador información de la conexión no se actualiza para 5 minutos y, a continuación, la conexión del conmutador y del puerto del conmutador se muestra información de la conexión como no actualizados (última que esté en buenas condiciones datos) los datos para todos los interfaces de usuario. En la interfaz, verá que es un icono de aviso amarillo natural representación y no indica ningún aviso.

Vista Conexión los valores posibles

Conexión posible ver los datos	Descripción
Función desactivada	Vista Conexión función está desactivada, ver los datos para ver la conexión activar la función.
Enlace	Indica que el enlace asociado con la red puerto de la controladora está desactivado.
No disponible	LLDP no está activado en el conmutador. Compruebe si LLDP está activado en el puerto del conmutador.
No compatible	Controladora de red no es compatible con vista Conexión función.
Datos obsoletos	Los datos, ya sea que esté en buenas condiciones por última vez la controladora de red enlace del puerto está apagado o el sistema está apagado. Utilice la opción refresh para actualizar la conexión View Details (Ver detalles) para obtener los datos más recientes.
Datos válidos	Muestra la conexión del conmutador válido ID. ID. de conexión y el puerto del conmutador información.

Vista Conexión controladoras de red admitidos

Tarjetas siguientes o controladoras admiten Conexión función Vista.

Fabricante	Tipo
Broadcom	• 57414 Rndc 25GE • 57416/5720 Rndc de 10 GbE • 57412/5720 Rndc de 10 GbE • 57414 PCIe FH/LP 25GE • PCIe FH/LP (10 GbE) • PCIe FH/LP (10 GbE)

Fabricante	Tipo
Intel	• X710 bNDC de 10 Gb • X710 PCIe de 10 Gb • X710 PCIe de 10 Gb • X710+I350 rNDC de 10 Gb+1 Gb • X710 rNDC de 10 Gb • X710 bNDC de 10 Gb • XL710 PCIe de 40 Gb • XL710 Mezz de 10 Gb • X710 PCIe de 10 Gb
Mellanox	• MT27710 rNDC de 40 Gb • MT27710 PCIe de 40 Gb • MT27700 PCIe de 100 Gb
QLogic	• QL41162 PCIe 2P • QL41112 PCIe 2P • QL41262 PCIe 2P 25GE

Inventario y supervisión de dispositivos HBA FC

Es posible supervisar el estado de manera remota de los siguientes dispositivos de Adaptadores de bus del host del canal de fibra (FC HBA) en el sistema administrado. Se admiten los FC HBA Emulex y QLogic. Para cada dispositivo FC HBA, puede ver la siguiente información para los puertos:

- Información y estado del vínculo
- Propiedades de puertos
- Estadísticas de recepción y transmisión

Supervisión de dispositivos HBA FC mediante la interfaz web

Para consultar la información del dispositivo FC HBA mediante la interfaz web, vaya a **Sistema** > **Descripción general** > **Dispositivos de red** > **Fibre Channel**. Para obtener más información acerca de las propiedades que se muestran, consulte la *Ayuda en línea de iDRAC*.

El nombre de la página muestra también el número de ranura en donde el dispositivo HBA FC está disponible y el tipo de dispositivo HBA FC.

Supervisión de dispositivos HBA FC mediante RACADM

Para ver la información de dispositivos FC HBA mediante RACADM, utilice el comando **hwinventory**.

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

Configuración dinámica de las direcciones virtuales, del iniciador y del destino de almacenamiento

De manera dinámica, se pueden ver y configurar los valores de la dirección virtual, el iniciador y el destino de almacenamiento, así como aplicar una política de persistencia. Esto permite que la aplicación implemente la configuración según los cambios en el estado de la alimentación (es decir, el reinicio del sistema operativo, el restablecimiento mediante sistema operativo, el restablecimiento mediante suministro de energía o ciclo de CA) y también en función de la configuración de la política de persistencia para ese estado de la alimentación. Esto proporciona más flexibilidad en las implementaciones en las que se necesita una reconfiguración rápida de las cargas de trabajo de un sistema a otro.

Las direcciones virtuales son:

- Dirección MAC virtual
- Dirección MAC de iSCSI virtual
- Dirección MAC de FIP virtual
- WWN virtual
- WWPN virtual

NOTA: Al borrar la política de persistencia, todas las direcciones virtuales se restablecen a la dirección permanente predeterminada de fábrica.

NOTA: En algunas tarjetas con los atributos MAC de FIP virtual, WWPN virtual y WWN virtual, los atributos MAC de WWN virtual y WWPN virtual se configuran automáticamente cuando configura FIP virtual.

Con la característica de identidad de E/S, es posible:

- Ver y configurar las direcciones virtuales para los dispositivos de red y Fibre Channel (por ejemplo, NIC, CNA, HBA de Fibre Channel).
- Configurar los valores del iniciador (para iSCSI y FCoE) y del destino de almacenamiento (para iSCSI, FCoE y FC).
- Especificar la persistencia o la autorización de los valores configurados sobre una pérdida de alimentación de CA, un restablecimiento mediante sistema operativo y un restablecimiento mediante suministro de energía en el sistema

Los valores configurados para las direcciones virtuales, el iniciador y los destinos de almacenamiento pueden variar en función de la forma en que se maneja la alimentación eléctrica principal durante el restablecimiento del sistema y si los dispositivos NIC, CNA o HBA de FC tienen una alimentación auxiliar. La persistencia de la configuración de identidad de E/S se puede lograr en función de la configuración de políticas realizada mediante iDRAC.

Las políticas de persistencia surten efecto únicamente si la función de identidad de E/S se encuentra activada. Cada vez que el sistema se restablece o se enciende, los valores se mantienen o se borran en función de la configuración de políticas.

NOTA: Una vez borrados los valores, no puede volver a aplicarlos antes de ejecutar el trabajo de configuración.

Tarjetas admitidas para la optimización de la identidad de E/S

La siguiente tabla proporciona las tarjetas que admiten la función de optimización de la identidad de E/S.

Tabla 31. Tarjetas admitidas para la optimización de la identidad de E/S

Fabricante	Tipo
Broadcom	• 5719 Mezz de 1GB • 5720 PCIe de 1 GB • 5720 bNDC de 1 GB • 5720 rNDC de 1 GB

Fabricante	Tipo
	• 57414 PCIe 25GbE
Intel	• i350 PCIe DP FH de 1GB • i350 PCIe QP de 1GB • i350 rNDC QP de 1GB • i350 Mezz de 1GB • i350 bNDC de 1GB • x520 PCIe de 10GB • x520 bNDC de 10GB • x520 Mezz de 10GB • x520 + i350 rNDC de 10GB+1GB • X710 bNDC de 10GB • X710 bNDC QP de 10GB • X710 PCIe de 10 GB • X710 + I350 rNDC de 10GB+1GB • X710 rNDC de 10GB • XL710 QSFP DP LP PCIe de 40GE • XL710 QSFP DP FH PCIe de 40GE • X550 DP BT PCIe de 2 x 10 Gb • X550 DP BT LP PCIe de 2 x 10 Gb
Mellanox	• ConnectX-3 Pro 10G Mezz de 10GB • ConnectX-4 LX 25GE SFP DP rNDC de 25GB • ConnectX-4 LX 25GE DP FH PCIe de 25GB • ConnectX-4 LX 25GE DP LP PCIe de 25GB
QLogic	• 57810 PCIe de 10GB • 57810 bNDC de 10GB • 57810 Mezz de 10GB • 57800 rNDC de 10GB+1GB • 57840 rNDC de 10GB • 57840 bNDC de 10GB • QME2662 Mezz FC16 • QLE 2692 SP FC16 Gen 6 HBA FH PCIe FC16 • SP FC16 Gen 6 HBA LP PCIe FC16 • QLE 2690 DP FC16 Gen 6 HBA FH PCIe FC16 • DP FC16 Gen 6 HBA LP PCIe FC16 • QLE 2742 DP FC32 Gen 6 HBA FH PCIe FC32 • DP FC32 Gen 6 HBA LP PCIe FC32 • QLE2740 PCIe FC32
Emulex	• LPe15002B-M8 (FH) PCIe FC8 • LPe15002B-M8 (LP) PCIe FC8 • LPe15000B-M8 (FH) PCIe FC8 • LPe15000B-M8 (LP) PCIe FC8 • LPe31000-M6-SP PCIe FC16 • LPe31002-M6-D DP PCIe FC16 • LPe32000-M2-D SP PCIe FC32

Fabricante	Tipo
	• LPe32002-M2-D DP PCIe FC32

Versiones del firmware de la NIC admitidas para la optimización de la identidad de E/S

En los servidores Dell PowerEdge de 14ª generación, el firmware de NIC necesario se encuentra disponible de manera predeterminada.

La siguiente tabla proporciona las versiones del firmware de la NIC para la función de optimización de la identidad de E/S.

Comportamiento de Flex Address virtual y de la política de persistencia cuando iDRAC está configurado en modo de Flex Address o en modo de Consola

En la siguiente tabla se describe el comportamiento de la configuración de la administración de direcciones virtuales (VAM) y de la política de persistencia según el estado de la función FlexAddress en la CMC, el modo establecido en iDRAC, el estado de la función de la identidad de E/S en iDRAC y la configuración de XML.

Tabla 32. Comportamiento de la dirección de Virtual/Flex y de la política de persistencia

Estado de la función FlexAddress en la CMC	Modo establecido en iDRAC	Estado de la función de identidad de E/S en el iDRAC	Configuración de XML	Política de persistencia	Borrar Persistence Policy - Dirección virtual
FlexAddress activado	Modo de FlexAddress	Activado	Administración de direcciones virtuales (VAM) configurada	VAM configurada persiste	Establecer en Flex Address
FlexAddress activado	Modo de FlexAddress	Activado	VAM no configurada	Establecer en Flex Address	Sin persistencia: está establecido en Flex Address
FlexAddress activado	Modo de Flex Address	Desactivado	Configurado mediante la ruta de acceso proporcionada en Lifecycle Controller	Establecer valor en Flex Address para ese ciclo	Sin persistencia: está establecido en Flex Address
FlexAddress activado	Modo de Flex Address	Desactivado	VAM no configurada	Establecer en Flex Address	Establecer en Flex Address
Flex Address desactivada	Modo de Flex Address	Activado	VAM configurada	VAM configurada persiste	Persistencia: el borrado no es posible
Flex Address desactivada	Modo de Flex Address	Activado	VAM no configurada	Establecer en dirección MAC de hardware	No se admite la persistencia. Depende del comportamiento de la tarjeta
Flex Address desactivada	Modo de Flex Address	Desactivado	Configurado mediante la ruta de acceso	La configuración de Lifecycle Controller	No se admite la persistencia. Depende del

Estado de la función FlexAddress en la CMC	Modo establecido en iDRAC	Estado de la función de identidad de E/S en el iDRAC	Configuración de XML	Política de persistencia	Borrar Persistence Policy - Dirección virtual
			proporcionada en Lifecycle Controller	persiste durante ese ciclo	comportamiento de la tarjeta
Flex Address desactivada	Modo de Flex Address	Desactivado	VAM no configurada	Establecer en dirección MAC de hardware	Establecer en dirección MAC de hardware
FlexAddress activado	Modo de consola	Activado	VAM configurada	VAM configurada persiste	Persistencia y borrado deben funcionar
FlexAddress activado	Modo de consola	Activado	VAM no configurada	Establecer en dirección MAC de hardware	Establecer en dirección MAC de hardware
FlexAddress activado	Modo de consola	Desactivado	Configurado mediante la ruta de acceso proporcionada en Lifecycle Controller	La configuración de Lifecycle Controller persiste durante ese ciclo	No se admite la persistencia. Depende del comportamiento de la tarjeta
Flex Address desactivada	Modo de consola	Activado	VAM configurada	VAM configurada persiste	Persistencia y borrado deben funcionar
Flex Address desactivada	Modo de consola	Activado	VAM no configurada	Establecer en dirección MAC de hardware	Establecer en dirección MAC de hardware
Flex Address desactivada	Modo de consola	Desactivado	Configurado mediante la ruta de acceso proporcionada en Lifecycle Controller	La configuración de Lifecycle Controller persiste durante ese ciclo	No se admite la persistencia. Depende del comportamiento de la tarjeta
FlexAddress activado	Modo de consola	Desactivado	VAM no configurada	Establecer en dirección MAC de hardware	Establecer en dirección MAC de hardware

Comportamiento del sistema para FlexAddress y la identidad de E/S

	Estado de la función FlexAddress en el CMC	Estado de la función de identidad de E/S en el iDRAC	Disponibilidad de dirección virtual del agente remoto para el ciclo de reinicio	Origen de programación de dirección virtual	Comportamiento de la persistencia de dirección virtual de ciclo de reinicio
Servidor con persistencia equivalente de FA	Activado	Desactivado		FlexAddress desde el CMC	Según las especificaciones de FlexAddress
	N/A, Activado o Desactivado	Activado	Sí: nuevo o que persiste	Dirección virtual de agente remoto	Según las especificaciones de FlexAddress

	Estado de la función FlexAddress en el CMC	Estado de la función de identidad de E/S en el iDRAC	Disponibilidad de dirección virtual del agente remoto para el ciclo de reinicio	Origen de programación de dirección virtual	Comportamiento de la persistencia de dirección virtual de ciclo de reinicio
			No	Dirección virtual borrada	
	Desactivado	Desactivado			
Servidor con función de política de persistencia de VAM	Activado	Desactivado		FlexAddress desde el CMC	Según las especificaciones de FlexAddress
	Activado	Activado	Sí: nuevo o que persiste	Dirección virtual de agente remoto	Según la configuración de la política de agente remoto
			No	FlexAddress desde el CMC	Según las especificaciones de FlexAddress
	Desactivado	Activado	Sí: nuevo o que persiste	Dirección virtual de agente remoto	Según la configuración de la política de agente remoto
			No	Dirección virtual borrada	
	Desactivado	Desactivado			

Activación o desactivación de la optimización de la identidad de E/S

Generalmente, después del inicio del sistema, los dispositivos se configuran y se inicializan después de un reinicio. Puede activar la función Optimización de la identidad de E/S para lograr la optimización del inicio. Si está activada, configura la dirección virtual, el iniciador y los atributos del destino de almacenamiento después de restablecer el dispositivo y antes de su inicialización, lo que elimina la necesidad de un segundo reinicio del BIOS. La configuración de los dispositivos y la operación de inicio se producen en un solo inicio del sistema y se optimiza para el rendimiento del tiempo de inicio.

Antes de activar la optimización de la identidad de E/S, asegúrese de que:

- Tiene privilegios de Inicio de sesión, Configurar y Control del sistema.
- BIOS, iDRAC y las tarjetas de red se actualizan al firmware más reciente.

Después activar la función Optimización de la identidad de E/S, exporte el archivo de configuración XML de iDRAC, modifique los atributos necesarios de la identidad de E/S en el archivo de configuración XML e importe el archivo nuevamente al iDRAC.

Para obtener la lista de atributos de Optimización de la identidad de E/S que puede modificar en el archivo de configuración XML, consulte el documento *Perfil de NIC* disponible en **delltechcenter.com/idrac**.

NOTA: No modifique los atributos que no corresponden a la optimización de la identidad de E/S.

Activación o desactivación de la optimización de la identidad de E/S mediante la interfaz web

Para activar o desactivar la optimización de la identidad de E/S:

1 En la interfaz web de iDRAC, vaya a **Configuration (Configuración)** > **System Settings (Configuración del sistema)** > **Hardware Settings (Configuración de hardware)** > **I/O Identity Optimization (Optimización de la identidad de E/S)**.

Aparecerá la página **I/O Identity Optimization (Optimización de la identidad de E/S)**.

2 Haga clic en la ficha **I/O Identity Optimization (Optimización de la identidad de E/S)** y seleccione la opción **Enable (Activar)** para activar esta función. Para desactivar, borre esta opción.

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

Activación o desactivación de la optimización de la identidad de E/S mediante RACADM

Para activar la optimización de la identidad de E/S, utilice el comando:

```
racadm set idrac.ioidopt.IOIDOptEnable Enabled
```

Después de activar esta función debe reiniciar el sistema para que la configuración surta efecto.

Para desactivar la optimización de la identidad de E/S, utilice el comando:

```
racadm set idrac.ioidopt.IOIDOptEnable Disabled
```

Para ver la configuración de la optimización de la identidad de E/S, utilice el comando:

```
racadm get iDRAC.IOIDOpt
```

Configuración de la política de persistencia

Con la identidad de E/S, es posible configurar políticas en las que se especifiquen los comportamientos de restablecimiento y ciclo de encendido del sistema con los que se determina la persistencia o la autorización de los valores de configuración de dirección virtual, iniciador y destino de almacenamiento. Cada uno de los atributos de política de persistencia se aplica a todos los puertos y las particiones de todos los dispositivos correspondientes en el sistema. El comportamiento de los dispositivos cambia según sean de alimentación auxiliar o no.

NOTA: Es posible que la función Política de persistencia no funcione cuando se configura en el valor predeterminado, si el atributo VirtualAddressManagement está establecido en modo de FlexAddress en iDRAC y si la función FlexAddress está desactivada en la CMC. Asegúrese de establecer el atributo VirtualAddressManagement en el modo Consola en iDRAC o de activar la función FlexAddress en la CMC.

Es posible configurar los siguientes políticas de persistencia:

- Dirección virtual: dispositivos de alimentación auxiliar
- Dirección virtual: dispositivos que no son de alimentación auxiliar
- Iniciador
- Destino de almacenamiento

Antes de aplicar la política de persistencia, asegúrese de:

- Realizar el inventario de hardware de red al menos una vez, es decir, activar la opción Recopilar inventario del sistema al reinicio.
- Activar Optimización de identidad de E/S.

Los sucesos se registran en el registro de Lifecycle Controller en las siguientes situaciones:

- Se activa o desactiva la opción Optimización de identidad de E/S.
- Se modifica la política de persistencia.
- Cuando la dirección virtual, el iniciador y los valores de destino se establecen según la política. Se registra una anotación de registro única para los dispositivos configurados y los valores que se han establecido para esos dispositivos cuando se aplica la política.

Las acciones de suceso están activadas para SNMP, correo electrónico o notificaciones de sucesos de WS. Los registros también se incluyen en los registros del sistema remoto.

Valores predeterminados para la política de persistencia

Política de persistencia	Pérdida de alimentación de CA	Reinicio mediante suministro de energía	Reinicio mediante sistema operativo
Dirección virtual: dispositivos de alimentación auxiliar	No seleccionado	Seleccionado	Seleccionado
Dirección virtual: dispositivos que no son de alimentación auxiliar	No seleccionado	No seleccionado	Seleccionado
Iniciador	Seleccionado	Seleccionado	Seleccionado
Destino de almacenamiento	Seleccionado	Seleccionado	Seleccionado

NOTA: Cuando se desactiva una política persistente y se toma la medida de perder la dirección virtual, al volver a habilitar la política persistente, no se obtiene la dirección virtual. Debe establecer la dirección virtual nuevamente después de activar la política persistente.

NOTA: Si se cuenta con una política de persistencia en vigor y las direcciones virtuales, el iniciador o los destinos de almacenamiento se establecen en una partición del dispositivo CNA, no restablezca ni borre los valores configurados para las direcciones virtuales, el iniciador y los destinos de almacenamiento antes de cambiar el modo de virtualización o la personalidad de la partición. La acción se llevará a cabo de manera automática al deshabilitar la política de persistencia. También puede utilizar un trabajo de configuración para establecer explícitamente los atributos de la dirección virtual en 0 y los valores del iniciador y los destinos de almacenamiento como se define en Valores predeterminados para el destino de almacenamiento y el iniciador iSCSI.

Configuración de la política de persistencia mediante la interfaz web de iDRAC

Para configurar la política de persistencia:

1 En la interfaz web de iDRAC, vaya a **Configuración** > **Configuración del sistema** > **Optimización de la identidad de E/S**.

2 Haga clic en la ficha **Optimización de identidad de E/S**.

3 En la sección **Política de persistencia**, seleccione una o varias de las siguientes opciones para cada política de persistencia:
   - **Restablecimiento mediante sistema operativo**: la dirección virtual o los valores de destino se conservan cuando se producen condiciones de reinicio mediante sistema operativo.
   - **Reinicio mediante suministro de energía**: la dirección virtual o los valores de destino se conservan cuando se producen condiciones de restablecimiento mediante suministro de energía.
   - **Pérdida de alimentación de CA**: la dirección virtual o los valores de destino se conservan cuando se producen condiciones de pérdida de la alimentación de CA.

4 Haga clic en **Aplicar**.

   Se configuran las políticas de persistencia.

Configuración de la política de persistencia mediante RACADM

Para configurar la política de persistencia, use el objeto racadm siguiente con el subcomando **set**:

- Para las direcciones virtuales, utilice los objetos **iDRAC.IOIDOpt.VirtualAddressPersistencePolicyAuxPwrd** e **iDRAC.IOIDOpt.VirtualAddressPersistencePolicyNonAuxPwrd**
- Para el iniciador, utilice el objeto **iDRAC.IOIDOPT.InitiatorPersistencePolicy**
- Para los destinos de almacenamiento, utilice el objeto **iDRAC.IOIDOpt.StorageTargetPersistencePolicy**

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

Valores predeterminados para el destino de almacenamiento y el iniciador iSCSI

En las siguientes tablas se proporciona la lista de valores predeterminados para el iniciador iSCSI y los destinos de almacenamiento cuando se borran las políticas de persistencia.

Tabla 33. Iniciador iSCSI: valores predeterminados

Iniciador iSCSI	Valores predeterminados en modo IPv4	Valores predeterminados en modo IPv6
IscsiInitiatorIpAddr	0.0.0.0	::
IscsiInitiatorIpv4Addr	0.0.0.0	0.0.0.0
IscsiInitiatorIpv6Addr	::	::
IscsiInitiatorSubnet	0.0.0.0	0.0.0.0
IscsiInitiatorSubnetPrefix	0	0
IscsiInitiatorGateway	0.0.0.0	::
IscsiInitiatorIpv4Gateway	0.0.0.0	0.0.0.0
IscsiInitiatorIpv6Gateway	::	::
IscsiInitiatorPrimDns	0.0.0.0	::
IscsiInitiatorIpv4PrimDns	0.0.0.0	0.0.0.0
IscsiInitiatorIpv6PrimDns	::	::
IscsiInitiatorSecDns	0.0.0.0	::
IscsiInitiatorIpv4SecDns	0.0.0.0	0.0.0.0
IscsiInitiatorIpv6SecDns	::	::
IscsiInitiatorName	Valor borrado	Valor borrado
IscsiInitiatorChapId	Valor borrado	Valor borrado
IscsiInitiatorChapPwd	Valor borrado	Valor borrado
IPVer	Ipv4	

Tabla 34. Atributos de destino de almacenamiento iSCSI: valores predeterminados

Atributos de destino de Almacenamiento iSCSI	Valores predeterminados en modo IPv4	Valores predeterminados en modo IPv6
ConnectFirstTgt	Desactivado	Desactivado
FirstTgtIpAddress	0.0.0.0	::
FirstTgtTcpPort	3260	3260
FirstTgtBootLun	0	0
FirstTgtIscsiName	Valor borrado	Valor borrado
FirstTgtChapId	Valor borrado	Valor borrado
FirstTgtChapPwd	Valor borrado	Valor borrado
FirstTgtIpVer	Ipv4	
ConnectSecondTgt	Desactivado	Desactivado
SecondTgtIpAddress	0.0.0.0	::
SecondTgtTcpPort	3260	3260
SecondTgtBootLun	0	0
SecondTgtIscsiName	Valor borrado	Valor borrado
SecondTgtChapId	Valor borrado	Valor borrado
SecondTgtChapPwd	Valor borrado	Valor borrado
SecondTgtIpVer	Ipv4	

15

Administración de dispositivos de almacenamiento

Empezando por la versión iDRAC 2.00.00.00, iDRAC amplía la administración sin agentes para incluir la configuración directa de las nuevas controladoras PERC9. Le permite configurar en forma remota los componentes de almacenamiento conectados al sistema en el momento de ejecución. Entre estos componentes se incluyen las controladoras RAID y no RAID, los canales, los puertos, los gabinetes y los discos conectados a estos componentes. Para los servidores PowerEdge de 14a generación, se admiten las controladoras PERC 9 y PERC 10.

La detección, topología, monitoreo de estado y configuración del subsistema de almacenamiento completos se realizan a través de la estructura de Administración incorporada integral (CEM) mediante la interconexión con las controladoras PERC internas y externas vía la interfaz de protocolo MCTP sobre I2C. Para realizar la configuración en tiempo real, CEM es compatible con las controladoras PERC9 y superiores. La versión de firmware para las controladoras PERC9 debe ser 9.1 o posterior.

NOTA: El S140 o RAID por software (SWRAID) no es compatible con CEM y, por lo tanto, no se admite en la GUI del iDRAC. SWRAID se puede administrar mediante la API de WSMan y RACADM.

Con iDRAC, es posible realizar la mayoría de las funciones que se encuentran disponibles en OpenManage Storage Management, lo que incluye los comandos de configuración (sin reinicio) en tiempo real (por ejemplo, la creación de un disco virtual). También se puede configurar RAID en forma completa antes de instalar el sistema operativo.

Es posible configurar y administrar las funciones de la controladora sin obtener acceso al BIOS. Estas funciones incluyen la configuración de discos virtuales y la aplicación de niveles de RAID y repuestos dinámicos para la protección de los datos. Es posible iniciar muchas otras funciones de la controladora, como la recreación y la solución de problemas. Para proteger los datos, se puede configurar la redundancia de datos o asignar repuestos dinámicos.

Los dispositivos de almacenamiento son:

- Controladoras: la mayoría de los sistemas operativos no leen y escriben datos directamente desde los discos, sino que envían instrucciones de lectura y escritura a una controladora. La controladora es el hardware de su sistema que interactúa directamente con los discos para escribir y recuperar datos. Una controladora tiene conectores (canales o puertos) que están conectados a uno o más discos físicos o un gabinete que contenga discos físicos. Las controladoras de RAID pueden extender los límites de los discos para crear un espacio de almacenamiento ampliado (o un disco virtual) con la capacidad de más de un disco. Las controladoras también realizan otras tareas, como el inicio de recreaciones, la inicialización de discos y mucho más. Para completar sus tareas, las controladoras requieren un software especial, conocido como firmware y controladores. Para funcionar correctamente, la controladora debe tener instalados la versión mínima requerida del firmware y los controladores. Diferentes controladoras tienen características diferentes de leer y escribir datos, como también de ejecutar tareas. Se recomienda comprender dichas funciones para administrar el almacenamiento más eficientemente.
- Los discos o dispositivos físicos residen dentro de un gabinete o están conectados a la controladora. En una controladora RAID, los discos o dispositivos físicos se utilizan para crear discos virtuales.
- Disco virtual: es el almacenamiento creado por una controladora RAID a partir de uno o varios discos físicos. Si bien se puede crear un disco virtual a partir de varios discos físicos, el sistema operativo lo percibirá como un solo disco. Según el nivel RAID usado, el disco virtual puede retener datos redundantes debido a la falla de un disco o en caso de tener atributos de rendimiento particulares. Los discos virtuales solo se pueden crear en una controladora RAID.
- Gabinete: se conecta al sistema de manera externa, mientras que el plano posterior y los discos físicos son internos.
- Plano posterior: es similar a un gabinete. En un plano posterior, el conector de la controladora y los discos físicos se conectan a un gabinete, pero no pueden contar con las funciones de administración (sondas de temperatura, alarmas, etc.) asociadas con los gabinetes externos. Los discos físicos se pueden contener en un gabinete o conectarse al plano posterior de un sistema.

Además de administrar los discos físicos del gabinete, puede supervisar el estado de los ventiladores, la fuente de alimentación y las sondas de temperatura del gabinete. Se pueden conectar gabinetes con acoplamiento activo. El acoplamiento activo se define como la adición de un componente a un sistema mientras el sistema operativo aún está ejecutándose.

Los dispositivos físicos conectados a la controladora deben contar con el firmware más reciente. Para obtener el firmware admitido más reciente, póngase en contacto con su proveedor de servicio.

Los sucesos de almacenamiento procedentes de PERC se asignan a capturas SNMP y sucesos WSMan, según corresponda. Todos los cambios en las configuraciones de almacenamiento se registran en el Registro de Lifecycle.

Capacidad de PERC	Controladora compatible con configuración CEM (PERC 9.1 o posterior)	Controladora no compatible con configuración CEM (PERC 9.0 y anterior)
Real-time (tiempo real)	**NOTA: Para los servidores PowerEdge de 14a generación, se admiten las controladoras PERC 9 y PERC 10.** Si no existen trabajos programados o pendientes para la controladora, se aplica la configuración. Si existen trabajos programados o pendientes para esa controladora, es necesario borrar los trabajos o esperar que los trabajos se completen antes de aplicar la configuración en el momento de ejecución. La ejecución en el momento o en tiempo real implica que no es necesario reiniciar el sistema.	Se aplicará la configuración. Aparece un mensaje de error. La creación de trabajos no se ejecutó correctamente y no se pueden crear trabajos en tiempo real mediante la interfaz web.
Organizado en etapas	Si todas las operaciones de configuración se establecen en etapas, la configuración se organiza en etapas y se aplica después de reiniciar el sistema o se aplica en tiempo real.	Se aplicará la configuración después del reinicio.

Temas:

Comprensión de los conceptos de RAID

Storage Management utiliza la tecnología de arreglo redundante de discos independientes (RAID) para proporcionar capacidad a Storage Management. Para entender Storage Management es necesario comprender los conceptos de RAID, como también estar familiarizado con las controladoras RAID y el espacio de disco de la vista del sistema operativo de su sistema.

¿Qué es RAID?

RAID es una tecnología para administrar el almacenamiento de datos en los discos físicos que residen en el sistema o están conectados al mismo. Un aspecto clave de RAID es la capacidad de organizar los discos físicos en tramos, de modo que la capacidad de almacenamiento combinada de varios discos físicos pueda ser tratada como un único espacio de disco ampliado. Otro aspecto clave de RAID es la capacidad de mantener datos redundantes que pueden utilizarse para restaurar datos en caso de una falla del disco. RAID usa técnicas diferentes, como es el seccionamiento, el reflejado y la paridad para almacenar y reconstruir los datos. Hay distintos niveles de RAID que usan métodos diferentes para almacenar y reconstruir datos. Los niveles de RAID tienen características diferentes en cuanto a rendimiento de lectura/escritura, protección de datos y capacidad de almacenamiento. No todos los niveles de RAID mantienen datos redundantes, lo que significa que, para algunos niveles de RAID, los datos perdidos no pueden ser restaurados. La elección de un nivel de RAID depende de si su prioridad es el rendimiento, la protección o la capacidad de almacenamiento.

NOTA: El Consejo consultivo de RAID (RAB) define las especificaciones que se utilizan para poner en práctica la tecnología RAID. Aunque el RAB define los niveles de RAID, la implementación comercial de los niveles de RAID por distintos proveedores puede variar con respecto a las especificaciones de RAID reales. La implementación que utiliza un proveedor en particular puede afectar el rendimiento de lectura y escritura, así como el grado de redundancia de los datos.

RAID por hardware y software

RAID puede implementarse mediante hardware o software. Un sistema que usa el RAID por hardware tiene una controladora RAID que implementa los niveles RAID y procesa la lectura y escritura de los datos en los discos físicos. Cuando se usa el RAID por software proporcionado por el sistema operativo, este implementa los niveles RAID. Por esta razón, la utilización del RAID por software por sí misma puede reducir el rendimiento del sistema. Sin embargo, puede usar el RAID por software con volúmenes de RAID por hardware para proporcionar un mejor rendimiento y variedad en la configuración de volúmenes de RAID. Por ejemplo, puede reflejar un par de volúmenes de RAID 5 por hardware en dos controladoras RAID a fin de proporcionar redundancia de la controladora RAID.

Conceptos de RAID

RAID usa técnicas particulares para escribir datos en los discos. Estas técnicas permiten que RAID proporcione una redundancia de datos o un mejor rendimiento. Estas técnicas incluyen:

- Reflejado: duplicación de datos de un disco físico a otro. El reflejado proporciona redundancia de datos al mantener dos copias de los mismos datos en discos físicos distintos. Si uno de los discos en el reflejo falla, el sistema puede continuar funcionando si utiliza el disco que no está afectado. En todo momento, ambos lados del reflejo contienen los mismos datos. Cualquier lado del reflejo puede actuar como el lado operativo. El grupo de discos RAID reflejado es comparable en rendimiento a un grupo de discos RAID 5 con respecto a las operaciones de lectura, pero es más rápido en lo que respecta a las operaciones de escritura.
- Seccionamiento: el seccionamiento de discos escribe datos en todos los discos físicos de un disco virtual. Cada sección consta de direcciones de datos de disco virtual consecutivos que se asignan en unidades de tamaño fijo a cada disco físico del disco virtual usando un patrón secuencial. Por ejemplo, si el disco virtual incluye cinco discos físicos, la sección escribe datos en los discos físicos del uno al cinco sin repetir ninguno de los discos físicos. La cantidad de espacio que consume una sección es la misma en todos los discos físicos. La parte de una sección que reside en un disco físico es un elemento de la sección. El seccionamiento por sí mismo no proporciona redundancia de datos. El seccionamiento en combinación con la paridad sí proporciona redundancia de datos.
- Tamaño de la sección: el espacio total en disco consumido por una sección, sin incluir un disco de paridad. Por ejemplo, considere una sección que contiene 64 KB de espacio en el disco y que tiene 16 KB de datos que residen en cada disco de la sección. En este caso, el tamaño de la sección es de 64 KB y el tamaño del elemento de la sección es de 16 KB.
- Elemento de la sección: un elemento de la sección es la porción de una sección que reside en un solo disco físico.

- Tamaño del elemento de la sección: cantidad de espacio en disco consumida por un elemento de la sección. Por ejemplo, considere una sección que contiene 64 KB de espacio en el disco y que tiene 16 KB de datos que residen en cada disco de la sección. En este caso, el tamaño del elemento de la sección es de 16 KB y el tamaño de la sección es de 64 KB.
- Paridad: la paridad se refiere a datos redundantes que se mantienen utilizando un algoritmo junto con el seccionamiento. Cuando uno de los discos seccionados falla, los datos se pueden reconstruir a partir de la información de paridad que utiliza el algoritmo.
- Tramo: un tramo es una técnica de RAID que se utiliza para combinar espacio de almacenamiento de grupos de discos físicos en un disco virtual RAID 10, 50 o 60.

Niveles RAID

Cada nivel de RAID usa alguna combinación de reflejado, seccionamiento y paridad para proporcionar redundancia de datos o un mejor rendimiento de lectura y escritura. Para obtener información específica sobre cada nivel de RAID, consulte Elección de niveles de Raid.

Organización del almacenamiento de datos para obtener disponibilidad y rendimiento

RAID proporciona distintos métodos o niveles RAID para organizar el almacenamiento de disco. Algunos niveles RAID mantienen datos redundantes para que usted pueda restaurar los datos después de una falla del disco. Los distintos niveles RAID pueden implicar también un aumento o disminución en el rendimiento de E/S (lectura y escritura) del sistema.

El mantenimiento de datos redundantes requiere el uso de discos físicos adicionales. Al aumentar la cantidad de discos, aumenta la probabilidad de falla de un disco. A causa de las diferencias en la redundancia y el rendimiento de E/S, un nivel RAID puede ser más apropiado que otro, según las aplicaciones que se utilicen en el entorno operativo y la naturaleza de los datos que se almacenen.

Al elegir un nivel RAID, se aplican las siguientes consideraciones de rendimiento y costos:

- Disponibilidad o tolerancia a fallas: la disponibilidad o tolerancia a fallas se refiere a la capacidad de un sistema para mantener las operaciones y proporcionar acceso a los datos aun cuando uno de sus componentes ha fallado. En los volúmenes de RAID, la disponibilidad o tolerancia a fallas se consigue manteniendo datos redundantes. Los datos redundantes incluyen reflejos (datos duplicados) e información de paridad (reconstrucción de los datos mediante un algoritmo).
- Rendimiento: el rendimiento de lectura y escritura puede aumentar o disminuir según el nivel RAID que elija. Algunos niveles RAID pueden ser más apropiados para ciertas aplicaciones.
- Rentabilidad: el mantenimiento de datos redundantes o de información de paridad en relación a volúmenes de RAID requiere de espacio de disco adicional. En situaciones en las que los datos son temporales, de fácil reproducción o no esenciales, es posible que no se justifique el aumento en el costo de la redundancia de datos.
- Tiempo promedio entre fallas (MTBF): el uso de discos adicionales para mantener la redundancia de los datos también aumenta la probabilidad de sufrir fallas de disco en un momento dado. Aunque esto no se puede evitar en situaciones en las que los datos redundantes son una necesidad, puede repercutir en la carga de trabajo del personal de asistencia de sistemas de su organización.
- Volumen: el volumen se refiere a un solo disco virtual no RAID. Puede crear volúmenes mediante utilidades externas, como el O-ROM <Ctrl> <r>. Storage Management no admite la creación de volúmenes. Sin embargo, puede ver volúmenes y usar unidades de estos volúmenes para crear nuevos discos virtuales o para la Expansión de capacidad en línea (OCE) de los discos virtuales existentes, siempre que disponga de espacio libre.

Elección de niveles RAID

Se puede usar RAID para controlar el almacenamiento de datos en varios discos. Cada nivel RAID o concatenación presenta distintos rendimientos y características para la protección de datos.

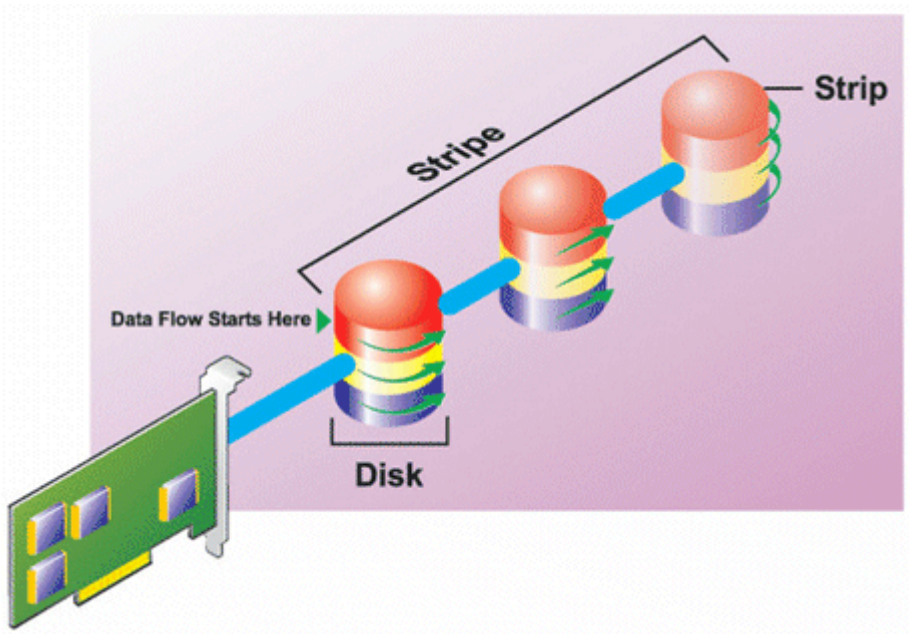
NOTA: Las controladoras PERC H3xx no admiten los niveles de RAID 6 y 60.

En los temas siguientes se proporciona información específica acerca de la forma en la que cada nivel RAID almacena los datos, así como sus características de protección y rendimiento:

- Nivel RAID 0 (seccionamiento)
- Nivel RAID 1 (reflejado)
- Nivel RAID 5 (seccionamiento con paridad distribuida)
- Nivel RAID 6 (seccionamiento con paridad distribuida adicional)
- Nivel RAID 50 (seccionamiento en conjuntos de RAID 5)
- Nivel RAID 60 (seccionamiento en conjuntos de RAID 6)
- Nivel RAID 10 (seccionamiento de conjuntos reflejados)

Nivel RAID 0 (seccionamiento)

RAID 0 utiliza el seccionamiento de datos, que consiste en escribir los datos en segmentos del mismo tamaño entre los discos físicos. RAID 0 no proporciona redundancia de datos.

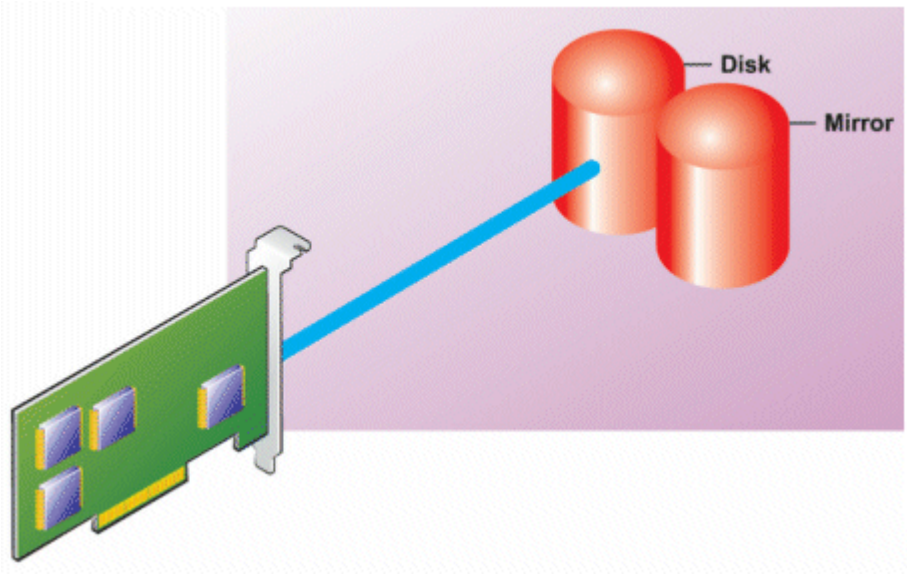


Características de RAID 0:

- Agrupa *n* discos en un disco virtual grande con una capacidad total de (tamaño de disco más pequeño)*n discos.
- Los datos se guardan en los discos alternadamente.
- No se mantiene la redundancia de los datos. Cuando un disco falla, el disco virtual grande fallará sin que haya alguna manera de recrear los datos.
- Mejor rendimiento de lectura y escritura.

Nivel RAID 1 (reflejado)

RAID 1 es la forma más sencilla de mantener datos redundantes. En RAID 1, los datos se reflejan o se duplican en uno o varios discos físicos. Si un disco físico genera errores, los datos se pueden recrear utilizando los datos del otro lado del reflejado.

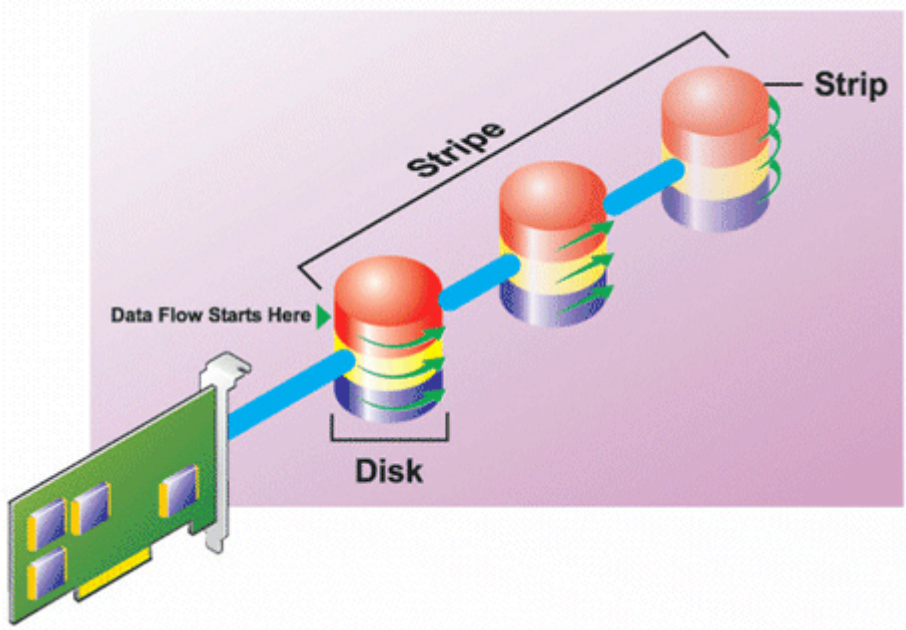


Características de RAID 1:

- Agrupa *n* + *n* discos en un disco virtual con capacidad de *n* discos. Las controladoras que actualmente son admitidas por Storage Management permiten seleccionar dos discos cuando se crea un RAID 1. Debido a que estos discos están reflejados, la capacidad total de almacenamiento equivale a un disco.
- Los datos se copian en ambos discos.
- Cuando un disco falla, el disco virtual continúa funcionando. Los datos se leen del reflejado del disco que presentó errores.
- Mejor rendimiento de lectura, pero un rendimiento de escritura ligeramente menor.
- Hay redundancia para la protección de datos.
- RAID 1 es más costoso en términos de espacio de disco, ya que se utiliza el doble de discos de lo que se requiere para almacenar los datos sin redundancia.

Nivel RAID 5 (seccionamiento con paridad distribuida)

RAID 5 proporciona redundancia de datos al utilizar el seccionamiento de datos en combinación con la información de paridad. En lugar de dedicar un disco físico a la paridad, la información de paridad se secciona entre todos los discos físicos en el grupo de discos.

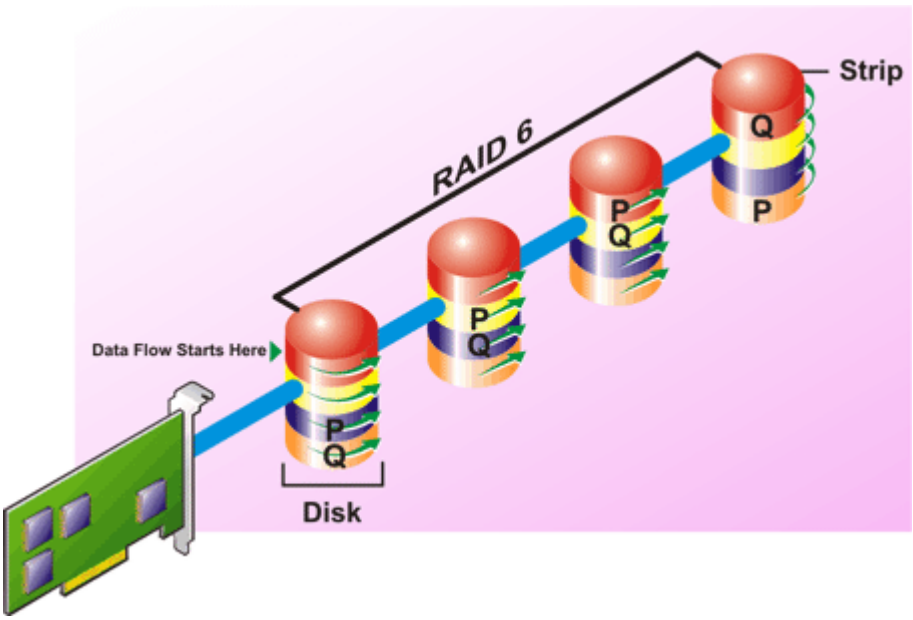


Características de RAID 5:

- Agrupa *n* discos en un disco virtual grande con capacidad de (*n*-1) discos.
- La información redundante (paridad) se almacena alternadamente entre todos los discos.
- Cuando un disco falla, el disco virtual seguirá funcionando, pero funcionará en estado degradado. Los datos se reconstruyen a partir de los discos que sobrevivan.
- Mejor rendimiento de lectura, pero un rendimiento de escritura más lento.
- Hay redundancia para la protección de datos.

Nivel RAID 6 (seccionamiento con paridad distribuida adicional)

RAID 6 proporciona redundancia de datos al utilizar el seccionamiento de datos en combinación con la información de paridad. Al igual que en RAID 5, la paridad se distribuye dentro de cada sección. Sin embargo, RAID 6 utiliza un disco físico adicional para mantener la paridad, de manera que cada sección en el grupo de discos mantiene dos bloques de disco con información de paridad. La paridad adicional proporciona protección de datos en el caso de dos fallas de disco. En la siguiente imagen, los dos conjuntos de información de paridad se identifican como **P** y **Q**.



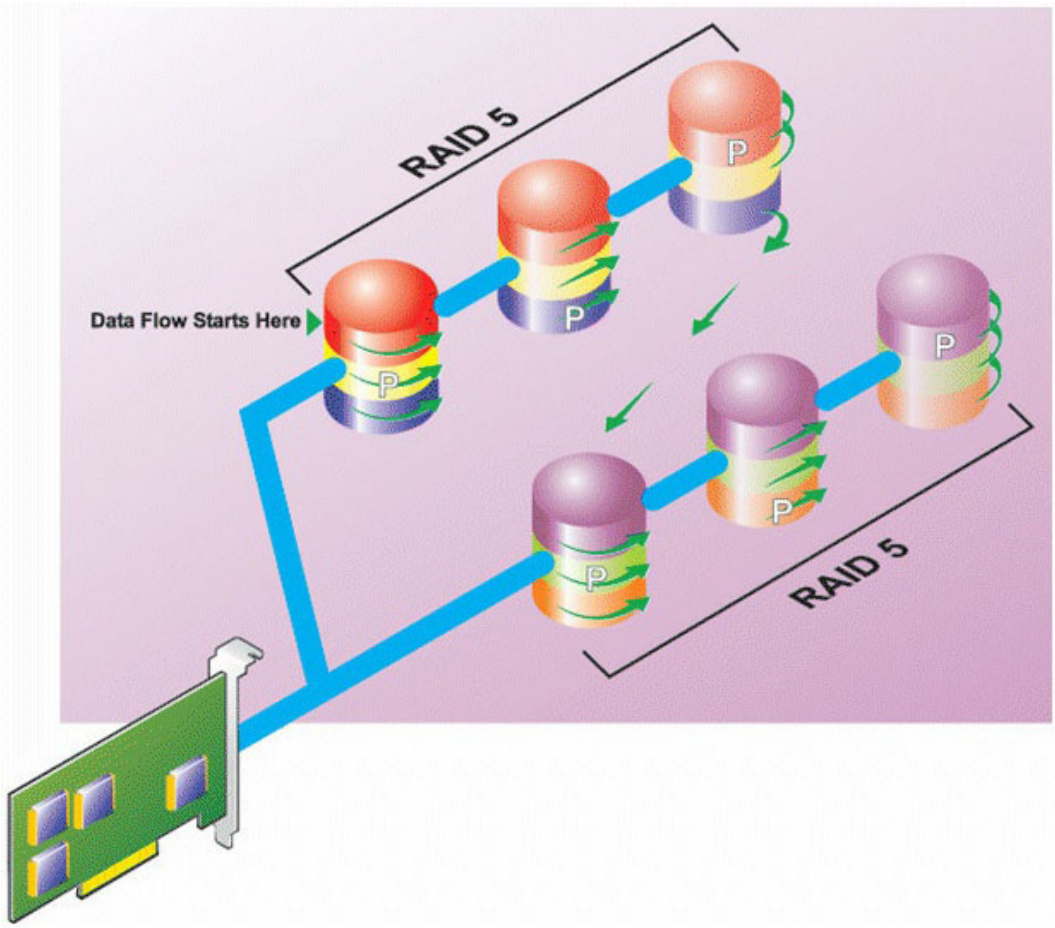
Características de RAID 6:

- Agrupa *n* discos en un disco virtual grande con capacidad de (*n*-2) discos.
- La información redundante (paridad) se almacena alternadamente entre todos los discos.
- El disco virtual sigue funcionando hasta con dos fallas de disco. Los datos se reconstruyen de los disco que siguen funcionando.
- Mejor rendimiento de lectura, pero un rendimiento de escritura más lento.
- Mayor redundancia para la protección de datos.
- Se requieren dos discos por tramo para la paridad. RAID 6 es más costoso en términos de espacio de disco.

Nivel RAID 50 (seccionamiento en conjuntos de RAID 5)

RAID 50 implementa el seccionamiento en más de un tramo de discos físicos. Por ejemplo, un grupo de discos RAID 5 que esté implementado con tres discos físicos y, luego, continúa con un grupo de tres discos físicos adicionales, sería un RAID 50.

Es posible implementar RAID 50 aun si el hardware no lo admite directamente. En este caso, puede establecer varios discos virtuales de RAID 5 y, luego, convertir los discos RAID 5 en discos dinámicos. Luego, puede crear un volumen dinámico que se extienda a todos los discos virtuales RAID 5.

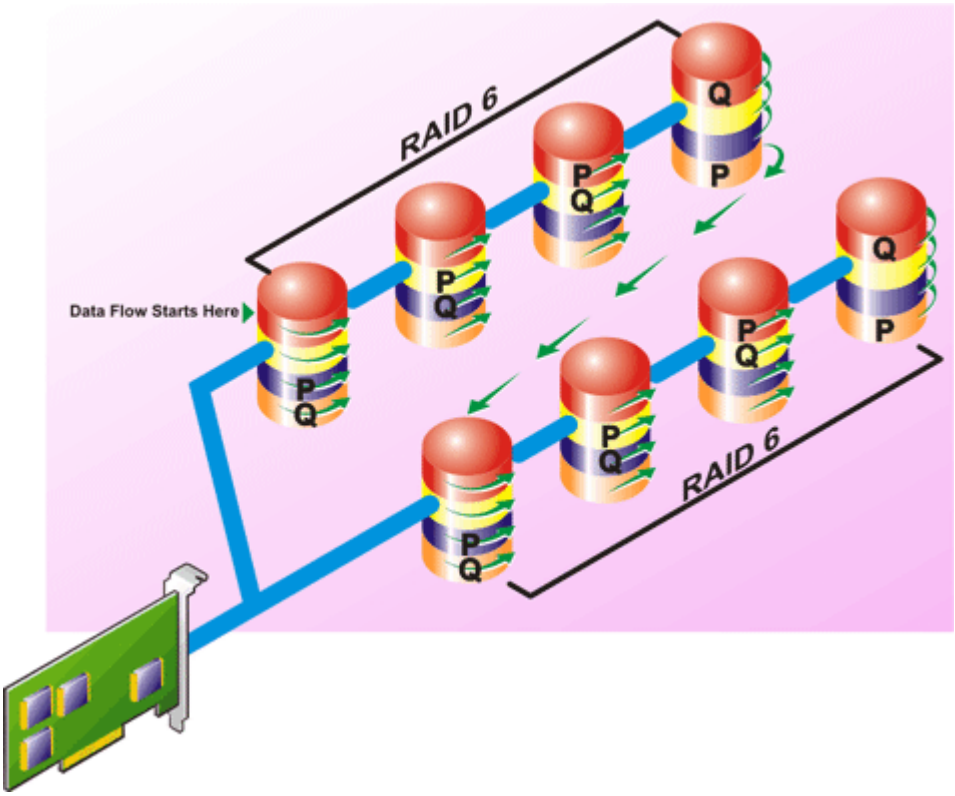


Características de RAID 50:

- Agrupa *n***s* discos para formar un disco virtual grande con capacidad de *s**(*n*-1) discos, en donde *s* representa el número de tramos y *n* es el número de discos dentro de cada tramo.
- La información redundante (paridad) se almacena alternadamente en todos los discos de cada tramo de RAID 5.
- Mejor rendimiento de lectura, pero un rendimiento de escritura más lento.
- Se requiere tanta información de paridad como en RAID 5 convencional.
- Los datos se seccionan en todos los tramos. RAID 50 es más costoso en términos de espacio de disco.

Nivel RAID 60 (seccionamiento en conjuntos de RAID 6)

RAID 60 es el seccionamiento en más de un tramo de discos físicos configurados como un RAID 6. Por ejemplo, un grupo de discos RAID 6 que esté implementado con cuatro discos físicos y, luego, continúa con un grupo de cuatro discos físicos adicionales, sería un RAID 60.

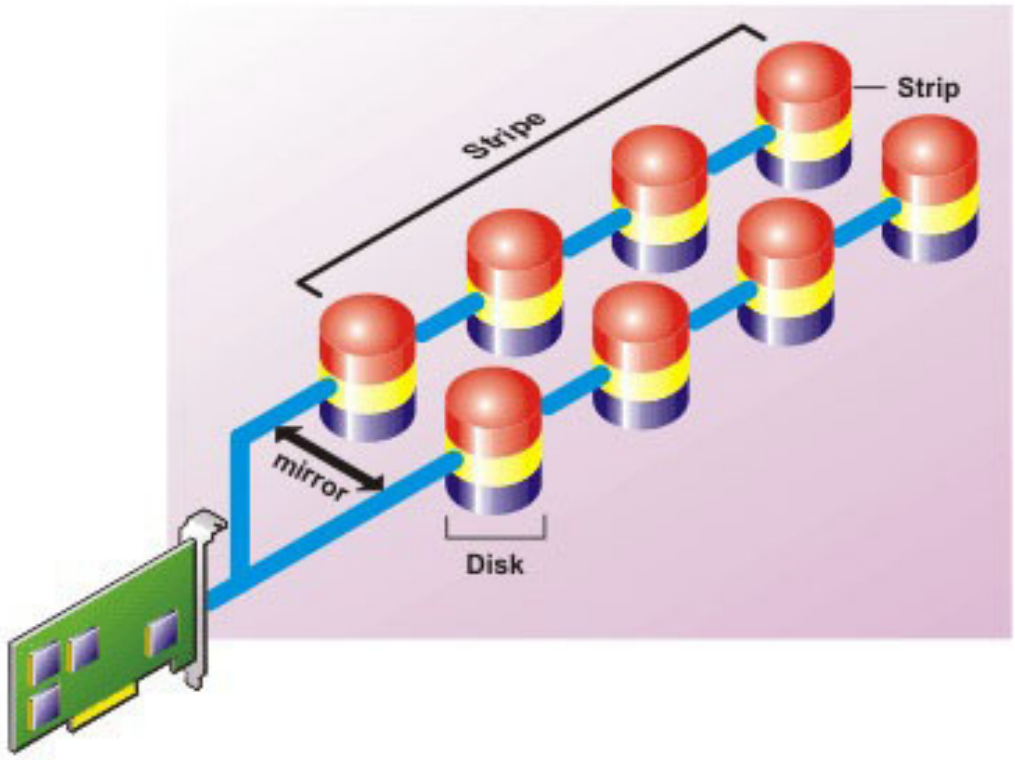


Características de RAID 60:

- Agrupa *n***s* discos para formar un disco virtual grande con capacidad de *s**(*n*-2) discos, en donde *s* representa el número de tramos y *n* es el número de discos dentro de cada tramo.
- La información redundante (paridad) se almacena alternadamente en todos los discos de cada tramo de RAID 6.
- Mejor rendimiento de lectura, pero un rendimiento de escritura más lento.
- La redundancia aumentada proporciona mayor protección de datos que un RAID 50.
- Proporcionalmente, requiere de tanta información de paridad como el RAID 6.
- Se requieren dos discos por tramo para la paridad. RAID 60 es más costoso en términos de espacio de disco.

Nivel RAID 10 (reflejos seccionados)

El RAB considera que el nivel RAID 10 es una implementación del nivel RAID 1. RAID 10 combina los discos físicos reflejados (RAID 1) con el seccionamiento de datos (RAID 0). Con RAID 10, los datos se seccionan en varios discos físicos. Luego, el grupo de discos seccionados se refleja en otro conjunto de discos físicos. RAID 10 se puede considerar un *reflejo de secciones*.



Características de RAID 10:

- Agrupa *n* discos en un disco virtual grande con una capacidad total de (*n*/2) discos, en donde *n* es un número entero par.
- Las imágenes de reflejo de los datos son seccionadas en conjuntos de discos físicos. Este nivel proporciona redundancia por medio del reflejado.
- Cuando un disco falla, el disco virtual continúa funcionando. Los datos se leen del disco del par reflejado que sigue funcionando.
- Rendimiento de lectura mejorado y rendimiento de escritura.
- Hay redundancia para la protección de datos.

Comparación de rendimiento de niveles RAID

La siguiente tabla compara las características de rendimiento asociadas a los niveles de RAID más comunes. Esta tabla proporciona las pautas generales para elegir un nivel de RAID. Evalúe los requisitos específicos de su entorno antes de elegir un nivel de RAID.

Tabla 35. Comparación de rendimiento de niveles RAID

Nivel RAID	Disponibilidad de datos	Rendimiento de lectura	Rendimiento de escritura	Rendimiento de recreación	Discos mínimos requeridos	Usos sugeridos
RAID 0	Ninguno	Muy bueno	Muy bueno	N/A	N	Datos no críticos.
RAID 1	Excelente	Muy bueno	En buen estado	En buen estado	2N (N = 1)	Pequeñas bases de datos, registros de base de datos, información crítica.

Nivel RAID	Disponibilidad de datos	Rendimiento de lectura	Rendimiento de escritura	Rendimiento de recreación	Discos mínimos requeridos	Usos sugeridos
RAID 5	En buen estado	Lecturas secuenciales: Bueno. Lecturas transaccionales: Muy bueno	Aceptable, a menos que se utilice la escritura no simultánea de la memoria caché	Aceptable	N + 1 (N = por lo menos dos discos)	Bases de datos y otros usos transaccionales de lecturas intensivas.
RAID 10	Excelente	Muy bueno	Aceptable	En buen estado	2N x X	Entornos con intensidad de datos (registros grandes).
RAID 50	En buen estado	Muy bueno	Aceptable	Aceptable	N + 2 (N = por lo menos 4)	Usos transaccionales de tamaño medio o usos con intensidad de datos.
RAID 6	Excelente	Lecturas secuenciales: Bueno. Lecturas transaccionales: Muy bueno	Aceptable, a menos que se utilice la escritura no simultánea de la memoria caché	Pobre	N + 2 (N = por lo menos dos discos)	Información crítica. Bases de datos y otros usos transaccionales de lecturas intensivas.
RAID 60	Excelente	Muy bueno	Aceptable	Pobre	X x (N + 2) (N = por lo menos 2)	Información crítica. Usos transaccionales de tamaño medio o usos con intensidad de datos.
N = cantidad de discos físicos X = cantidad de conjuntos RAID						

Controladoras admitidas

Controladoras RAID admitidas

Las interfaces de iDRAC son compatibles con las siguientes controladoras PERC10:

- Mini PERC H740P
- PERC H740P Adapter
- PERC H840 Adapter

Las interfaces de iDRAC son compatibles con las siguientes controladoras PERC9:

- Mini PERC H330
- Adaptador PERC H330

- Mini PERC H730P
- Adaptador PERC H730P

Controladoras no RAID admitidas

La interfaz del iDRAC admite una controladora externa de SAS HBA de 12 Gbps y HBA330 Mini o controladores de adaptador.

Gabinetes admitidos

iDRAC es compatible con gabinetes MD1400 y MD1420.

NOTA: No se admite el arreglo redundante de discos económicos (RBODS) conectados a las controladoras HBA.

NOTA: Para la versión de iDRAC 3.00.00.00, la conexión encadenada de gabinetes no es compatible con H840. Sólo se permite un gabinete por puerto.

Resumen de funciones admitidas para Storage Devices (Dispositivos de almacenamiento)

La siguiente tabla proporciona las funciones admitidas por los dispositivos de almacenamiento a través de iDRAC.

NOTA: Funciones tales como preparar para quitar y hacer parpadear o dejar de hacer parpadear el LED del componente no se aplican a las tarjetas SSD PCIe HHHL.

Nombre de la función	Controladoras PERC 10				Controladoras PERC 9				SSD PCIe
	Mini H740P	Adaptador H740P	Adaptador H840	Mini H330	Adaptador H330	Mini H730P	Adaptador H730P	FD33xS	
Asignar o desasignar un disco físico como un repuesto dinámico global	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Not applicable
Convertir a RAID/No RAID,	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Not applicable
Borrado seguro	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Not applicable
Recreación	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Not applicable
Cancelar recreación	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Not applicable

Nombre de la función	Controladoras PERC 10				Controladoras PERC 9				SSD PCIe
	Mini H740P	Adaptador H740P	Adaptador H840	Mini H330	Adaptador H330	Mini H730P	Adaptador H730P	FD33xS	
Crear discos virtuales	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Not applicable
Cambiar el nombre de los discos virtuales									
Editar las políticas de la caché de los discos virtuales	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Not applicable
Ejecutar una revisión de congruencia en el disco virtual	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Not applicable
Cancelar revisión de congruencia	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Not applicable
Inicializar discos virtuales	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Not applicable
Cancelar inicialización	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Not applicable
Cifrar discos virtuales	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Not applicable	Not applicable	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Not applicable
Asignar o desasignar repuestos dinámicos dedicados	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Not applicable
Eliminar discos virtuales	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Not applicable
Cancelar inicialización de segundo plano	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Not applicable

Nombre de la función	Controladoras PERC 10				Controladoras PERC 9				SSD PCIe
	Mini H740P	Adaptador H740P	Adaptador H840	Mini H330	Adaptador H330	Mini H730P	Adaptador H730P	FD33xS	
Expansión de la capacidad en línea	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Not applicable
Migración de nivel de RAID	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Not applicable
Descartar caché preservada	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Not applicable	Not applicable	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Not applicable
Establecer modo de lectura de patrullaje	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Not applicable
Modo de lectura de patrullaje manual	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Not applicable
Áreas de lectura de patrullaje no configuradas	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Tiempo real (solo en la interfaz de web)	Tiempo real (solo en la interfaz de web)	Tiempo real (solo en la interfaz de web)	Tiempo real (solo en la interfaz de web)	Tiempo real (solo en la interfaz de web)	Not applicable
Modo de revisión de congruencia	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Not applicable
Modo de escritura diferida	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Not applicable
Modo de equilibrio de carga	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Not applicable
Porcentaje de revisión de congruencia	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Not applicable

Nombre de la función	Controladoras PERC 10				Controladoras PERC 9				SSD PCIe
	Mini H740P	Adaptador H740P	Adaptador H840	Mini H330	Adaptador H330	Mini H730P	Adaptador H730P	FD33xS	
Porcentaje de recreación	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Not applicable
Porcentaje de inicialización de segundo plano	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Not applicable
Porcentaje de reconstrucción	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Not applicable
Importar configuración ajena	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Not applicable
Importar configuración ajena automáticamente	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Not applicable
Borrar configuración ajena	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Not applicable
Restablecer configuración de la controladora	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Not applicable
Crear o cambiar claves de seguridad	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Not applicable	Not applicable	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Not applicable
Inventario y supervisar de forma remota la condición de los dispositivos SSD PCIe	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Real-time (tiempo real)
Preparar para quitar SSD PCIe	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Real-time (tiempo real)
Borrar los datos de manera segura	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Not applicable	Not applicable	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Organizado en etapas

Nombre de la función	Controladoras PERC 10				Controladoras PERC 9				SSD PCIe
	Mini H740P	Adaptador H740P	Adaptador H840	Mini H330	Adaptador H330	Mini H730P	Adaptador H730P	FD33xS	
Configurar el modo de plano posterior (dividido/unificado)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Not applicable
Hacer parpadear o dejar de hacer parpadear LED de componentes	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)	Real-time (tiempo real)
Cambiar modo de la controladora	Not applicable	Not applicable	Not applicable	Organizado en etapas	Organizado en etapas	Organizado en etapas	Organizado en etapas	Organizado en etapas	Not applicable
Soporte de T10PI para discos virtuales	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable

NOTA: PERC 10 ya no admite la conversión de unidades a No RAID, la conversión de la controladora al modo HBA y el soporte de tramo dispar RAID 10.

Inventario y supervisión de dispositivos de almacenamiento

Es posible supervisar de manera remota la condición y ver el inventario de los siguientes dispositivos de almacenamiento con capacidad CEM (administración incorporada completa) en el sistema administrador mediante la interfaz web de iDRAC:

- Controladoras RAID, controladoras no RAID y extensores de PCIe
- Gabinetes que incluyen módulos de administración de gabinetes (EMM), suministros de energía, sonda de ventilador y sonda de temperatura
- Discos físicos
- Discos virtuales
- Baterías

También se muestran los sucesos de almacenamiento recientes y la topología de los dispositivos de almacenamiento.

Se generan alertas y capturas SNMP para sucesos de almacenamiento. Los sucesos se registran en el registro de Lifecycle.

NOTA: Si enumere el comando WSMan de la vista del gabinete en un sistema mientras que un cable de PSU se ha extraído, el estado principal de la vista del gabinete se informa como en buen estado en lugar de advertencia.

NOTA: La recopilación del estado de almacenamiento sigue la misma convención del producto DellEMC OpenManage. Consulte la *Guía de usuario de DellEMC OpenManage Server Administrator*.

Supervisión de dispositivos de red mediante la interfaz web

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

- Vaya a **Almacenamiento** > **Descripción general** > **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 **Almacenamiento** > **Descripción general** > **Controladoras** para ver la información de la controladora RAID. Se mostrará la página **Controladoras**.

- Vaya a **Almacenamiento** > **Descripción general** > **Discos físicos** para ver la información de los discos físicos. Se mostrará la página **Discos físicos**.
- Vaya a **Almacenamiento** > **Descripción general** > **Discos virtuales** para ver la información de los discos virtuales. Se mostrará la página **Discos virtuales**.
- Vaya a **Almacenamiento** > **Descripción general** > **Gabinetes** para ver la información de los gabinetes. Aparecerá la página **Gabinetes**.

También puede utilizar filtros para ver información de un dispositivo específico.

NOTA: La lista de hardware de almacenamiento no se visualizará en caso de que el sistema no cuente con dispositivos de almacenamiento con soporte de CEM.

NOTA: Cuando las SSD NVMe se encuentran en modo RAID (detrás de S140), la interfaz web no muestra información de la ranura de la SSD NVMe en la página del gabinete. Para más información, consulte la página de discos físicos.

Para obtener más información acerca de las propiedades mostradas y el uso de las opciones de filtro, consulte la *Ayuda en línea de iDRAC*.

Supervisión de dispositivos de red mediante RACADM

Para ver la información del dispositivo de almacenamiento, utilice el comando **storage**.

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

Supervisión de plano posterior mediante la utilidad de configuración de iDRAC

En la utilidad de configuración de iDRAC, vaya a **Resumen del sistema**. Aparece la página **Resumen del sistema de la configuración de iDRAC**. La sección **Inventario de plano posterior** muestra información del plano posterior. Para obtener información acerca de los campos, consulte la *Ayuda en línea de la utilidad de configuración de iDRAC*.

Visualización de la topología de un dispositivo de almacenamiento

Es posible consultar la vista jerárquica de contención física de los componentes de almacenamiento clave, es decir, una lista de las controladoras, los gabinetes conectados a la controladora y un enlace al disco físico que contiene cada gabinete. También se muestran los discos físicos conectados directamente a la controladora.

Para ver la topología de los dispositivos de almacenamiento, vaya a **Descripción general** > **Almacenamiento**. La página **Descripción general** muestra la representación jerárquica de los componentes de almacenamiento en el sistema. Las opciones posibles son:

- Controladoras
- Discos físicos
- Discos virtuales
- Gabinetes

Haga clic en los vínculos para ver los detalles correspondientes a cada componente.

Administración de discos físicos

Es posible realizar las siguientes tareas para los discos físicos:

- Ver propiedades del disco físico.
- Asignar o desasignar un disco físico como un repuesto dinámico global.

- Convertir a disco con capacidad de RAID.
- Convertir a disco no RAID.
- Hacer parpadear o dejar de hacer parpadear el LED.
- Recrear el disco físico
- Cancelar la recreación del disco físico
- Borrado seguro

Asignación o desasignación de un disco físico como repuesto dinámico global

El repuesto dinámico global es un disco de reserva no utilizado que forma parte del grupo de discos. Los repuestos dinámicos permanecen en el modo de espera. Cuando un disco físico utilizado en un disco virtual falla, el repuesto dinámico asignado se activará con el fin de reemplazar el disco físico fallido sin interrumpir el sistema ni requerir de intervención. Cuando un repuesto dinámico se activa, recrea los datos de todos los discos virtuales redundantes que usaban el disco físico fallido.

NOTA: Desde iDRAC v2.30.30.30 o posterior, puede agregar repuestos dinámicos globales cuando los discos virtuales no se crean.

Puede cambiar la asignación del repuesto dinámico al desasignar un disco y elegir otro, según sea necesario. También puede asignar más de un disco físico como repuesto dinámico global.

Los repuestos dinámicos globales se deben asignar y desasignar manualmente. Estos no se asignan a discos virtuales específicos. Si desea asignar un repuesto dinámico a un disco virtual (reemplaza cualquier disco físico que falle en el disco virtual), consulte Asignación o desasignación de repuestos dinámicos dedicados.

Al eliminar discos virtuales, todos los repuestos dinámicos globales asignados se pueden desasignar automáticamente en el momento en que se elimina el último disco virtual asociado con la controladora.

Si se restablece la configuración, los discos virtuales se borran y todos los repuestos dinámicos se desasignan.

Es necesario estar familiarizado con los requisitos de tamaño y otras consideraciones relacionadas con los repuestos dinámicos.

Antes de asignar un disco físico como un repuesto dinámico global:

- Asegúrese de que Lifecycle Controller se encuentre activado.
- Si no existen unidades de disco disponibles en estado Listo, inserte unidades de disco adicionales y asegúrese de que las unidades se encuentren en estado Listo.
- Si los discos físicos están en modo no RAID, conviértalos a modo de RAID mediante las interfaces de iDRAC, como la interfaz web de iDRAC, RACADM, Redfish o WSMan, o <CTRL+R>.

  NOTA: Durante la POST, puede presionar <F2> para ingresar la configuración del sistema. La opción <CTRL+R> ya no es compatible con PERC 10, sólo funciona con PERC 9.

Si ha asignado un disco físico como repuesto dinámico global en el modo Agregar a operaciones pendientes, se crea la operación pendiente pero no se crea un trabajo. Por lo tanto, si intenta desasignar el mismo disco como repuesto dinámico global, la operación pendiente Asignar repuesto dinámico global se borra.

Si ha desasignado un disco físico como repuesto dinámico global en el modo Agregar a operaciones pendientes, se crea la operación pendiente pero no se crea un trabajo. Por lo tanto, si intenta asignar el mismo disco como repuesto dinámico global, la operación pendiente Desasignar repuesto dinámico global se borra.

Si se elimina el último VD, los repuestos dinámicos globales también vuelven al estado listo.

Si un PD ya es un repuesto dinámico global, el usuario aún puede asignarlo nuevamente como repuesto dinámico global.

Asignación o desasignación de un repuesto dinámico global mediante la interfaz web

Para asignar o desasignar un repuesto dinámico global para una unidad de disco físico:

1 En la interfaz web de iDRAC, vaya a **Descripción general** > **Almacenamiento** > **Discos físicos** > **Configuración**.

Se mostrará la página **Configuración de discos físicos**.

2 En el menú desplegable **Controladora**, seleccione la controladora para ver los discos físicos asociados.

3 Para asignar un repuesto dinámico global, en los menús desplegables de la columna **Acción: Asignar a todos**, seleccione **Repuesto dinámico global** para uno o varios discos físicos.

4 Para desasignar un repuesto dinámico, en los menús desplegables de la columna **Acción: Asignar a todos**, seleccione **Desasignar repuesto dinámico** para uno o varios discos físicos.

5 En el menú desplegable **Aplicar modo de operación**, seleccione el momento en que desea aplicar la configuración.

6 Haga clic en **Aplicar**.

Según el modo de operación seleccionado, se aplicará la configuración.

Asignación o desasignación de un repuesto dinámico global mediante RACADM

Utilice el comando **storage** y especifique el tipo como repuesto dinámico global.

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

Conversión de un disco físico en modo RAID a modo no RAID

La conversión de un disco físico a modo RAID activa el disco para todas las operaciones RAID. Cuando un disco se encuentra en modo no RAID, dicho disco está expuesto al sistema operativo no como discos no configurados y en buen estado y se utiliza en un modo de paso directo.

PERC 10 no es compatible para convertir las unidades a no RAID.

Puede convertir las unidades de discos físicos a modo RAID o no RAID de la siguiente manera:

- Mediante las interfaces de iDRAC, como la interfaz web de iDRAC, RACADM, Redfish o WSMan.
- Si presiona <Ctrl+R> mientras se reinicia el servidor y si selecciona la controladora requerida.

NOTA: Si las unidades físicas están conectadas a una controladora PERC en modo no RAID, es posible que el tamaño del disco que se muestra en las interfaces de iDRAC, como la interfaz gráfica de usuario de iDRAC, RACADM, Redfish y WSMan, sea algo menor que el tamaño real del disco. Sin embargo, puede utilizar la capacidad total del disco para implementar sistemas operativos.

NOTA: Los discos con acoplamiento activo en H330 se encuentran siempre en modo no RAID. En otras controladoras RAID, están siempre en modo RAID.

Conversión de discos físicos a modo RAID o no RAID mediante la interfaz web de iDRAC

Para convertir los discos físicos al modo RAID o no RAID, realice los siguientes pasos:

1 En la interfaz web de iDRAC, haga clic en **Almacenamiento** > **Descripción general** > **Discos físicos**.

2 Haga clic en **Filtro avanzado**.

Se muestra una lista elaborada que le permite configurar parámetros diferentes.

3 Desde el menú desplegable **Agrupar por**, seleccione un gabinete o discos virtuales.

Se muestran los parámetros asociados con el gabinete o el VD.

4 Una vez seleccionados todos los parámetros deseados, haga clic en **Aplicar**. Para obtener más información acerca de los campos, consulte la *Ayuda en línea de iDRAC*.

Los valores se aplican según la opción seleccionada en el modo de funcionamiento.

Conversión de discos físicos a modo RAID o no RAID mediante RACADM

Según si desea convertir a modo RAID o no RAID, utilice los siguientes comandos RACADM

- Para convertir a modo RAID, utilice el comando `racadm storage converttoraid`.
- Para convertir a modo no RAID, utilice el comando `racadm storage converttononraid`.

NOTA: En el controlador S140, sólo se admite la interfaz RACADM al convertir las unidades de no RAID a RAID. El software RAID admitido puede ser en modo Windows o Linux.

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

Borrado instantáneo del disco físico seguro

El borrado instantáneo del disco físico seguro garantiza la capacidad para borrar con seguridad el contenido de unidades físicas de autocifrado. Esta función también se admite en unidades ISE. El SSD PCIe NVMe también admite la operación de borrado criptográfico junto con unidades SED e ISE.

Los datos seguirán residiendo en las unidades físicas de autocifrado y las unidades ISE, aún después de que todos los discos virtuales se hayan eliminado. Esto supone un riesgo de seguridad con datos que aún se encuentran en el disco físico. Esta función permite al usuario borrar con seguridad o eliminar todos los datos en las unidades de autocifrado y unidades ISE. Por medio de esta función, el usuario puede borrar todas las unidades SED e ISE que están conectadas a una controladora PERC.

NOTA:

En este momento, puede utilizar la opción de Borrado del sistema para borrar en forma segura todas las unidades ISE.

Esta función no está disponible en las siguientes condiciones:

- Cuando un disco físico ya está en uso por un VD.
- Cuando el disco físico seleccionado no es la unidad SED ni la ISE
- Cuando el disco físico se utiliza como repuesto dinámico.

Esta función está disponible para:

- Las unidades SED e ISE no configuradas
- Unidad cifrada configurada ajena

- Unidad ajena y no configurada incluso cuando la clave de cifrado no está presente en la controladora

NOTA: Borrado criptográfico: utilice esta opción en todos los discos físicos SED e ISE para borrar en forma segura los discos físicos SED e ISE. Esta configuración es compatible con configuraciones organizadas y en tiempo real.

Recrear un disco físico

La recreación de un disco físico es la capacidad de reconstruir el contenido de un disco con error. Esto es cierto sólo cuando la opción de recreación automática se establece en false (falso). Si hay un disco virtual redundante, la operación de recreación puede reconstruir el contenido de un disco físico con error. Una recreación se puede realizar durante la operación normal, pero degrada el rendimiento.

La operación de Cancelar la recreación se puede utilizar para cancelar una recreación que está en progreso. Si cancela una recreación, el disco virtual permanece en un estado degradado. La falla de un disco físico adicional puede hacer que el disco virtual falle y puede ocasionar la pérdida de datos. Se recomienda llevar a cabo lo antes posible una recreación en el disco físico con error.

En caso de cancelar la recreación de un disco físico asignado como un repuesto dinámico, reinicie la recreación en el mismo disco físico para poder restaurar los datos. La cancelación de la recreación de un disco físico y la asignación de otro disco físico como repuesto dinámico no hace que el repuesto dinámico recientemente asignado recree los datos.

Administración de discos virtuales

Es posible realizar las siguientes operaciones para los discos virtuales:

- Crear
- Eliminar
- Editar políticas
- Inicializar
- Revisión de congruencia
- Cancelar revisión de congruencia
- Cifrar discos virtuales
- Asignar o desasignar repuestos dinámicos dedicados
- Hacer parpadear y dejar de hacer parpadear el disco virtual
- Cancelar la inicialización de segundo plano
- Expansión de la capacidad en línea
- Migración de nivel RAID

NOTA: Puede administrar y supervisar 192 discos virtuales si la configuración automática está activada a través de la controladora PERC en el BIOS, la infraestructura de interfaz humana (HII) y Dell OpenManage Server Administrator (OMSA).

NOTA: El conteo de PERC 10 es menor ya que no es compatible con arreglos de conexión encadenada.

Creación de discos virtuales

Para implementar las funciones de RAID, se debe crear un disco virtual. Un disco virtual hace referencia al almacenamiento creado por una controladora RAID desde uno o más discos físicos. Aunque se puede crear un disco virtual a partir de varios discos físicos, el sistema operativo lo percibirá como un solo disco.

Antes de crear un disco virtual, debe familiarizarse con la información de la sección Consideraciones antes de crear discos virtuales.

Es posible crear un disco virtual mediante el uso de los discos físicos conectados a la controladora PERC. Para crear un disco virtual, es necesario tener privilegio de usuario de control del servidor. Puede crear un máximo de 64 unidades virtuales y un máximo de 16 unidades virtuales en el mismo grupo de la unidad.

No se puede crear un disco virtual si:

- Las unidades de disco físico no están disponibles para la creación del disco virtual. Instale unidades de disco físico adicionales.
- Se ha alcanzado el número máximo de discos virtuales que se pueden crear en la controladora. Debe eliminar al menos un disco virtual y, a continuación, crear un nuevo disco virtual.
- Se ha alcanzado el número máximo de discos virtuales admitidos por un grupo de unidades. Debe eliminar un disco virtual del grupo seleccionado y, a continuación, crear un nuevo disco virtual.
- Hay un trabajo en ejecución o programado actualmente en la controladora seleccionada. Debe esperar que finalice este trabajo o puede eliminarlo antes de intentar una nueva operación. Puede ver y administrar el estado del trabajo programado en la página Job Queue (Cola de trabajos).
- El disco físico están en modo no RAID. Debe convertirlo a modo RAID mediante las interfaces de iDRAC, como la interfaz web de iDRAC, RACADM, Redfish, WSMan o <CTRL+R>.

NOTA: Si se crea un disco virtual en el modo Agregar a operaciones pendientes, pero no se crea un trabajo, cuando se elimina el disco virtual, se borra la operación pendiente Crear para el disco virtual.

NOTA: No se admiten los niveles RAID 6 y RAID 60 en H330.

Consideraciones antes de crear discos virtuales

Antes de crear discos virtuales, tenga en cuenta lo siguiente:

- Nombres de los discos virtuales no almacenados en la controladora: los nombres de los discos virtuales que crea no se almacenan en la controladora. Esto significa que si reinicia mediante un sistema operativo distinto, es posible que el nuevo sistema operativo cambie el nombre del disco virtual aplicando sus propias convenciones de nombres.
- La agrupación de discos es una agrupación lógica de discos conectados a una controladora RAID donde se crean uno o varios discos virtuales de manera tal que todos los discos virtuales en el grupo de discos usen todos los discos físicos en el grupo. La implementación actual admite la formación de bloques con grupos de discos mixtos durante la creación de dispositivos lógicos.
- Los discos físicos se unen a grupos de discos. Por lo tanto, los niveles de RAID no se mezclan en un grupo de discos.
- Existen limitaciones respecto del número de discos físicos que se pueden incluir en el disco virtual. Estas limitaciones dependen de la controladora. Cuando se crea un disco virtual, las controladoras admiten un cierto número de secciones y tramos (métodos para combinar el almacenamiento en los discos físicos). Debido a que el número total de secciones y tramos es limitado, el número de discos físicos que se pueden utilizar también es limitado. Las limitaciones de secciones y tramos afectan los niveles de RAID como se indica a continuación:
  - Número máximo de tramos afecta a los niveles RAID 10, RAID 50 y RAID 60.
  - Número máximo de secciones afecta a los niveles RAID 0, RAID 5, RAID 50, RAID 6 y RAID 60.
  - La cantidad de discos físicos en un reflejo es siempre 2. Esto afecta a RAID 1 y RAID 10.
- No se pueden crear discos virtuales en SSD PCIe.

Creación de discos virtuales mediante la interfaz web

Para crear un disco virtual:

1 En la interfaz web de iDRAC, vaya a **Almacenamiento** > **Descripción general** > **Discos virtualesFiltro avanzado**.

2 En la sección **Disco virtual**, realice lo siguiente:

a En el menú desplegable **Controladora**, seleccione la controladora para la que desea crear el disco virtual.

b En el menú desplegable **Diseño**, seleccione el nivel RAID para el disco virtual.

Solo los niveles RAID compatibles con la controladora se muestran en el menú desplegable y esto se basa en los niveles RAID disponibles según el número total de discos físicos disponibles.

c Seleccione **Tipo de medios**, **Tamaño de la sección**, **Política de lectura**, **Política de escritura**, **Política de caché de disco**.

Solo los valores compatibles con la controladora se muestran en los menús desplegables para estas propiedades.

d En el campo **Capacidad**, especifique el tamaño del disco virtual.

Se muestra el tamaño máximo y este se actualiza a medida que se seleccionan los discos.

e El campo **Recuento de tramos** se muestra en función de los discos físicos seleccionados (paso 3). No se puede establecer este valor. Se calcula automáticamente después de seleccionar discos para un nivel de múltiples RAID. Si ha seleccionado RAID 10 y la

controladora admite RAID 10 dispar, no se muestra el valor de recuento de tramos. La controladora establece automáticamente el valor apropiado.

3 En la sección **Seleccionar discos físicos**, seleccione la cantidad de discos físicos.

Para obtener más información acerca de los campos, consulte *iDRAC Online Help* (Ayuda en línea de iDRAC).

4 En el menú desplegable **Aplicar modo de operación**, seleccione el momento en que desea aplicar la configuración.

5 Haga clic en **Crear disco virtual**.

Según en la opción de **Aplicar modo de operación** seleccionada, se aplicará la configuración.

NOTA: Puede utilizar caracteres alfanuméricos, espacios, guiones y guiones bajos en el nombre del disco. Cualquier otro caracter especial que se introduzca se elimina durante la creación del disco virtual.

Creación de discos virtuales mediante RACADM

Utilice el comando. `racadm storage createvd`

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

Edición de políticas de caché de discos virtuales

Es posible cambiar la política de lectura, de escritura o de caché de disco de un disco virtual.

NOTA: Algunas controladoras no admiten todas las políticas de lectura o escritura. Por lo tanto, cuando se aplique una política, se mostrará un mensaje de error.

Las políticas de lectura indican si la controladora debe leer los sectores secuenciales del disco virtual al buscar datos:

- **Adaptative Read Ahead (Lectura anticipada adaptativa)**: La controladora inicia la lectura anticipada solamente si las dos solicitudes de lectura más recientes han obtenido acceso a sectores secuenciales del disco. Si las solicitudes de lectura posteriores acceden a sectores aleatorios del disco, la controladora vuelve a la política Sin lectura anticipada. La controladora continuará evaluando si las solicitudes de lectura están obteniendo acceso a sectores secuenciales del disco y, si es necesario, podrá iniciar una lectura anticipada.
- **Lectura anticipada**: La controladora lee los sectores secuenciales del disco virtual cuando busca datos. La política Lectura anticipada puede mejorar el rendimiento del sistema si los datos se escriben en los sectores secuenciales del disco virtual.
- **Sin lectura anticipada**: si selecciona la política sin lectura anticipada indica que la controladora no debe usar la política de lectura anticipada.

Las políticas de escritura especifican si la controladora enviará una señal de término de la solicitud de escritura en cuanto los datos estén en la caché o después de que se hayan escrito en el disco.

- **Escritura simultánea**: la controladora envía una señal de finalización de la solicitud de escritura solamente después de que los datos se escriben en el disco. La escritura simultánea de la memoria caché proporciona una mayor seguridad de datos que la escritura no simultánea de la memoria caché, ya que el sistema da por sentado que los datos solo estarán disponibles después de que se hayan escrito en forma segura en el disco.
- **Escritura no simultánea**: la controladora envía una señal de terminación de solicitud de escritura en cuanto los datos están en la memoria caché de la controladora, pero todavía no se han escrito en el disco. La escritura no simultánea de la memoria caché puede mejorar el rendimiento, ya que las solicitudes de lectura posteriores pueden recuperar datos de la memoria caché más rápidamente que del disco. Sin embargo, la pérdida de datos se puede producir en caso de una falla del sistema que impida que los datos se escriban en un disco. Otras aplicaciones también podrían experimentar problemas cuando las acciones asumen que los datos están disponibles en el disco.
- **Force Write Back (Forzar escritura no simultánea)**: la caché de escritura está habilitada independientemente de si la controladora tiene una batería. Si la controladora no tiene una batería y se usa la escritura no simultánea de la memoria caché, podrían perderse datos ante un fallo de alimentación.

La política de caché de disco se aplica a las lecturas en un disco virtual específico. Estos valores no afectan a la política de lectura anticipada.

NOTA:

- Las opciones de caché no volátil de la controladora y de respaldo de batería para la caché de la controladora afectan la política de lectura o la política de escritura que una controladora puede admitir. No todas las controladoras PERC contienen batería y caché.
- La lectura anticipada y la escritura no simultánea requieren una caché. Por lo tanto, si la controladora no dispone de una caché, no se permite la configuración de valores de políticas.

  De manera similar, si PERC dispone de una caché, pero no de una batería, y se ha establecido una política por la que se requiere acceso a la memoria caché, se puede producir una pérdida de datos en caso de apagado. Por eso, muy pocas PERC no permiten esa política.

  Por lo tanto, se establece el valor de política en función de la controladora PERC.

Eliminación de discos virtuales

La eliminación de un disco virtual destruye toda la información, incluidos los sistemas de archivos y los volúmenes que residen en el disco virtual, y quita el disco virtual de la configuración de la controladora. Al eliminar discos virtuales, todos los repuestos dinámicos globales asignados se pueden desasignar automáticamente en el momento en que se elimina el último disco virtual asociado con la controladora. Cuando se elimina el último disco virtual de un grupo de discos, todos los repuestos dinámicos dedicados asignados automáticamente se vuelven repuestos dinámicos globales.

Si elimina todos los discos virtuales para un repuesto dinámico global, el repuesto dinámico global se elimina automáticamente.

Es necesario tener el privilegio de inicio de sesión y control del servidor para eliminar discos virtuales.

Cuando se permite esta operación, puede eliminar una unidad virtual de inicio. Esto se realiza desde la banda lateral y de manera independiente al sistema operativo. Por lo tanto, aparece un mensaje de advertencia antes de eliminar la unidad virtual.

Si se elimina un disco virtual e inmediatamente se crea un nuevo disco virtual con las mismas características que el disco eliminado, la controladora reconoce los datos como si el primer disco virtual nunca se hubiera eliminado. En esta situación, si no desea conservar los datos antiguos después de recrear un nuevo disco virtual, vuelva a inicializar el disco virtual.

Revisión de congruencia en el disco virtual

Esta operación verifica la precisión de la información redundante (paridad). Esta tarea solo se aplica a los discos virtuales redundantes. De ser necesario, la tarea de verificación de congruencia regenera los datos redundantes. Si la unidad virtual tiene un estado degradado, la ejecución de una revisión de congruencia puede devolver la unidad virtual al estado Listo. Puede realizar una verificación de congruencia por medio de la interfaz web o RACADM.

También es posible cancelar la operación de verificación de congruencia. La opción Cancelar revisión de congruencia es una operación en tiempo real.

Es necesario tener el privilegio de inicio de sesión y control del servidor para realizar una revisión de congruencia en los discos virtuales.

NOTA: La revisión de congruencia no se admite cuando las unidades están establecidas en modo RAID0.

Inicialización de discos virtuales

La inicialización de discos virtuales borra todos los datos en el disco, pero no cambia la configuración del disco virtual. Es necesario inicializar un disco virtual ya configurado antes de usarlo.

NOTA: No inicialice discos virtuales si intenta recrear una configuración existente.

Es posible realizar una inicialización rápida o una inicialización completa o bien, cancelar la operación de inicialización.

NOTA: La opción Cancelar inicialización es una operación en tiempo real. Se puede cancelar la inicialización utilizando solamente la interfaz web de iDRAC y no por medio de RACADM.

Inicialización rápida

La operación de Inicialización rápida inicializa todos los discos físicos incluidos en el disco virtual. Actualiza los metadatos en los discos físicos, de modo que todo el espacio en disco quede disponible para futuras operaciones de escrituras. La tarea de inicialización se puede completar rápidamente, ya que la información existente en los discos físicos no se borra, a pesar de que las operaciones de escritura futuras sobrescribirán toda la información que permanezca en los discos físicos.

La inicialización rápida solo elimina la información en las secciones y en el sector de inicio. Realice una inicialización rápida solo si tiene limitaciones de tiempo o las unidades de disco duro son nuevas o no fueron utilizadas. La inicialización rápida se completa en menos tiempo (generalmente entre 30 y 60 segundos).

PRECAUCIÓN: Después de ejecutar una inicialización rápida, no se puede obtener acceso a los datos existentes.

La tarea de Inicialización rápida no escribe ceros en los bloques de discos de los discos físicos. Esto se debe a que la tarea de Inicialización rápida no realiza una operación de escritura y produce menos degradación en el disco.

Si se realiza una inicialización rápida en un disco virtual, se sobrescriben los primeros y últimos 8 MB del disco virtual, con lo que se eliminan los registros de inicio y la información sobre particiones. Esta operación tarda solo 2 o 3 segundos en completarse y se recomienda realizarla al recrear discos virtuales.

La inicialización de segundo plano se inicia cinco minutos después de que se haya finalizado la inicialización rápida.

Inicialización completa o lenta

La operación de Inicialización completa (también llamada inicialización lenta) inicializa todos los discos físicos incluidos en el disco virtual. Esta tarea actualiza los metadatos en los discos físicos y borra todos los datos y sistemas de archivos existentes. Es posible realizar una inicialización completa después de crear el disco virtual. En comparación con la operación de inicialización rápida, se recomienda utilizar la inicialización completa si existe algún problema con un disco físico o se sospecha que contiene bloques de disco dañados. La operación de inicialización completa reasigna los bloques dañados y escribe ceros en todos los bloques de disco.

Si se lleva a cabo la inicialización completa de un disco virtual, no se necesita una inicialización de segundo plano. Durante una inicialización completa, el host no puede acceder al disco virtual. Si el sistema se reinicia durante una inicialización completa, la operación se anula y se comienza un proceso de inicialización de segundo plano en el disco virtual.

Siempre se recomienda ejecutar una inicialización completa en las unidades en donde se hayan almacenado datos anteriormente. La inicialización completa puede tardar entre 1 y 2 minutos por GB. La velocidad de inicialización varía según el modelo de la controladora, la velocidad de las unidades de disco duro y la versión de firmware.

La tarea de inicialización completa inicializa un disco físico a la vez.

NOTA: La inicialización completa solo se admite en tiempo real. Pocas controladoras admiten la inicialización completa.

Cifrado de discos virtuales

Cuando se desactiva el cifrado en una controladora (es decir, se elimina la clave de seguridad), es necesario activar manualmente el cifrado para los discos virtuales creados con unidades SED. Si el disco virtual se crea después de haber activado el cifrado en una controladora, el disco virtual se cifra automáticamente. Se configurará automáticamente como un disco virtual cifrado, a menos que se desactive la opción de cifrado activada durante la creación del disco virtual.

Es necesario tener el privilegio de inicio de sesión y control del servidor para administrar las claves de cifrado.

NOTA: Aunque se habilita el cifrado en las controladoras, el usuario necesita activar manualmente el cifrado en el VD si el VD se crea a partir de iDRAC. Solo si el disco virtual se crea a partir de OMSA, se cifraría de manera automática.

Asignación o desasignación de repuestos dinámicos dedicados

El repuesto dinámico global es un disco de reserva no utilizado que forma parte del grupo de discos. Cuando falla un disco físico en el disco virtual, el repuesto dinámico asignado se activará con el fin de reemplazar el disco físico fallido sin interrumpir el sistema ni requerir su intervención.

Es necesario tener el privilegio de inicio de sesión y control del servidor para ejecutar esta operación.

Es posible asignar solamente unidades de 4000 como repuesto dinámico a discos virtuales de 4000.

Si ha asignado un disco físico como repuesto dinámico dedicado en el modo Agregar a operaciones pendientes, se crea la operación pendiente pero no se crea un trabajo. Por lo tanto, si intenta desasignar el repuesto dinámico dedicado, la operación pendiente Asignar repuesto dinámico dedicado se borra.

Si ha desasignado un disco físico como repuesto dinámico dedicado en el modo Agregar a operaciones pendientes, se crea la operación pendiente pero no se crea un trabajo. Por lo tanto, si intenta asignar el repuesto dinámico dedicado, la operación pendiente Desasignar un repuesto dinámico dedicado se borra.

NOTA: Mientras la operación de exportación del registro esté en curso, no podrá ver información sobre repuestos dinámicos dedicados en la página Administrar discos virtuales. Después de que la operación de exportación del registro se haya completado, vuelva a cargar o actualice la página Administrar discos virtuales para ver la información.

Cambiar nombre de VD

Para cambiar el nombre de un disco virtual, el usuario debe contar con el privilegio de Control del sistema. El nombre del disco virtual puede contener solo caracteres alfanuméricos, espacios, guiones y guiones bajos. La longitud máxima del nombre depende de la controladora individual. En la mayoría de los casos, la longitud máxima es de 15 caracteres. El nombre no puede comenzar o finalizar con un espacio ni se puede dejar en blanco. Cada vez que se cambia el nombre de un disco virtual, se crea un registro de LC.

Editar capacidad de disco (Expansión de capacidad en línea (OCE))

La Expansión de capacidad en línea (OCE) le permite aumentar la capacidad de almacenamiento de los niveles de RAID seleccionados mientras el sistema permanece en línea. La controladora redistribuye los datos en el arreglo (denominado Reconfiguración), colocando nuevo espacio disponible al final de cada arreglo RAID.

La Expansión de capacidad en línea (OCE) se puede lograr de dos maneras:

- Si el espacio libre está disponible en la unidad física más pequeña en el grupo de discos virtuales después de iniciar LBA de discos virtuales, la capacidad del disco virtual se podrá expandir dentro de dicho espacio libre. Esta opción le permite introducir el nuevo

tamaño aumentado del disco virtual. Si grupo de discos en un disco virtual tiene espacio disponible solamente antes de iniciar el LBA, la edición de la capacidad de disco en el mismo grupo de discos no se permite a pesar de haber espacio disponible en una unidad física.

- La capacidad de un disco virtual también se puede ampliar al agregar discos físicos compatibles adicionales al grupo de discos virtuales existentes. Esta opción no le permite introducir el nuevo tamaño aumentado del disco virtual. El nuevo tamaño aumentado del disco virtual se calcula y se muestra al usuario, de acuerdo con el espacio de disco utilizado del grupo de discos físicos existente en un disco virtual específico, el nivel de raid existente del disco virtual y la cantidad de nuevas unidades agregadas al disco virtual.

La expansión de la capacidad permite que el usuario especifique el tamaño de VD final. Internamente, el tamaño final del VD se transmite a PERC en porcentaje (este porcentaje es el espacio que el usuario desea utilizar del espacio vacío restante del arreglo para la expansión del disco local). Debido a esta lógica de porcentaje, el tamaño de VD final, una vez finalizada la reconfiguración, puede ser diferente de lo que el usuario proporcionó para el escenario en el que el usuario no brinda el tamaño máximo posible de VD (el porcentaje termina siendo inferior al 100%). El usuario no ve la diferencia en este tamaño de VD y el tamaño de VD final ingresados después de la reconfiguración, si el usuario ingresa el tamaño máximo de VD posible.

Migración de nivel RAID (RLM)

La Migración de nivel RAID (RLM) hace referencia al cambio de nivel RAID de un disco virtual. La iDRAC9 proporciona una opción para aumentar el tamaño del disco virtual (VD) mediante RLM. De una forma, RLM permite migrar el nivel RAID de un disco virtual, que a su vez puede aumentar el tamaño del disco virtual.

La migración del nivel RAID es el proceso de conversión de un disco virtual con un nivel RAID a otro. Cuando migre un VD a un nivel RAID diferente, los datos de usuario en este disco se redistribuyen en el formato de la nueva configuración.

Esta configuración se puede organizar en etapas y en tiempo real.

En la siguiente tabla, se describen los posibles diseños de VD reconfigurables durante la reconfiguración (RLM) de un disco virtual con adición de discos y sin adición de discos.

Diseño de VD de origen	Posible diseño de VD de destino con adición de discos	Posible diseño de VD de destino sin adición de discos
R0 (un solo disco)	R1	NA
R0	R5/R6	NA
R1	R0/R5/R6	R0
R5	R0/R6	R0
R6	R0/R5	R0/R5

Operaciones permitidas cuando se está ejecutando OCE/RLM

Las siguientes operaciones están permitidas cuando se está ejecutando OCE/RLM:

Desde la parte frontal de la controladora, detrás de la cual se está ejecutando un VD mediante OCE/RLM	Desde la parte frontal del VD (la cual se está ejecutando mediante OCE/RLM)	Desde cualquier otro Disco físico en estado listo en la misma controladora	Desde cualquier otra parte frontal de VD (que no se está ejecutando mediante OCE/RLM) en la misma controladora
Restablecer configuración	Eliminar	Blink (Hacer parpadear)	Eliminar
Export Log (Exportar registro)	Blink (Hacer parpadear)	Unblink (Dejar de parpadear)	Blink (Hacer parpadear)
Establecer modo de lectura de patrullaje	Unblink (Dejar de parpadear)	Asignar un repuesto dinámico global	Unblink (Dejar de parpadear)

Comenzar lectura de patrullaje	Convertir a discos no RAID	Cambiar nombre
Cambiar propiedades de la controladora		Cambiar política
Administrar alimentación de discos físicos		Inicialización lenta
Convertir a discos compatibles con RAID		Inicialización rápida
Convertir a discos no RAID		Reemplazo del disco miembro
Cambiar el modo de la controladora		

Restricciones o limitaciones de OCE y RLM

A continuación, se indican las limitaciones comunes para OCE y RLM:

- La OCE/RLM queda limitada a la situación en la que el grupo de discos contiene un único VD.
- OCE no se admite en RAID50 y RAID50. RLM no es compatible con RAID10, RAID50 y RAID60.
- Si la controladora ya contiene el número máximo de discos virtuales, no puede realizar una migración de nivel RAID o expansión de capacidad en ningún disco virtual.
- La controladora cambia la política de caché de escritura de todos los discos virtuales en los que se está realizando una RLM/OCE a Escritura simultánea hasta que finaliza la RLM/OCE.
- Generalmente, la reconfiguración de los Virtual Disks (Discos virtuales) afecta al rendimiento del disco hasta que la operación de reconfiguración concluya.
- El número total de discos físicos de un grupo de discos no puede ser superior a 32.
- Si ya se está ejecutando alguna operación en segundo plano (como BGI/recreación/escritura diferida/lectura de patrullaje) en el correspondiente VD/PD, en ese caso, la Reconfiguración (OCE/RLM) no se permite en ese momento.
- Cualquier tipo de migración de discos cuando la Reconfiguración (OCE/RLM) se encuentra en curso en las unidades asociadas con VD hace que la reconfiguración falle.
- Toda unidad nueva adicionada para OCE/RLM se vuelve parte del VD una vez finalizada la reconstrucción. Pero el Estado para esas nuevas unidades cambia a En línea justo después de que se inicia la reconstrucción.

Cancelar inicialización

Esta función es la capacidad de cancelar la inicialización de segundo plano en un disco virtual. En las controladoras PERC, la inicialización de segundo plano del disco virtual redundante se inicia automáticamente después de crear un disco virtual. La inicialización de segundo plano de un disco virtual redundante prepara el disco virtual para recibir información de paridad y mejora el rendimiento de escritura. Sin embargo, algunos procesos, como la creación de un disco virtual, no se pueden ejecutar mientras la inicialización de segundo plano está en curso. Cancelar la inicialización proporciona la posibilidad de cancelar la inicialización de segundo plano manualmente. Una vez cancelada, la inicialización de segundo plano se reinicia automáticamente entre 0 y 5 minutos después.

NOTA: La inicialización en segundo plano no es aplicable para discos virtuales RAID 0.

Administración de discos virtuales mediante la interfaz web

1 En la interfaz web de iDRAC, vaya a **Almacenamiento** > **Descripción general** > **Discos virtuales** > **Filtro avanzado**.
2 En los **Discos virtuales**, seleccione la controladora para la que desea administrar los discos virtuales.
3 Para uno o varios discos virtuales, en cada menú desplegable **Acción**, seleccione una acción.

Puede especificar más de una acción para una unidad virtual. Cuando se selecciona una acción, aparece un menú desplegable **Acción** adicional. Seleccione otra acción desde este menú desplegable. La acción que ya se ha seleccionado no aparece en los menús desplegables **Acción** adicionales. Además, aparece el vínculo **Quitar** al lado de la acción seleccionada. Haga clic en este enlace para eliminar la acción seleccionada.

- **Eliminar**
- **Editar política: caché de lectura**: cambie la política de caché de lectura a una de las siguientes opciones:
  - **Sin lectura anticipada**: indica que para un volumen determinado, no se utiliza ninguna política de lectura anticipada.
  - **Lectura anticipada**: Indica que para un volumen determinado, la controladora realiza una lectura secuencial anticipada de los datos solicitados y almacena los datos adicionales en la memoria caché para anticiparse a una solicitud de datos. Esto permite acelerar las lecturas de datos secuenciales, aunque no se observa la misma mejora cuando se accede a datos aleatorios.
  - **Lectura anticipada adaptativa**: indica que para un volumen determinado, la controladora utiliza la política de caché de lectura anticipada si los dos accesos más recientes al disco se registraron en los sectores secuenciales. Si las solicitudes de lectura son aleatorias, la controladora regresa al modo Sin lectura anticipada.
- **Editar política: caché de escritura**: cambie la política de caché de escritura a una de las siguientes opciones:
  - **Escritura simultánea**: indica que para un volumen determinado, la controladora envía una señal de finalización de transferencia de datos al sistema host una vez que el subsistema del disco recibe todos los datos de una transacción.
  - **Escritura no simultánea**: Indica que para un volumen determinado, la controladora envía una señal de finalización de transferencia de datos al sistema host una vez que la caché del sistema recibe todos los datos de una transacción. A continuación, la controladora graba los datos almacenados en la caché en el dispositivo de almacenamiento en segundo plano.
  - **Forzar escritura no simultánea**: al usar la escritura no simultánea de la memoria caché, la caché de escritura se activa sin importar si la controladora tiene una batería. Si la controladora no tiene una batería y se usa la escritura no simultánea de la memoria caché, podrían perderse datos ante un fallo de alimentación.
- **Editar política: caché de disco**: cambie la política de caché de disco a una de las siguientes opciones:
  - **Predeterminada**: indica que el disco está utilizando el modo de caché de escritura predeterminada. En el caso de los discos SATA, esta opción está activada. Para los discos SAS, esta opción está desactivada.
  - **Activada**: indica que la caché de escritura del disco está activada. Esto aumenta el rendimiento y la probabilidad de pérdida de datos ante un fallo de alimentación.
  - **Desactivada**: indica que la caché de escritura del disco está desactivada. Esto disminuye el rendimiento y la probabilidad de pérdida de datos.
- **Inicialización: rápida**: actualiza los metadatos en los discos físicos, de modo que todo el espacio en disco quede disponible para operaciones de escritura futuras. La opción de inicialización se puede completar rápidamente, ya que la información existente en los discos físicos no se borra, a pesar de que las operaciones de escritura futuras sobrescribirán toda la información que permanezca en los discos físicos.
- **Inicialización: total**: se borran todos los datos y los sistemas de archivos existentes.

  NOTA: La opción Inicialización: total no se aplica a las controladoras PERC H330.
- **Revisión de congruencia**: para verificar la congruencia de un disco virtual, seleccione **Revisión de congruencia** en el menú desplegable.

  NOTA: La revisión de congruencia no se admite en las unidades establecidas en modo RAID0.
- **Cifrar disco virtual**: cifra la unidad de disco virtual. Si la controladora no admite el cifrado, es posible crear, cambiar o eliminar las claves de seguridad.

  NOTA: La opción Cifrar disco virtual solo está disponible si el disco virtual se crea mediante unidades de autocifrado (SED).
- **Administrar repuestos dinámicos dedicados**: asigne o desasigne un disco físico como un repuesto dinámico dedicado. Solo se muestran los repuestos dinámicos dedicados válidos. Si no hay repuestos dinámicos dedicados válidos, esta sección no aparece en el menú desplegable.

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

4 En el menú desplegable **Aplicar modo de operación**, seleccione el momento en que desea aplicar la configuración.

5 Haga clic en **Aplicar**.

Según el modo de operación seleccionado, se aplicará la configuración.

Las otras opciones son:

Migración de nivel de RAID: muestra el Nombre del disco, el Nivel de RAID actual y el tamaño del disco virtual. Le permite seleccionar un nuevo nivel de RAID. El usuario puede tener que añadir unidades adicionales a los discos virtuales existentes para migrar a un nuevo nivel de raid. Esta función no es aplicable en RAID 10, 50 y 60.

Administración de discos virtuales mediante RACADM

Utilice los siguientes comandos para administrar discos virtuales:

- Para eliminar un disco virtual:
  ```
  racadm storage deletevd:<VD FQDD>
  ```
- Para inicializar un disco virtual:
  ```
  racadm storage init:<VD FQDD> -speed {fast|full}
  ```
- Para verificar la coherencia en los discos virtuales (no compatible con RAID0):
  ```
  racadm storage ccheck:<vdisk fqdd>
  ```
  Para cancelar la comprobación de coherencia:
  ```
  racadm storage cancelcheck: <vdisks fqdd>
  ```
- Para descifrar discos virtuales:
  ```
  racadm storage encryptvd:<VD FQDD>
  ```
- Para asignar o desasignar repuestos dinámicos dedicados:
  ```
  racadm storage hotspare:<Physical Disk FQDD> -assign <option> -type dhs -vdkey: <FQDD of VD>
  ```

<option>=sí	Asignar repuesto dinámico
<Option>=no	Desasignar repuesto dinámico

Administración de controladoras

Es posible realizar las siguientes tareas para las controladoras:

- Configurar propiedades de la controladora
- Importar o importar automáticamente configuración ajena
- Borrar configuración ajena
- Restablecer configuración de la controladora
- Crear, modificar o eliminar claves de seguridad
- Descarte la caché preservada.

Configuración de las propiedades de la controladora

Es posible configurar las siguientes propiedades de la controladora:

- Modo de lectura de patrullaje (automático o manual)
- Iniciar o detener la lectura de patrullaje si el modo de lectura de patrullaje es manual
- Áreas de lectura de patrullaje no configuradas
- Modo de revisión de congruencia
- Modo de escritura diferida
- Modo de equilibrio de carga
- Porcentaje de revisión de congruencia
- Porcentaje de recreación

- Porcentaje de inicialización de segundo plano
- Porcentaje de reconstrucción
- Importación automática de configuración ajena mejorada
- Crear o cambiar claves de seguridad

Es necesario tener el privilegio de inicio de sesión y control del servidor para configurar las propiedades de la controladora.

Consideraciones sobre el modo de lectura de patrullaje

La lectura de patrullaje identifica los errores en el disco para evitar fallas de disco y pérdida o daño de datos.

La lectura de patrullaje no se ejecuta en un disco físico en las siguientes circunstancias:

- El disco físico no está incluido en un disco virtual o no está asignado como un repuesto dinámico.
- El disco físico está incluido en un disco virtual que actualmente está experimentando alguna de las siguientes acciones:
  - Una recreación
  - Una reconfiguración o reconstrucción
  - Una inicialización de segundo plano
  - Una revisión de congruencia

Además, la lectura de patrullaje se suspende durante actividad de E/S intensa y se reanuda una vez completada la actividad de E/S.

NOTA: Para obtener más información acerca de la frecuencia con la que se ejecuta la lectura de patrullaje en modo automático, consulte la documentación de la controladora correspondiente.

NOTA: Los operaciones de modo de lectura de patrullaje como Iniciar y Detener no son compatibles si no hay discos virtuales disponibles en la controladora. Aunque puede invocar las operaciones correctamente con las interfaces de iDRAC, las operaciones fallan cuando se inicia el trabajo asociado.

Equilibrio de carga

La propiedad Equilibrio de carga ofrece la capacidad de utilizar automáticamente los dos puertos o conectores de la controladora conectados al mismo gabinete para dirigir solicitudes de E/S. Esta propiedad solo se encuentra disponible en las controladoras SAS.

Porcentaje de inicialización de segundo plano

En las controladoras PERC, la inicialización de segundo plano de un disco virtual redundante comienza automáticamente de 0 a 5 minutos después de la creación del disco virtual. La inicialización de segundo plano de un disco virtual redundante prepara el disco virtual para mantener datos redundantes y mejora el rendimiento de escritura. Por ejemplo, una vez completada la inicialización de segundo plano de un disco virtual RAID 5, se inicializa la información de paridad. Una vez completada la inicialización de segundo plano de un disco virtual RAID 1, se reflejan los discos físicos.

El proceso de inicialización de segundo plano ayuda a la controladora a identificar y corregir problemas que se podrían producir en otro momento con los datos redundantes. Con respecto a esto, el proceso de inicialización de segundo plano es similar al de la revisión de congruencia. Se debe permitir que la inicialización de segundo plano se ejecute hasta su finalización. Si se cancela, la inicialización de segundo plano se reinicia automáticamente entre 0 y 5 minutos después. Algunos procesos, como las operaciones de lectura y escritura, son posibles mientras se ejecuta la inicialización de segundo plano. Otros procesos, como la creación de un disco virtual, no pueden ejecutarse de forma simultánea con la inicialización de segundo plano. Estos procesos provocan la cancelación de la inicialización de segundo plano.

El porcentaje de inicialización de segundo plano, que se puede configurar entre 0 % y 100 %, representa el porcentaje de recursos del sistema dedicado a ejecutar la tarea de inicialización de segundo plano. En 0 %, la inicialización de segundo plano queda última en la lista de prioridades de la controladora, demora el mayor tiempo posible en completarse y es la configuración con el menor impacto sobre el

rendimiento del sistema. Un porcentaje de inicialización de segundo plano de 0 % no significa que el proceso quede detenido o en pausa. Con un valor de 100%, la inicialización en segundo plano es la principal prioridad de la controladora. El tiempo de inicialización de segundo plano se reduce y es la configuración con el mayor impacto en el rendimiento del sistema.

Revisión de congruencia

La tarea de Revisión de congruencia verifica la precisión de la información redundante (paridad). Esta tarea solo se aplica a los discos virtuales redundantes. De ser necesario, la tarea de Revisión de congruencia regenera los datos redundantes. Si el disco virtual está en estado Redundancia fallida, ejecutar una revisión de congruencia puede regresar el disco virtual a un estado Listo.

El porcentaje de revisión de congruencia, que se puede configurar entre 0 % y 100 %, representa el porcentaje de recursos del sistema dedicado a ejecutar la tarea de revisión de congruencia. En 0 %, la revisión de congruencia queda última en la lista de prioridades de la controladora, demora el mayor tiempo posible en completarse y es la configuración con el menor impacto sobre el rendimiento del sistema. Un porcentaje de revisión de congruencia de 0 % no significa que el proceso quede detenido o en pausa. Con un valor de 100%, la revisión de congruencia es la principal prioridad de la controladora. El tiempo de revisión de congruencia se reduce y es la configuración con el mayor impacto en el rendimiento del sistema.

Crear o cambiar claves de seguridad

Al configurar las propiedades de la controladora, es posible crear o cambiar las claves de seguridad. La controladora usa la clave de cifrado para bloquear o desbloquear el acceso a los discos de cifrado automático (SED). Se puede crear una sola clave de cifrado para cada controladora con funciones de cifrado. La clave de seguridad se administra mediante el uso de la función Administración de claves locales (LKM). LKM se utiliza para generar la identificación de la clave y la clave o contraseña requerida para proteger el disco virtual. Si se usa LKM, se debe proporcionar el identificador de clave de seguridad y la frase de contraseña para crear la clave de cifrado.

Esta tarea no se admite en las controladoras de hardware PERC que se ejecutan en modo HBA.

Si se crea la clave de seguridad en el modo Agregar a operaciones pendientes, pero no se crea un trabajo, cuando se elimina la clave de seguridad, se borra la operación pendiente Crear clave de seguridad.

Configuración de las propiedades de la controladora mediante la interfaz web

1. En la interfaz web de iDRAC, vaya a **Almacenamiento** > **Descripción general** > **Controladoras**.
   Se mostrará la página **Configuración de controladoras**.
2. En la sección **Controladora**, seleccione la controladora que desea configurar.
3. Especifique la información necesaria para las distintas propiedades.
   La columna **Valor actual** muestra los valores existentes para cada propiedad. Puede modificar este valor si selecciona la opción del menú desplegable **Acción** de cada propiedad.
   Para obtener información acerca de los campos, consulte la *Ayuda en línea de iDRAC7*.
4. En **Aplicar modo de operación**, seleccione el momento en que desea aplicar la configuración.
5. Haga clic en **Aplicar**.
   Según el modo de operación seleccionado, se aplicará la configuración.

Configuración de las propiedades de la controladora mediante RACADM

- Para establecer el modo de lectura de patrullaje:

```
racadm set storage.controller.<index>.PatrolReadMode  {Automatic | Manual | Disabled}
```

- Si el modo de lectura de patrullaje se ha configurado en Manual, utilice los comandos siguientes para iniciar y detener el modo de lectura de patrullaje:

```
racadm storage patrolread:<Controller FQDD> -state {start|stop}
```

> **NOTA: Las operaciones en modo de lectura de patrullaje, como por ejemplo, Iniciar y Detener, no son compatibles si no hay discos virtuales disponibles en la controladora. Aunque puede invocar las operaciones correctamente mediante las interfaces de iDRAC, las operaciones fallarán cuando se inicia el trabajo asociado.**

- Para especificar el modo de revisión de congruencia, utilice el objeto **Storage.Controller.CheckConsistencyMode**.
- Para activar o desactivar el modo de escritura diferida, utilice el objeto **Storage.Controller.CopybackMode**.
- Para activar o desactivar el modo de equilibrio de carga, utilice el objeto **Storage.Controller.PossibleloadBalancedMode**.
- Para especificar el porcentaje de recursos del sistema dedicados a realizar la revisión de congruencia en un disco virtual redundante, utilice el objeto **Storage.Controller.CheckConsistencyRate**.
- Para especificar el porcentaje de recursos de la controladora dedicados a recrear un disco fallido, utilice el objeto **Storage.Controller.RebuildRate**.
- Para especificar el porcentaje de recursos de la controladora dedicados a realizar la inicialización de segundo plano (BGI) de un disco virtual tras su creación, utilice el objeto **Storage.Controller.BackgroundInitializationRate**.
- Para especificar el porcentaje de recursos de la controladora dedicados a reconstruir un grupo de discos después de agregar un disco físico o cambiar el nivel RAID de un disco virtual que reside en el grupo de discos, utilice el objeto **Storage.Controller.ReconstructRate**.
- Para activar o desactivar la importación automática mejorada de la configuración ajena para la controladora, utilice el objeto **Storage.Controller.EnhancedAutoImportForeignConfig**.
- Para crear, modificar o eliminar la clave de seguridad para cifrar las unidades virtuales:

```
racadm storage createsecuritykey:<Controller FQDD> -key <Key id> -passwd <passphrase>
racadm storage modifysecuritykey:<Controller FQDD> -key <key id> -oldpasswd <old passphrase> -
newpasswd <new passphrase>
racadm storage deletesecuritykey:<Controller FQDD>
```

Importación o importación automática de la configuración ajena

Una configuración ajena son datos que residen en discos físicos y que han sido movidos de una controladora a otra. Los discos virtuales que residen en discos físicos y que han sido movidos se consideran como una configuración externa.

Es posible importar configuraciones ajenas de manera que los discos virtuales no se pierdan después de cambiar los discos físicos. Una configuración ajena se puede importar únicamente si contiene un disco virtual en estado Listo o Degradado o bien, un repuesto dinámico dedicado a un disco virtual que se puede importar o ya se encuentra presente.

Todos los datos de los discos virtuales deben estar presentes, pero si los discos virtuales usan un nivel RAID redundante, no se requieren los datos redundantes adicionales.

Por ejemplo, si la configuración ajena contiene solo un lado de un reflejo en un disco virtual RAID 1, el disco virtual se encuentra en estado Degradado y se puede importar. Si la configuración ajena contiene solo un disco físico que se configuró originalmente como RAID 5 usando tres discos físicos, el disco virtual RAID 5 se encuentra en estado Fallido y no se puede importar.

Además de discos virtuales, una configuración ajena puede consistir en un disco físico que se ha asignado como repuesto dinámico de una controladora y que a continuación se ha movido a otra controladora. La tarea Importar configuración ajena importa el nuevo disco físico como repuesto dinámico. Si el disco físico se ha establecido como un repuesto dinámico dedicado en la controladora anterior pero el disco virtual al que el repuesto dinámico se ha asignado ya no está presente en la configuración ajena, el disco físico se importa como un repuesto dinámico global.

Si se detecta alguna configuración ajena bloqueada mediante el Administrador de claves locales (LKM), no se podrá ejecutar la operación Importar configuración ajena en iDRAC en esta versión. Es necesario desbloquear las unidades mediante CTRL-R y continuar con la importación de la configuración ajena desde iDRAC.

La tarea Importar Configuración ajena solo aparece cuando la controladora ha detectado una configuración ajena. También puede identificar si un disco físico contiene una configuración ajena (disco virtual o repuesto dinámico) seleccionando el estado del disco físico. Si el estado del disco físico es Ajeno, el disco físico contiene toda o parte de la porción de un disco virtual o tiene una asignación de repuesto dinámico.

NOTA: La tarea de importación de configuración ajena importa todos los discos virtuales que residen en los discos físicos que se han agregado a la controladora. Si hay más de un disco virtual ajeno presente, se importan todas las configuraciones ajenas.

La controladora PERC9 admite la importación automática de configuraciones ajenas sin la interacción de los usuarios. La importación automática puede estar activada o desactivada. Si se encuentra activada, la controladora PERC puede importar automáticamente cualquier configuración ajena detectada sin intervención manual. Si se encuentra desactivada, la controladora PERC no importa automáticamente ninguna configuración ajena.

Es necesario tener el privilegio de inicio de sesión y control del servidor para importar configuraciones ajenas.

Esta tarea no se admite en las controladoras de hardware PERC que se ejecutan en modo HBA.

NOTA: No se recomienda quitar el cable de un gabinete externo mientras el sistema operativo se esté ejecutando en el sistema. Quitar el cable puede provocar una configuración ajena cuando la conexión se vuelva a establecer.

Es posible administrar configuraciones ajenas en los siguientes casos:

- Se quitan y se vuelven a insertar todos los discos físicos de una configuración.
- Se quitan y se vuelven a insertar algunos de los discos físicos de una configuración.
- Se quitan todos los discos físicos de un disco virtual, pero en momentos diferentes; a continuación, se vuelven a insertar.
- Se quitan los discos físicos de un disco virtual sin redundancia.

Las siguientes limitaciones se aplican para los discos físicos que se considera importar:

- El estado de la unidad de un disco físico puede cambiar desde el momento en que se analiza la configuración ajena hasta el momento en que se ejecuta la propia importación. La importación de configuraciones ajenas solo se realiza en unidades que se encuentran en buen estado y no configuradas.
- Las unidades que se encuentran en el estado Fallido o Fuera de línea no pueden importarse.
- El firmware no permite importar más de ocho configuraciones ajenas.

Importación de la configuración ajena mediante la interfaz web

Para importar la configuración ajena:

1. En la interfaz web de iDRAC, vaya a **Almacenamiento** > **Descripción general** > **Controladoras**.
2. En la sección **Configuración ajena de importación automática mejorada**, desde el menú **Controladora**, seleccione la controladora que desea configurar.
3. En el menú desplegable **Aplicar modo de operación**, seleccione el momento en que desea realizar la importación.
4. Haga clic en **Importar configuración ajena**.

   Según el modo de operación seleccionado, se importará la configuración.

   Para importar configuraciones ajenas automáticamente, en la sección **Configurar propiedades de la controladora**, active la opción **Importación automática de configuración ajena mejorada**, seleccione **Aplicar modo de operación** y haga clic en **Aplicar**.

   NOTA: Después de activar la opción Importación automática de configuración ajena mejorada, es necesario reiniciar el sistema para importar la configuración ajena.

Importación de la configuración ajena mediante RACADM

Para importar la configuración ajena:

```
racadm storage importconfig:<Controller FQDD>
```

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

Borrar configuración ajena

Después de mover un disco físico de una controladora a otra, es posible que el disco físico contenga todos o algunos discos virtuales (configuración ajena). Puede identificar si un disco físico utilizado previamente contiene una configuración ajena (disco virtual) al verificar el estado del disco físico. Si el estado del disco físico es Ajeno, el disco físico contiene todos o algunos discos virtuales. Es posible borrar o eliminar la información del disco virtual de los discos físicos recientemente conectados.

La operación Borrar configuración ajena borra permanentemente todos los datos que residen en los discos físicos que se agregan a la controladora. Si hay más de un disco virtual ajeno presente, todas las configuraciones se borran. Puede que prefiera importar el disco virtual en lugar de destruir los datos. La inicialización debe llevarse a cabo para eliminar datos ajenos. Si se cuenta con una configuración ajena incompleta que no puede importarse, es posible usar la opción Borrado de la configuración ajena para borrar los datos ajenos de los discos físicos.

Borrado de la configuración ajena mediante la interfaz web

Para borrar la configuración ajena:

1. En la interfaz web de iDRAC, vaya a **Descripción general** > **Almacenamiento** > **Controladoras** > **Configuración**.
   Se mostrará la página **Configuración de controladoras**.
2. En la sección **Configuración ajena**, en el menú desplegable **Controladora**, seleccione la controladora en la que desea borrar la configuración ajena.
3. En el menú desplegable **Aplicar modo de operación**, seleccione el momento en que desea borrar los datos.
4. Haga clic en **Borrar**.
   Según el modo de operación seleccionado, se borrarán los discos virtuales que residen en el disco físico.

Borrado de la configuración ajena mediante RACADM

Para borrar una configuración ajena:

```
racadm storage clearconfig:<Controller FQDD>
```

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

Restablecimiento de la configuración de la controladora

Es posible restablecer la configuración de una controladora. Esta operación elimina las unidades de disco virtual y desasigna todos los repuestos dinámicos de la controladora. Esto no borra ningún dato, excepto la eliminación de los discos de la configuración. Al restablecer la configuración tampoco se eliminan las configuraciones ajenas. El soporte en tiempo real de esta función solo se encuentra disponible únicamente en el firmware PERC 9.1. Restablecer configuración no borrará datos. Puede volver a crear exactamente la misma configuración

sin una operación de inicialización que puede dar como resultado una recuperación de los datos. Debe contar con privilegio de control del servidor.

NOTA: El restablecimiento de la configuración de la controladora no elimina una configuración ajena. Para eliminar una configuración ajena, ejecute una operación de borrado de configuración.

Restablecimiento de la configuración de la controladora mediante la interfaz web

Para restablecer la configuración de la controladora:

1. En la interfaz web de iDRAC, vaya a **Almacenamiento** > **Descripción general** > **Controladoras**.
2. En **Acciones**, seleccione la opción **Restablecer configuración** para una o varias controladoras.
3. Para cada controladora, en el menú desplegable **Aplicar modo de operación**, seleccione el momento en que desea aplicar la configuración.
4. Haga clic en **Aplicar**.

   Según el modo de operación seleccionado, se aplicará la configuración.

Restablecimiento de la configuración de la controladora mediante RACADM

Para restablecer la configuración de la controladora:

```
racadm storage resetconfig:<Controller FQDD>
```

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

Cambio de modo de la controladora

NOTA: El cambio de modo de la controladora no es compatible con las controladoras PERC 10.

En las controladoras PERC 9.1, puede cambiar la personalidad de la controladora cambiando el modo de RAID a HBA. El controlador funciona de manera similar a una controladora HBA donde los controladores pasan directamente a través del sistema operativo. El cambio de modo de la controladora es una operación organizada en etapas y no ocurre en tiempo real. Antes de cambiar el modo de la controladora de RAID a HBA, asegúrese de que:

- La controladora RAID admita el cambio de modo de la controladora. La opción para cambiar el modo de la controladora no está disponible en las controladoras donde la personalidad de RAID requiere una licencia.
- Se debe eliminar o quitar todos los discos virtuales.
- Se debe eliminar o quitar los repuestos dinámicos.
- Se debe eliminar o borrar las configuraciones ajenas.
- Todos los discos físicos que se encuentran en estado de error deben ser eliminados o se debe borrar el caché fijado.
- Cualquier clave de seguridad local asociada con SED debe ser eliminada.
- La controladora no debe tener una caché preservada.
- Tiene privilegios de control de servidor para cambiar el modo de la controladora.

NOTA: Asegúrese de realizar una copia de seguridad de la configuración ajena, la clave de seguridad, los discos virtuales y los repuestos activos antes de cambiar el modo ya que los datos se eliminan.

NOTA: Asegúrese de contar con una licencia de CMC para los sleds de almacenamiento FD33xS y FD33xD de PERC antes de cambiar el modo de la controladora. Para más información sobre la licencia de CMC para los sleds de almacenamiento, consulte *Dell Chassis Management Controller Versión 1.2 para la Guía de usuario PowerEdge FX2/FX2s,* disponible en dell.com/support/manuals.

Excepciones al cambiar el modo de la controladora

La siguiente lista proporciona las excepciones al configurar el modo de la controladora mediante las interfaces de iDRAC, como la interfaz web, RACADM y WSMan:

- Si la controladora PERC se encuentra en modo RAID, debe borrar los discos virtuales, los repuestos dinámicos, las configuraciones ajenas, las claves de la controladora o la caché preservada antes de cambiar al modo HBA.
- No puede configurar otras operaciones de RAID mientras configura el modo de la controladora. Por ejemplo, si la PERC se encuentra en modo RAID y establece el valor pendiente de la PERC al modo HBA e intenta establecer el atributo BGI, el valor pendiente no se inicializa.
- Cuando cambia la controladora PERC desde el modo HBA a RAID, las unidades permanecen en estado no RAID y no se establecen automáticamente en el estado Listo. Además, el atributo **RAIDEnhancedAutoImportForeignConfig** se establece automáticamente en **Activado**.

La siguiente lista proporciona las excepciones al configurar el modo de la controladora mediante la función Perfil de configuración del servidor mediante la interfaz de RACADM o WSMan:

- La función Perfil de configuración del servidor le permite configurar varias operaciones de RAID, como también establecer el modo de la controladora. Por ejemplo, si la controladora PERC está en modo HBA, puede editar el xml de exportación para cambiar el modo de la controladora a RAID, convertir las unidades al estado Listo y crear un disco virtual.
- Al cambiar el modo de RAID a HBA, el atributo **RAIDaction pseudo** se configura para actualizarse (comportamiento predeterminado). El atributo se ejecuta y crea un disco virtual que falla. Sin embargo, aunque se cambie el modo de la controladora, el trabajo se completa con errores. Para evitar este problema, debe insertar un comentario para anular el atributo RAIDaction en el archivo XML.
- Cuando la controladora PERC está en modo HBA, si ejecuta importar la vista previa de exportación xml que está editada para cambiar el modo de la controladora a RAID e intenta crear un VD, la creación del disco virtual falla. Importar vista previa no admite la validación de las operaciones de RAID con apilamiento con el cambio de modo de la controladora.

Cambio de modo de la controladora mediante la interfaz web del iDRAC

Para cambiar el modo de la controladora, realice los siguientes pasos:

1 En la interfaz web de iDRAC, haga clic en **Almacenamiento** > **Descripción general** > **Controladoras**.
2 En la página **Controladoras** , haga clic en **Configuración** > **Modo de la controladora**.
La columna **Valor actual** muestra la configuración actual de la controladora.
3 En el menú desplegable, seleccione el modo de controladora al que desea cambiar y haga clic en **Aplicar**.
Reinicie el sistema para aplicar el cambio.

Cambio de modo de la controladora mediante RACADM

Para cambiar el modo de la controladora mediante RACADM, ejecute los comandos siguientes.

- Para ver el modo actual de la controladora:
```
$ racadm get Storage.Controller.1.RequestedControllerMode[key=<Controller_FQDD>]
```
Aparece la siguiente información:
```
RequestedControllerMode = NONE
```
- Para establecer el modo de la controladora como HBA:
```
$ racadm set Storage.Controller.1.RequestedControllerMode  HBA [Key=<Controller_FQDD>]
```

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

Operaciones con adaptadores HBA SAS de 12 Gbps

Las controladoras no RAID son HBA que no disponen de algunas capacidades de RAID. Estas controladoras no admiten discos virtuales.

La interfaz del iDRAC de 14G admite una controladora de SAS HBA de 12 Gbps y controladoras HBA330 (integradas y de adaptador).

Es posible realizar las siguientes tareas para controladoras no RAID:

- Consulte las propiedades de la controladora, los discos físicos y el gabinete según corresponda para la controladora no RAID. Consulte también las propiedades de EMM, el ventilador, la unidad de fuente de alimentación y la sonda de temperatura asociadas al gabinete. Las propiedades se muestran en función del tipo de controladora.
- Ver información sobre el inventario de software y hardware.
- Actualizar el firmware para gabinetes detrás de la controladora HBA SAS de 12 Gbps (organizados en etapas).
- Supervisar el sondeo o la frecuencia de sondeo para el estado de intervalo SMART en el disco físico cuando se detecta un cambio de estado.
- Supervisar el estado de acoplamiento activo o extracción directa en los discos físicos.
- Hacer parpadear o dejar de hacer parpadear los LED.

NOTA:

- Es necesario realizar la operación Recopilar inventario del sistema en el reinicio (CSIOR) antes de hacer un inventario o supervisar las controladoras no RAID.
- Reinicie el sistema después de realizar una actualización del firmware.
- La supervisión en tiempo real para unidades con capacidad SMART y sensores de un gabinete SES solo se realiza en las controladoras HBA SAS de 12 Gbps y en las controladoras internas HBA330.

Supervisión de análisis de falla predictiva en unidades

Storage Management es compatible con la tecnología de supervisión automática, análisis y generación de informes (SMART) en discos físicos habilitados para SMART.

SMART realiza un análisis predictivo de fallas en cada disco y envía alertas si se predice una falla del disco. Las controladoras revisan los discos físicos en busca de predicciones de fallas y, si encuentran alguna, pasan esta información a iDRAC. iDRAC inmediatamente registra una alerta.

Operaciones de la controladora en modo no RAID (HBA)

Si la controladora se encuentra en el modo no-RAID (modo HBA):

- Los discos virtuales o los repuestos dinámicos no se encuentran disponibles.
- El estado de seguridad de la controladora se encuentra desactivado.
- Todos los discos físicos se encuentran en el modo no RAID.

Es posible realizar las siguientes operaciones si la controladora se encuentra en modo no RAID:

- Hacer parpadear y dejar de hacer parpadear el disco físico.
- Configure todas las propiedades, incluidas las siguientes:
  - Modo de equilibrio de carga

- Modo de revisión de congruencia
- Modo de lectura de patrullaje
- Modo de escritura diferida
- Modo de inicio de la controladora
- Importación automática de configuración ajena mejorada
- Porcentaje de recreación
- Porcentaje de revisión de congruencia
- Porcentaje de reconstrucción
- Porcentaje de inicialización de segundo plano
- Modo de gabinete o de plano posterior
- Áreas de lectura de patrullaje no configuradas

- Ver todas las propiedades que se aplican a una controladora RAID esperadas para discos virtuales.
- Borrar configuración ajena

NOTA: Si una operación no se admite en el modo no RAID, se mostrará un mensaje de error.

Cuando la controladora se encuentra en el modo no RAID, no es posible supervisar las sondas de temperatura de gabinete, los ventiladores ni los suministros de energía.

Ejecución de trabajos de configuración de RAID en varias controladoras de almacenamiento

Al realizar operaciones en más de dos controladoras de almacenamiento desde cualquier interfaz de iDRAC compatible, asegúrese de realizar lo siguiente:

- Ejecute los trabajos en cada controladora de manera individual. Espere a que cada trabajo se complete antes de comenzar con la configuración y la creación de trabajos en la siguiente controladora.
- Programe varios trabajos de manera que se ejecuten más tarde utilizando las opciones de programación.

Administrar caché preservada

La función de caché preservada administrada es una opción de la controladora que proporciona al usuario una opción para desestimar los datos de la caché de la controladora. En la política de escritura no simultánea, los datos se escriben en la caché antes de escribirse en el disco físico. Si el disco virtual se desconecta o se elimina por cualquier motivo, los datos en la memoria caché se eliminan.

La controladora PREC conserva los datos escritos en la caché preservada o "sucia" en caso de producirse una falla en la alimentación o el cable se desconecta hasta que se recupere el disco virtual o se borre la caché.

El estado de la controladora se ve afectado por la caché preservada. El estado de la controladora aparece como degradado si la controladora tiene una caché preservada. Descartar la caché preservada solo es posible si se cumplen todas las condiciones siguientes:

- La controladora no tiene ninguna configuración ajena.
- La controladora no tiene ningún disco virtual faltante o fuera de línea.
- Ningún disco virtual tiene los cables desconectados.

Administración de SSD PCIe

El Dispositivo de estado sólido (SSD) Peripheral Component Interconnect Express (PCIe) es un dispositivo de almacenamiento de alto rendimiento diseñado para soluciones que requieren una latencia baja, muchas operaciones de entrada/salida por segundo (IOPS), y un almacenamiento profesional fiable y funcional. El diseño de SSD PCIe se basa en tecnología flash NAND con celda de nivel único (SLC) y celda de múltiples niveles (MLC) con una interfaz de alta velocidad compatible con PCIe 2.0 y PCIe 3.0. En los servidores PowerEdge de

14a generación, tenemos tres maneras diferentes de conectar SSD. Puede utilizar un extensor para conectar las unidades SSD a través de un plano posterior, conectar directamente las unidades SSD desde un plano posterior a la placa madre mediante un cable ultradelgado sin extensión, y utilizar la tarjeta HHHL (Complemento), la cual se encuentra en la placa base.

NOTA: Los servidores PowerEdge de 14a generación son compatibles con la especificación NVMe-MI estándar de la industria basada en SSD NVMe Sin embargo, los servidores PowerEdge de 13a generación solían admitir las SSD basadas en la especificación de propiedad de Dell. La adición de SSD desde cualquier generación anterior de servidores no es compatible con iDRAC9.

Si se usan interfaces de iDRAC, es posible visualizar y configurar los unidades SSD PCIe de NVMe.

A continuación se enumeran las funciones clave de PCIe SSD:

- Capacidad de acoplamiento activo
- Dispositivo de alto rendimiento

En algunos de los servidores PowerEdge de 14a generación, se admiten hasta 32 SSD NVMe.

Es posible realizar las siguientes operaciones para SSD PCIe:

- Crear inventario y supervisar de manera remota la condición de los dispositivos SSD PCIe en el servidor
- Preparar para quitar dispositivo SSD PCIe
- Borrar los datos de manera segura
- Haga parpadear o dejar de parpadear la LED de dispositivos (identifique el dispositivo)

Es posible realizar las siguientes operaciones para SSD HHHL:

- Inventario y supervisión en tiempo real del SSD HHHL en el servidor
- Informe y registro de tarjeta fallida en iDRAC y OMSS
- Borrado seguro de datos y extracción de la tarjeta
- Informes de registros TTY

Es posible realizar las siguientes operaciones para SSD:

- Informe de estado de la unidad, como por ejemplo En línea, Fallido y Desconectado

NOTA: Capacidad de acoplamiento en marcha, preparar para quitar, y hacer parpadear o dejar de hacer parpadear el LED de los dispositivos no se aplican a los dispositivos SSD PCIe HHHL.

NOTA: Cuando los dispositivos NVMe son controlados por detrás de S140, no se admiten las operaciones Prepararse para eliminar y Borrar en forma segura, aunque sí se admiten las operaciones de Parpadear y Dejar de parpadear.

Inventario y supervisión de unidades de estado sólido PCIe

La siguiente información de inventario y supervisión se encuentra disponible para los dispositivos SSD de PCIe:

- Información de hardware:
  - Tarjeta de extensión de SSD PCIe
  - Plano posterior SSD de PCIe

    Si el sistema tiene un plano posterior PCIe dedicado, se muestran dos FQDD. Una FQDD es para unidades regulares y la otra es para SSD. Si el plano posterior se comparte (universal), se muestra solo una FQDD. En caso de que las SSD estén conectados directamente, la controladora FQDD informará como CPU.1, lo que indica que la SSD está conectada directamente a la CPU.
- El inventario de software incluye solamente la versión de firmware para SSD PCIe.

Inventario y supervisión de unidades de estado sólido PCIe con la interfaz web

Para crear un inventario y supervisar los dispositivos SSD PCIe, en la interfaz web de iDRAC, vaya a **Almacenamiento** > **Descripción general** > **Discos físicos**. Aparecerá la página **Propiedades**. Para SSD PCIe, la columna **Nombre** muestra **SSD PCIe**. Expanda para ver las propiedades.

Inventario y supervisión de unidades de estado sólido PCIe con RACADM

Utilice el comando `racadm storage get controllers:<PcieSSD controller FQDD>` para crear un inventario y supervisar las SSD PCIe

Para ver todas las unidades SSD PCIe:

```
racadm storage get pdisks
```

Para ver las tarjetas de extensión PCIe:

```
racadm storage get controllers
```

Para ver la información sobre el plano posterior de SSD PCIe:

```
racadm storage get enclosures
```

NOTA: Para todos los comandos mencionados, también se muestran los dispositivos PERC.

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

Preparar para quitar una unidad SSD PCIe

Las unidades SSD PCIe admiten el intercambio directo ordenado. Esto permite agregar o quitar dispositivos sin interrumpir ni reiniciar el sistema en el que se encuentran instalados los dispositivos. Para evitar la pérdida de datos, debe utilizar la operación Preparar para quitar antes de retirar físicamente un dispositivo.

El intercambio directo ordenado solo se admite cuando las unidades SSD PCIe se encuentran instaladas en un sistema compatible donde se ejecuta un sistema operativo admitido. Para asegurarse de tener la configuración correcta para SSD PCIe, consulte el Manual del propietario específico de su sistema.

La operación Preparar para quitar no se admite para SSD PCIe en los sistemas VMware vSphere (ESXi) y en los dispositivos SSD PCIe HHHL.

NOTA: La operación Preparar para quitar se admite en sistemas con ESXi 6.0 con la versión 2.1 o posteriores del módulo de servicio de iDRAC.

La operación Preparar para quitar se puede llevar a cabo en tiempo real mediante el módulo de servicios del iDRAC.

La operación Preparar para quitar detiene toda actividad en segundo plano y toda actividad de E/S en proceso para que el dispositivo pueda extraerse de forma segura. Esta tarea hace que los LED de estado parpadeen en el dispositivo. El dispositivo se puede extraer del sistema de forma segura en las siguientes condiciones después de iniciar la operación Preparar para quitar:

- La SSD PCIe está haciendo parpadear el modelo LED seguro para quitar (parpadea una luz ámbar).
- El sistema ya no puede acceder al SSD PCIe.

Antes de preparar el SSD de PCIe para su extracción, asegúrese de lo siguiente:

- El módulo de servicio de iDRAC se encuentra instalado.

- Lifecycle Controller está activado.
- Cuenta con privilegios de inicio de sesión y control del servidor.

Forma de preparar para quitar una unidad SSD PCIe mediante la interfaz web

Para preparar el dispositivo SSD PCIe para su extracción:

1 En la interfaz web de iDRAC, vaya a **Almacenamiento** > **Descripción general** > **Discos físicos**.
Se mostrará la página **Configuración de discos físicos**.

2 En el menú desplegable **Controladora**, seleccione la tarjeta de extensión para ver las unidades SSD PCIe asociadas.

3 En los menús desplegables, seleccione **Preparar para quitar** para una o varias unidades SSD PCIe.
Si ha seleccionado **Preparar para quitar** y desea ver las otras opciones en el menú desplegable, seleccione **Acción** y, a continuación, haga clic en el menú desplegable para ver las otras opciones.

NOTA: Asegúrese de que iSM esté instalado y en ejecución para llevar a cabo la operación `preparetoremove`.

4 En el menú desplegable **Aplicar modo de operación**, seleccione **Aplicar ahora** para aplicar las acciones de inmediato.
Si hay trabajos pendientes de finalización, esta opción aparece atenuada.

NOTA: Para los dispositivos SSD PCIe, solo la opción Aplicar ahora está disponible. Esta operación no se admite en modo organizado.

5 Haga clic en **Aplicar**.
Si el trabajo no se creó, aparecerá un mensaje indicando que el trabajo no se creó correctamente. El mensaje también muestra la identificación de mensaje y las acciones de respuesta recomendadas.
Si el trabajo se creó correctamente, aparece un mensaje que indica que se ha creado la ID de trabajo para la controladora seleccionada. Haga clic en **Cola de trabajos** para ver el progreso del trabajo en la página **Cola de trabajos**.

Si no se ha creado la operación pendiente, se mostrará un mensaje de error. Si la operación pendiente es exitosa y la creación de un trabajo no se ejecuta correctamente, se mostrará un mensaje de error.

Forma de preparar para quitar una unidad SSD PCIe mediante RACADM

Para preparar el dispositivo PCIeSSD para su extracción:

```
racadm storage preparetoremove:<PCIeSSD FQDD>
```

Para crear el trabajo de destino después de ejecutar el comando **preparetoremove**:

```
racadm jobqueue create <PCIe SSD FQDD> -s TIME_NOW --realtime
```

Para consultar el id. de trabajo devuelto:

```
racadm jobqueue view -i <job ID>
```

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

Borrado de datos de un dispositivo SSD PCIe

El borrado seguro borra permanentemente todos los datos presentes en el disco. La realización de borrado criptográfico en un SSD de PCIe sobrescribe todos los bloques y provoca la pérdida permanente de todos los datos en la SSD de PCIe. Durante el borrado criptográfico, el host no puede acceder a la SSD de PCIe. Los cambios se aplican después del reinicio del sistema.

Si el sistema se reinicia o sufre una pérdida de alimentación durante el borrado criptográfico, se cancela la operación. Debe reiniciar el sistema y el proceso.

Antes de borrar datos en un dispositivo SSD PCIe, asegúrese de lo siguiente:

- Lifecycle Controller está activado.
- Cuenta con privilegios de inicio de sesión y control del servidor.

NOTA:

- El borrado de SSD de PCIe solo se puede realizar como una operación organizada en etapas.
- Después de que se borra la unidad, se muestra en línea en el sistema operativo pero no se inicializa. Debe inicializar y formatear la unidad para poder usarla nuevamente.
- Después de realizar el acoplamiento activo de una unidad SSD de PCIe, es posible que demore varios segundos para aparecer en la interfaz web.
- La función de borrado seguro es compatible con el acoplamiento activo de una unidad SSD de PCIe para servidores PowerEdge de 14ta generación.

Borrado de datos de un dispositivo SSD PCIe mediante la interfaz web

Para borrar los datos en el dispositivo SSD PCIe:

1 En la interfaz web de iDRAC, vaya a **Almacenamiento** > **Descripción general** > **Discos físicos**.
Se mostrará la página **Discos físicos**.

2 En el menú desplegable **Controladora**, seleccione la controladora para ver las unidades SSD PCIe asociadas.

3 En los menús desplegables, seleccione **Borrado seguro** para una o varias unidades SSD PCIe.
Si ha seleccionado **Borrado seguro** y desea ver las otras opciones en el menú desplegable, seleccione **Acción** y, a continuación, haga clic en el menú desplegable para ver las otras opciones.

4 En el menú desplegable **Aplicar modo de operación**, seleccione una de las siguientes opciones:
   - **Al siguiente reinicio**: seleccione esta opción para aplicar las acciones durante el siguiente reinicio del sistema.
   - **A la hora programada**: seleccione esta opción para aplicar la acciones en un día y hora programados:
     - **Hora de inicio** y **Hora de finalización**: haga clic en los iconos de calendario y seleccione los días. Desde los menús desplegables, seleccione la hora. La acción se aplica entre la hora de inicio y la hora de finalización.
     - En el menú desplegable, seleccione el tipo de reinicio:
       - Sin reinicio (se reinicia el sistema manualmente)
       - Apagado ordenado
       - Forzar apagado
       - Realizar ciclo de encendido del sistema (reinicio mediante suministro de energía)

5 Haga clic en **Aplicar**.
Si el trabajo no se creó, aparecerá un mensaje indicando que el trabajo no se creó correctamente. El mensaje también muestra la identificación de mensaje y las acciones de respuesta recomendadas.
Si el trabajo se creó correctamente, aparece un mensaje que indica que se ha creado la ID de trabajo para la controladora seleccionada. Haga clic en **Cola de trabajo en espera** para ver el progreso del trabajo en la página Cola de trabajo en espera.

Si no se ha creado la operación pendiente, se mostrará un mensaje de error. Si la operación pendiente es exitosa y la creación de un trabajo no se ejecuta correctamente, se mostrará un mensaje de error.

Borrado de datos de un dispositivo SSD PCIe mediante RACADM

Para borrar de forma segura un dispositivo SSD de PCIe:

```
racadm storage secureerase:<PCIeSSD FQDD>
```

Para crear el trabajo de destino después de ejecutar el comando **secureerase**:

```
racadm jobqueue create <PCIe SSD FQDD> -s TIME_NOW -e <start_time>
```

Para consultar el id. de trabajo devuelto:

```
racadm jobqueue view -i <job ID>
```

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

Administración de gabinetes o planos posteriores

Es posible realizar las siguientes tareas para los gabinetes o los planos posteriores:

- Ver propiedades
- Configurar el modo universal o el modo dividido
- Ver información de ranura (universal o compartida)
- Establecer el modo de SGPIO
- Set Asset Tag (Establecer etiqueta de propiedad)
- Nombre de la propiedad

Configuración del modo de plano posterior

Los servidores PowerEdge de 14ª generación de Dell admiten una nueva topología de almacenamiento interno, donde se pueden conectar dos controladoras de almacenamiento (PERC) a un conjunto de unidades internas a través de un único dispositivo expansor. Esta configuración se utiliza para el modo de alto rendimiento sin protección contra fallas o la funcionalidad de alta disponibilidad (HA). El gabinete divide el arreglo de la unidad interna entre las dos controladoras de almacenamiento. En este modo, la creación del disco virtual muestra solo las unidades conectadas a una controladora en particular. No existen requisitos de licencia para esta función. Esta función sólo se admite en algunos sistemas.

El plano posterior admite los modos siguientes:

- Modo unificado: este es el modo predeterminado. La controladora PERC primaria obtiene acceso a todas las unidades conectadas al plano posterior, incluso si existe una segunda controladora PERC instalada.
- Modo dividido: una controladora obtiene acceso a las primeras 12 unidades y la segunda controladora obtiene acceso a las últimas 12 unidades. Las unidades conectadas a la primera controladora se enumeran de 0 a 11, mientras que las unidades conectadas a la segunda controladora se enumeran de 12 a 23.
- Modo dividido 4:20: una controladora obtiene acceso a las primeras cuatro unidades y la segunda controladora obtiene acceso a las últimas 20 unidades. Las unidades conectadas a la primera controladora se enumeran de 0 a 3, mientras que las unidades conectadas a la segunda controladora se enumeran de 4 a 23.
- Modo dividido 8:16: una controladora obtiene acceso a las primeras ocho unidades y la segunda controladora obtiene acceso a las últimas 16 unidades. Las unidades conectadas a la primera controladora se enumeran de 0 a 7, mientras que las unidades conectadas a la segunda controladora se enumeran de 8 a 23.
- Modo dividido 16:8: una controladora obtiene acceso a las primeras 16 unidades y la segunda controladora obtiene acceso a las últimas ocho unidades. Las unidades conectadas a la primera controladora se enumeran de 0 a 15, mientras que las unidades conectadas a la segunda controladora se enumeran de 16 a 23.
- Modo dividido 20:4: una controladora obtiene acceso a las primeras 20 unidades y la segunda controladora obtiene acceso a las últimas cuatro unidades. Las unidades conectadas a la primera controladora se enumeran de 0 a 19, mientras que las unidades conectadas a la segunda controladora se enumeran de 20 a 23.
- Información no disponible: la información de la controladora no está disponible.

iDRAC permite el valor de modo dividido si el expansor admite la configuración. Asegúrese de activar este modo antes de instalar la segunda controladora. iDRAC realiza una comprobación de capacidad sobre el extensor antes de permitir que se configure este modo y no verifica la presencia de la segunda controladora PERC.

NOTA: Pueden aparecer errores de cable (u otros errores) si pone el plano posterior en modo dividido con solo una PERC conectada, o si pone el plano posterior en modo unificado con dos PERC conectados.

Para modificar la configuración, es necesario tener el privilegio de control del servidor.

Si alguna otra operación de RAID se muestra como pendiente o se programa un trabajo de RAID, no se puede cambiar el modo de plano posterior. De forma similar, si este valor se muestra pendiente, no es posible programar otros trabajos de RAID.

NOTA:

- Cuando se intenta modificar la configuración, se muestran mensajes de advertencia debido a la posibilidad de pérdida de datos.
- Las operaciones de eliminación de LC o restablecimiento de iDRAC no cambian la configuración del expansor para este modo.
- Esta operación solo se admite en tiempo real y no en etapas.
- Puede cambiar la configuración de plano posterior varias veces.
- La operación de división del plano posterior puede provocar la pérdida de datos o configuración ajena si la asociación de unidades cambia de una controladora a otra.
- Durante la operación de división del plano posterior, es posible que la configuración RAID sea vea afectada según la asociación de unidades.

Cualquier cambio en esta configuración sólo entra en vigencia después del reinicio durante el encendido del sistema. Al pasar del modo dividido a unificado, se mostrará un mensaje de error en el próximo inicio, ya que la segunda controladora no ve ninguna de las unidades. Además, la primera controladora verá una configuración ajena. Si se ignora el error, se perderán los discos virtuales existentes.

Configuración del modo de plano posterior mediante la interfaz web

Para configurar el modo de plano posterior mediante la interfaz web de iDRAC:

1. En la interfaz web de iDRAC, vaya a **Almacenamiento** > **Descripción general** > **Gabinetes**
2. En el menú **Gabinetes**, seleccione la controladora para configurar sus gabinetes asociados.
3. En la columna **Valor**, seleccione el modo requerido para el plano posterior o gabinete requerido:
   - Modo unificado
   - Modo dividido
   - Modo dividido 4:20
   - Modo dividido 8:16
   - Modo dividido 16:8
   - Modo dividido 20:4
   - Información no disponible

     NOTA: Para C6420, los modos disponibles son: modo dividido y modo dividido: 6:6:6:6.

   Para R740xd y R940, se necesita el ciclo de encendido del servidor para aplicar la nueva zona de plano posterior y para que C6420, el ciclo de CA (del chasis de blade) aplique la nueva zona de plano posterior.
4. En el menú desplegable **Aplicar modo de operación**, seleccione **Aplicar ahora** para aplicar las acciones inmediatamente y, a continuación, haga clic en **Aplicar**.

   Se creará una identificación de trabajo.
5. Vaya a la página **Cola de trabajos** y compruebe que se muestre el estado Completado para el trabajo.
6. Realice un ciclo de encendido del sistema para que se aplique la configuración.

Configuración de un gabinete mediante RACADM

Para configurar el gabinete o el plano posterior, utilice el comando `set` con los objetos en **BackplaneMode**.

Por ejemplo, para establecer el atributo BackplaneMode en el modo dividido:

1 Ejecute el siguiente comando para ver el modo de plano posterior actual:

```
racadm get storage.enclosure.1.backplanecurrentmode
```

El resultado es:

```
BackplaneCurrentMode=UnifiedMode
```

2 Ejecute el siguiente comando para ver el modo solicitado:

```
racadm get storage.enclosure.1.backplanerequestedmode
```

El resultado es:

```
BackplaneRequestedMode=None
```

3 Ejecute el siguiente comando para establecer el modo de plano posterior solicitado en el modo dividido:

```
racadm set storage.enclosure.1.backplanerequestedmode "splitmode"
```

Se muestra el mensaje que indica que el comando se ejecutó correctamente.

4 Ejecute el siguiente comando para verificar si el atributo **backplanerequestedmode** se ha establecido en el modo dividido:

```
racadm get storage.enclosure.1.backplanerequestedmode
```

El resultado es:

```
BackplaneRequestedMode=None (Pending=SplitMode)
```

5 Ejecute el comando `storage get controllers` y anote el valor de la Id. de la instancia de la controladora.

6 Ejecute el siguiente comando para crear un trabajo:

```
racadm jobqueue create <controller instance ID> -s TIME_NOW --realtime
```

Se devolverá una identificación de trabajo.

7 Ejecute el siguiente comando para consultar el estado del trabajo:

```
racadm jobqueue view -i JID_xxxxxxxx
```

donde `JID_xxxxxxxx` es la Id. de trabajo del paso 6.

Se indicará el estado Pendiente.

Continúe consultando el valor de ID de trabajo hasta ver el estado Completado (este proceso puede tardar hasta tres minutos).

8 Ejecute el siguiente comando para ver el valor del atributo `backplanerequestedmode`:

```
racadm get storage.enclosure.1.backplanerequestedmode
```

El resultado es:

```
BackplaneRequestedMode=SplitMode
```

9 Ejecute el siguiente comando para reiniciar mediante suministro de energía el servidor:

```
racadm serveraction powercycle
```

10 Una vez que el sistema complete el proceso POST y CSIOR, escriba el siguiente comando para verificar el valor de `backplanerequestedmode`:

```
racadm get storage.enclosure.1.backplanerequestedmode
```

El resultado es:

```
BackplaneRequestedMode=None
```

11 Ejecute el siguiente comando para verificar que el modo de plano posterior se haya establecido en el modo dividido:

```
racadm get storage.enclosure.1.backplanecurrentmode
```

El resultado es:

```
BackplaneCurrentMode=SplitMode
```

12 Ejecute el siguiente comando y verifique que solo se muestren las unidades 0-11:

```
racadm storage get pdisks
```

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

Visualización de ranuras universales

Algunos planos posteriores de servidores PowerEdge de 14.ª generación admiten unidades SAS/SATA y SSD PCIe en la misma ranura. Estas ranuras se llaman ranuras universales y se conectan a la controladora de almacenamiento primaria (PERC) y a una tarjeta de extensión PCIe. El firmware de plano posterior proporciona información sobre las ranuras que admiten esta función. El plano posterior admite discos SAS/SATA o SSD PCIe. Normalmente, las cuatro ranuras con los números más altos son universales. Por ejemplo, en un plano posterior universal que admite 24 ranuras, las ranuras de la 0 a la 19 solo admiten discos SAS/SATA, mientras que las ranuras de la 20 a la 23 admiten discos SAS/SATA o SSD PCIe.

El estado de condición de acumulación para el gabinete proporciona el estado de condición combinado para todas las unidades en el gabinete. El vínculo del gabinete en la página **Topology (Topología)** muestra toda la información del gabinete, independientemente de la controladora con la que esté asociado. Debido a que dos controladoras de almacenamiento (PERC y extensión PCIe) se pueden conectar al mismo plano posterior, solo el plano posterior asociado con la controladora PERC aparece en la página **System Inventory (Inventario del sistema)**.

En **Storage (Almacenamiento)** > **Enclosures (Gabinetes)** > **Properties (Propiedades)**, la sección **Physical Disks Overview (Descripción general de discos físicos)** muestra lo siguiente:

- **Ranura vacía**: si una ranura está vacía.
- **Compatible con PCIe**: si no hay ranuras compatibles con PCIe, esta columna no se muestra.
- **Protocolo de bus**: si se trata de un plano posterior universal con SSD de PCIe instalados en una de las ranuras, esta columna muestra **PCIe**.
- **Repuesto dinámico**: esta columna no se aplica a SSD de PCIe.

NOTA: El intercambio directo es compatible con las ranuras universales. Si desea eliminar una unidad SSD PCIe y cambiarla por una unidad SAS/SATA, asegúrese de completar primero la tarea PrepareToRemove para la unidad SSD PCIe. Si no lleva a cabo esta tarea, el sistema operativo host puede presentar problemas como una pantalla azul, una condición de pánico de kernel, etc.

Configuración de modo de SGPIO

La controladora de almacenamiento se puede conectar al plano posterior en el modo I2C (valor predeterminado para planos posteriores Dell) o en el modo de entrada/salida en serie de uso general (SGPIO). Esta conexión es necesaria para el parpadeo de los indicadores LED en las unidades. Tanto las controladoras PERC como el plano posterior Dell admiten estos modos. Para admitir ciertos adaptadores de canal, el modo de plano posterior se debe cambiar al modo de SGPIO.

El modo de SGPIO solamente es compatible con los planos posteriores pasivos. No se admite en planos posteriores basados en expansor o planos posteriores pasivos en modo descendente. El firmware de plano posterior proporciona información sobre la capacidad, el estado actual y el estado requerido.

Después de una operación de eliminación de LC o un restablecimiento de iDRAC a los valores predeterminados, el modo de SGPIO se restablece al estado desactivado. Se compara la configuración de iDRAC con la configuración del plano posterior. Si el plano posterior se ha configurado en el modo de SGPIO, iDRAC cambia su configuración para que coincida con la configuración del plano posterior.

Se requiere un ciclo de encendido del servidor para que se implementen los cambios en la configuración.

Es necesario tener el privilegio de control del servidor para modificar este valor.

NOTA: No se puede establecer el modo de SGPIO mediante la interfaz web de iDRAC.

Configuración del modo de SGPIO mediante RACADM

Para configurar el modo SGPIO, utilice el comando **set** con los objetos del grupo **SGPIOMode**.
Si el objeto se establece en desactivado, se usa el modo I2C. Si se establece en activado, se usa el modo de SGPIO.

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

Establecer la etiqueta de propiedad de un gabinete

Establecer la etiqueta de propiedad de un gabinete le permite configurar la etiqueta de propiedad de un gabinete de almacenamiento.
El usuario puede cambiar la propiedad de la etiqueta del gabinete para identificar los gabinetes. Estos campos se analizan en busca de valores inválidos y se muestra un error si se ingresa un valor inválido. Estos campos forman parte del firmware del gabinete; los datos que se muestran al comienzo son los valores guardados en el firmware.

NOTA: La etiqueta de la propiedad tiene un límite de caracteres de 10 que incluye el carácter nulo.

NOTA: Estas operaciones no se admiten en los gabinetes internos.

Establecer el nombre de propiedad de un gabinete

Establecer el nombre de propiedad de un gabinete le permite al usuario configurar el nombre de la propiedad de un gabinete de almacenamiento.
El usuario puede cambiar la propiedad de nombre del gabinete para identificar fácilmente los gabinetes. Estos campos se analizan en busca de valores inválidos y se muestra un error si se ingresa un valor inválido. Estos campos forman parte del firmware del gabinete; los datos que se muestran al comienzo son los valores guardados en el firmware.

NOTA: El nombre de la propiedad tiene un límite de caracteres de 32 que incluye el carácter nulo.

NOTA: Estas operaciones no se admiten en los gabinetes internos.

Elección de modo de operación para aplicar configuración

Durante la creación y la administración de discos virtuales, la configuración de discos físicos, controladoras y gabinetes o el restablecimiento de controladoras, antes de aplicar los distintos valores, se debe seleccionar el modo de operación. Es decir, se debe especificar el momento en que se desea aplicar la configuración:

- Inmediatamente
- Durante el siguiente reinicio del sistema
- En un tiempo programado
- Como una operación pendiente que se aplique como un lote como parte de un único trabajo

Elección del modo de operación mediante la interfaz web

Para seleccionar el modo de operación para aplicar la configuración:

1 Se puede seleccionar el modo de operación al estar en alguna de las páginas siguientes:

- **Almacenamiento** > **Discos físicos** .
- **Almacenamiento** > **Discos virtuales**
- **Almacenamiento** > **Controladoras**
- **Almacenamiento** > **Gabinetes**

2 Seleccione una de las siguientes opciones en el menú desplegable **Aplicar modo de operación**:

- **Aplicar ahora**: seleccione esta opción para aplicar los valores inmediatamente. Esta opción está disponible solo para las controladoras PERC 9. Si hay trabajos pendientes de finalización, esta opción aparece atenuada. Esta tarea demorará al menos dos minutos en completarse.
- **Al siguiente reinicio**: seleccione esta opción para aplicar los valores durante el siguiente reinicio del sistema.
- **A la hora programada**: seleccione esta opción para aplicar la configuración en un día y una hora programados:
  - **Hora de inicio** y **Hora de finalización**: haga clic en los iconos de calendario y seleccione los días. Desde los menús desplegables, seleccione la hora. La configuración se aplicará entre la hora de inicio y la hora de finalización.
  - En el menú desplegable, seleccione el tipo de reinicio:
    - Sin reinicio (se reinicia el sistema manualmente)
    - Apagado ordenado
    - Forzar apagado
    - Realizar ciclo de encendido del sistema (reinicio mediante suministro de energía)
- **Agregar a operaciones pendientes**: seleccione esta opción para crear una operación pendiente para aplicar los valores. Puede ver todas las operaciones pendientes de una controladora en la página **Almacenamiento** > **Descripción general** > **Operaciones pendientes**.

  NOTA:
  - La opción **Agregar a operaciones pendientes** no es aplicable para la página **Operaciones pendientes** ni para los dispositivos SSD PCIe en la página **Discos físicos** > **Configuración** .
  - Solo la opción **Aplicar ahora** se encuentra disponible en la página **Configuración de gabinete**.

3 Haga clic en **Aplicar**.

Según el modo de operación seleccionado, se aplicará la configuración.

Elección del modo de operación mediante RACADM

Para seleccionar el modo de operación, utilice el comando `jobqueue`.

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

Visualización y aplicación de operaciones pendientes

Puede ver y confirmar las operaciones pendientes de la controladora de almacenamiento. Todos los valores se aplicarán a la vez, durante el siguiente reinicio o a una hora programada en función de las opciones seleccionadas. Puede eliminar todas las operaciones pendientes para una controladora. No puede eliminar las operaciones pendientes individuales.

Las operaciones pendientes se crean en los componentes seleccionados (controladoras, gabinetes, discos físicos y discos virtuales).

Los trabajos de configuración se crean únicamente en la controladora. En el caso de SSD PCIe, el trabajo se crea en el disco SSD PCIe y no en la extensión PCIe.

Visualización, aplicación o eliminación de operaciones pendientes mediante la interfaz web

1 En la interfaz web de iDRAC, vaya a **Almacenamiento** > **Descripción general** > **Operaciones pendientes**.

Se mostrará la página **Operaciones pendientes**.

2 Desde el menú desplegable **Componente**, seleccione la controladora para la que desea ver, confirmar o eliminar las operaciones pendientes.

Se mostrará la lista de operaciones pendientes para la controladora seleccionada.

NOTA:

- Se crean operaciones pendientes para importar la configuración ajena, borrar la configuración ajena, operaciones de clave de seguridad y cifrar discos virtuales. Sin embargo, no se muestran en la página **Operaciones pendientes** ni en el mensaje emergente Operaciones pendientes.
- Los trabajos para SSD PCIe no se pueden crear desde la página **Operaciones pendientes**.

3 Para eliminar las operaciones pendientes en la controladora seleccionada, haga clic en **Eliminar todas las operaciones pendientes**.

4 En el menú desplegable, seleccione una de las opciones siguientes y haga clic en **Aplicar** para confirmar la pendiente operaciones:

- **Aplicar ahora**: seleccione esta opción para confirmar todas las operaciones inmediatamente. Esta opción está disponible para las controladoras PERC 9 con las últimas versiones de firmware.
- **Al siguiente reinicio**: seleccione esta opción para confirmar todas las operaciones durante el siguiente reinicio del sistema.
- **A la hora programada**: seleccione esta opción para confirmar las operaciones en un día y hora programados.
  - **Hora de inicio** y **Hora de finalización**: haga clic en los iconos de calendario y seleccione los días. Desde los menús desplegables, seleccione la hora. La acción se aplica entre la hora de inicio y la hora de finalización.
  - En el menú desplegable, seleccione el tipo de reinicio:
    - Sin reinicio (se reinicia el sistema manualmente)
    - Apagado ordenado
    - Forzar apagado
    - Realizar ciclo de encendido del sistema (reinicio mediante suministro de energía)

5 Si el trabajo de confirmación no se ha creado, aparecerá un mensaje indicando que la creación de trabajos no se completó correctamente. También se muestra la identificación del mensaje y la acción de respuesta recomendada.

6 Si el trabajo de confirmación no se ha creado, aparecerá un mensaje indicando que no se creó la Id. del trabajo para la controladora seleccionada. Haga clic en **Cola de trabajo en espera** para ver el progreso del trabajo en la página **Cola de trabajo en espera**.

Si las operaciones Borrar configuración ajena, Importar configuración ajena, Clave de seguridad o Cifrar disco virtual se encuentran en estado pendiente, y si estas son las únicas operaciones pendientes, no se podrá crear un trabajo desde la página **Operaciones pendientes**. Es necesario realizar otra operación de configuración de almacenamiento o usar el comando RACADM o WSMan para crear el trabajo de configuración requerido en la controladora requerida.

No se pueden ver ni borrar operaciones pendientes para los dispositivos SSD PCIe en la página **Operaciones pendientes**. Utilice el comando racadm para borrar las operaciones pendientes para SSD PCIe.

Visualización y aplicación de operaciones pendientes mediante RACADM

Para aplicar las operaciones pendientes, utilice el comando **jobqueue**.

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

Situaciones de almacenamiento: situaciones de aplicación de la operación

Caso 1: se seleccionó una operación de aplicación (Aplicar ahora, En el siguiente reinicio, o A la hora programada) y no hay operaciones pendientes existentes

Si seleccionó la opción **Aplicar ahora**, **En el siguiente reinicio** o **A la hora programada** y, a continuación, hizo clic en **Aplicar**, primero se crea la operación pendiente para la operación de configuración del almacenamiento seleccionada.

- Si la operación pendiente se realiza correctamente y no existen operaciones pendientes anteriores, se crea el trabajo. Si el trabajo se creó correctamente, aparece un mensaje que indica que se ha creado la Id. de trabajo para el dispositivo seleccionado. Haga clic en **Cola de trabajos** para ver el progreso del trabajo en la página **Cola de trabajos**. Si el trabajo no se creó, aparecerá un mensaje indicando que el trabajo no se creó correctamente. También se muestra la identificación del mensaje y la acción de respuesta recomendada.
- Si la operación pendiente no se crea correctamente y no hay operaciones pendientes anteriores, aparecerá un mensaje de error con la Id. y la acción de respuesta recomendada.

Caso 2: se seleccionó una operación de aplicación (Aplicar ahora, En el siguiente reinicio o A la hora programada) y existen operaciones pendientes

Si seleccionó la opción **Aplicar ahora**, **En el siguiente reinicio** o **A la hora programada** y, a continuación, hizo clic en **Aplicar**, primero se crea la operación pendiente para la operación de configuración del almacenamiento seleccionada.

- Si la operación pendiente se creó correctamente y hay operaciones pendientes, aparecerá un mensaje.
  - Haga clic en el vínculo **Ver operaciones pendientes** para ver las operaciones pendientes para el dispositivo.
  - Haga clic en **Crear trabajo** para crear el trabajo para el dispositivo seleccionado. Si el trabajo se creó correctamente, aparece un mensaje que indica que se ha creado la Id. de trabajo para el dispositivo seleccionado. Haga clic en **Cola de trabajos** para ver el progreso del trabajo en la página **Cola de trabajos**. Si el trabajo no se creó, aparecerá un mensaje indicando que el trabajo no se creó correctamente. El mensaje también muestra la identificación de mensaje y las acciones de respuesta recomendadas.
  - Haga clic en **Cancelar** para no crear el trabajo y permanecer en la página para realizar más operaciones de configuración del almacenamiento.
- Si la operación pendiente no se crea correctamente y hay operaciones pendientes, aparecerá un mensaje de error.
  - Haga clic en **Operaciones pendientes** para ver las operaciones pendientes para el dispositivo.
  - Haga clic en **Crear trabajo para operaciones correctas** para crear el trabajo para las operaciones pendientes existentes. Si el trabajo se creó correctamente, aparece un mensaje que indica que se ha creado la Id. de trabajo para el dispositivo seleccionado. Haga clic en **Cola de trabajos** para ver el progreso del trabajo en la página **Cola de trabajos**. Si el trabajo no se creó, aparecerá un mensaje indicando que el trabajo no se creó correctamente. También se muestra la identificación del mensaje y la acción de respuesta recomendada.
  - Haga clic en **Cancelar** para no crear el trabajo y permanecer en la página para realizar más operaciones de configuración del almacenamiento.

Caso 3: se seleccionó Agregar a operaciones pendientes y no existen operaciones pendientes

Si seleccionó **Agregar a operaciones pendientes** y, a continuación, hizo clic en **Aplicar**, primero se crea la operación pendiente para la operación de configuración del almacenamiento seleccionada.

- Si la operación pendiente se creó correctamente y no existen operaciones pendientes, aparecerá un mensaje informativo:
  - Haga clic en **Aceptar** para permanecer en la página para realizar más operaciones de configuración del almacenamiento.
  - Haga clic en **Operaciones pendientes** para ver las operaciones pendientes para el dispositivo. Estas operaciones pendientes no se aplican hasta que se crea el trabajo en la controladora seleccionada.
- Si la operación pendiente no se crea correctamente y no existen operaciones pendientes, aparecerá un mensaje de error.

Caso 4: se seleccionó Agregar a operaciones pendientes y no existen operaciones pendientes anteriores

Si seleccionó **Agregar a operaciones pendientes** y, a continuación, hizo clic en **Aplicar**, primero se crea la operación pendiente para la operación de configuración del almacenamiento seleccionada.

- Si la operación pendiente se crea correctamente y si existen operaciones pendientes, aparecerá un mensaje informativo:
  - Haga clic en **Aceptar** para permanecer en la página para realizar más operaciones de configuración del almacenamiento.
  - Haga clic en **Operaciones pendientes** para ver las operaciones pendientes para el dispositivo.
- Si la operación pendiente no se crea correctamente y hay operaciones pendientes, aparecerá un mensaje de error.
  - Haga clic en **Aceptar** para permanecer en la página para realizar más operaciones de configuración del almacenamiento.
  - Haga clic en **Operaciones pendientes** para ver las operaciones pendientes para el dispositivo.

NOTA:

- En cualquier momento, si no aparece la opción para crear un trabajo en las páginas de configuración del almacenamiento, vaya a la página **Descripción general del almacenamiento** > **Operaciones pendientes** para ver las operaciones pendientes existentes y para crear el trabajo en la controladora correspondiente.
- Solo los casos 1 y 2 se aplican a las SSD de PCIe. No puede ver las operaciones pendientes para los dispositivos SSD de PCIe y, por lo tanto, la opción **Agregar a operaciones pendientes** no está disponible. Utilice el comando racadm para borrar las operaciones pendientes para SSD PCIe.

Forma de hacer parpadear o dejar de hacer parpadear LED de componentes

Es posible localizar un disco físico, una unidad de disco virtual y PCIe SSD dentro de un gabinete cuando se hace parpadear uno de los diodos emisores de luz (LED) en el disco.

Es necesario tener privilegios de inicio de sesión para hacer parpadear o dejar de hacer parpadear un LED.

La controladora debe ser compatible con la configuración en tiempo real. El soporte en tiempo real de esta función solo se encuentra disponible en el firmware PERC 9.1 y las versiones posteriores.

NOTA: La opción para hacer parpadear o dejar de hacer parpadear no es compatible con los servidores sin plano posterior.

Forma de hacer parpadear o dejar de hacer parpadear LED de componentes mediante la interfaz web

Para hacer parpadear o dejar de hacer parpadear un LED de componente:

1 En la interfaz web de iDRAC, vaya a cualquiera de las siguientes páginas según su requisito:
   - **Almacenamiento** > **Descripción general** > **Discos físicos** > **Estado**: se muestra la página Discos físicos identificados, donde se puede hacer parpadear o dejar de hacer parpadear los discos físicos y los SSD PCIe.
   - **Almacenamiento** > **Descripción general** > **Discos virtuales** > **Estados**: se muestra la página Discos virtuales identificados, donde se pueden hacer parpadear o dejar de hacer parpadear los discos virtuales.
2 Si selecciona el disco físico:
   - Seleccione o anule la selección de LED de los componentes: seleccione la opción **Seleccionar/Deseleccionar todo** y haga clic en **Hacer parpadear** para iniciar el parpadeo de los LED del componente. De forma similar, haga clic en **Dejar de hacer parpadear** para detener el parpadeo de los LED del componente.
   - Seleccione o anule la selección de los LED de los componente individuales: seleccione uno o más componentes y haga clic en **Hacer parpadear** para iniciar el parpadeo del LED del componente seleccionado. De forma similar, haga clic en **Dejar de hacer parpadear** para detener el parpadeo de los LED del componente.
3 Si selecciona el disco virtual:
   - Seleccione o anule la selección de todas las unidades de disco físico o SSD PCIe: seleccione la opción **Seleccionar/Deseleccionar todo** y haga clic en **Hacer parpadear** para iniciar el parpadeo de todas las unidades de disco físico y los SSD PCIe. De forma similar, haga clic en **Dejar de hacer parpadear** para detener el parpadeo de los LED .

- Seleccione o anule la selección de unidades de disco físico o SSD PCIe: seleccione una o más unidades de disco físico y haga clic en **Hacer parpadear** para iniciar el parpadeo de los LED para las unidades de disco físicas o los SSD PCIe. De forma similar, haga clic en **Dejar de hacer parpadear** para detener el parpadeo de los LED .

4 Si se encuentra en la página **Identificar discos virtuales**:

- Seleccione o anule la selección de todos los discos virtuales: seleccione la opción **Seleccionar/Deseleccionar todo** y haga clic en **Hacer parpadear** para iniciar el parpadeo de los LED para todos los discos virtuales. De forma similar, haga clic en **Dejar de hacer parpadear** para detener el parpadeo de los LED .
- Seleccione o anule la selección de discos virtuales individuales: seleccione uno o más discos virtuales y haga clic en **Hacer parpadear** para iniciar el parpadeo de los LED de los discos virtuales. De forma similar, haga clic en **Dejar de hacer parpadear** para detener el parpadeo de los LED .

Si la operación de hacer parpadear o dejar de parpadear no es satisfactoria, se mostrarán mensajes de error.

Forma de hacer parpadear o dejar de hacer parpadear LED de componentes mediante RACADM

Para hacer parpadear o dejar de hacer parpadear LED de componentes, utilice los siguientes comandos:

```
racadm storage blink:<PD FQDD, VD FQDD, or PCIe SSD FQDD>
```

```
racadm storage unblink:<PD FQDD, VD FQDD, or PCIe SSD FQDD>
```

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

16

Configuración de BIOS

Puede ver varios atributos que se están utilizando para un servidor específico en la configuración del BIOS. Puede modificar diferentes parámetros de cada atributo desde este valor de configuración del BIOS. Una vez que seleccione un atributo, muestra los diferentes parámetros que se relacionan con dicho atributo específico. Puede modificar varios parámetros de un atributo y aplicar los cambios antes de modificar un atributo diferente. Cuando un usuario expande un grupo de configuración, se muestran los atributos en orden alfabético.

NOTA: El contenido de ayuda de nivel de atributo se genera dinámicamente.

Aplicar

El botón **Aplicar** permanece en gris hasta que alguno de los atributos se haya modificado. Una vez que realizó cambios en un atributo e hizo clic en **Aplicar,** le permite modificar el atributo con cambios necesarios. En caso de que la solicitud falle para establecer el atributo del BIOS, arroja un error con código de estado de respuesta HTTP correspondiente, asignado al error de la API SMIL o el error de creación de trabajos. Se genera un mensaje y se muestra en ese momento. Para obtener más información, consulte la *Guía de referencia de mensajes de error y de sucesos para los servidores PowerEdge Dell EMC de 14a generación,* disponibles en **dell.com/openmanagemanuals**.

Discard changes (desestimar cambios)

El botón **Discard Changes** permanece en gris hasta que se haya modificado alguno de los atributos. Si hace clic en el botón **Discard changes**, todos los cambios recientes se desestiman y se restauran con los valores anteriores o iniciales.

Aplicar y reiniciar

Cuando un usuario modifica el valor de un atributo o secuencia de inicio, tiene dos opciones para aplicar la configuración: **Aplicar y reiniciar** o **Aplicar en el siguiente reinicio**. En cualquiera de las opciones de aplicar, el usuario se redirige a la página de cola de trabajo para supervisar el progreso de ese trabajo específico.

Un usuario puede ver información de auditoría relacionada con la configuración del BIOS en los registros LC.

Si hace clic en **Aplicar y reiniciar**, se reiniciará el servidor inmediatamente para configurar todos los cambios necesarios. En caso de que la solicitud falle para establecer los atributos del BIOS, arroja un error con código de estado de respuesta HTTP correspondiente, asignado al error de la API SMIL o el error de creación de trabajos. Se genera un mensaje EEMI y se muestra en ese momento.

Aplicar en el siguiente reinicio

Cuando un usuario modifica el valor de un atributo o secuencia de inicio, tiene dos opciones para aplicar la configuración: **Aplicar y reiniciar** o **Aplicar en el siguiente reinicio**. En cualquiera de las opciones de aplicar, el usuario se redirige a la página de cola de trabajo para supervisar el progreso de ese trabajo específico.

Un usuario puede ver información de auditoría relacionada con la configuración del BIOS en los registros LC.

Si hace clic en **Aplicar en el siguiente reinicio**, configura todos los cambios necesarios en el próximo reinicio del servidor. No se verá afectado por ninguna modificación inmediata en función de los cambios de configuración recientes hasta que la siguiente sesión de reinicio se lleve a cabo correctamente. En caso de que la solicitud falle para establecer los atributos del BIOS, arroja un error con código de estado

de respuesta HTTP correspondiente, asignado al error de la API SMIL o el error de creación de trabajos. Se genera un mensaje EEMI y se muestra en ese momento.

Eliminar todos los valores pendientes

El botón **Eliminar todos los valores pendientes** se activa sólo cuando haya valores pendientes en función de los últimos cambios de configuración. En caso de que el usuario decida no aplicar los cambios de configuración, puede hacer clic en el botón **Eliminar todos los valores pendientes** para finalizar todas las modificaciones. En caso de que la solicitud falle para eliminar los atributos del BIOS, arroja un error con código de estado de respuesta HTTP correspondiente, asignado al error de la API SMIL o el error de creación de trabajos. Se genera un mensaje EEMI y se muestra en ese momento.

Valor pendiente

La configuración de un atributo del BIOS a través de la iDRAC no se aplica de inmediato a BIOS. Se debe reiniciar el servidor para que los cambios surtan efecto. Cuando se modifica un atributo del BIOS, se actualiza el **valor pendiente**. Si un atributo ya tiene un valor pendiente (el cual se ha configurado), este se muestra en la GUI.

Modificar la configuración del BIOS

La modificación de la configuración del BIOS produce entradas en el registro de auditoría, el cual se ingresa en registros LC.

17

Configuración y uso de la consola virtual

Puede utilizar la consola virtual para administrar un sistema remoto mediante el teclado, video y mouse de la estación de administración para controlar los dispositivos correspondientes en un servidor administrado. Esta es una función con licencia para los servidores en rack y torre. Está disponible de manera predeterminada para los servidores blade.

Las características claves son las siguientes:

- Se admite un máximo de seis sesiones simultáneas de la consola virtual. Todas las sesiones visualizan la misma consola de servidor administrado a la vez.
- Puede iniciar la consola virtual en un explorador web admitido con el complemento Java, ActiveX o HTML5.
- 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 un segundo usuario solicita una sesión de la 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 recibirá una notificación de que el primer usuario tiene el control. El primer usuario debe responder en treinta segundos o, de lo contrario, el acceso se otorga al segundo usuario en función de la configuración predeterminada. Cuando haya dos sesiones activas simultáneamente, el primer usuario verá un mensaje en la esquina superior derecha 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 finalización de la sesión del primer usuario terminará automáticamente la sesión del segundo usuario.

  NOTA: El número de sesiones activas de la consola virtual que se muestra en la interfaz web es solo de las sesiones de la interfaz web activa. Este número no incluye sesiones de otras interfaces como Telnet, SSH y RACADM.

  NOTA: Para obtener información sobre cómo configurar el navegador a fin de tener acceso a la consola virtual, consulte Configuración de exploradores web para usar la consola virtual.

Temas:

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 36. 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
1920 x 1200	60

Se recomienda configurar la resolución del monitor en 1920 x 1200 píxeles.

NOTA: Si hay una sesión de la 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 se selecciona el servidor en la consola local. Si el sistema ejecuta el sistema operativo Linux, es posible que no pueda visualizarse una consola X11 en el monitor local. Presione las teclas <Ctrl><Alt><F1> en la consola virtual de iDRAC para cambiar Linux a una consola de texto.

Configuración de la consola virtual

Antes de configurar la consola virtual, asegúrese de que esté configurada la estación de administración.

Es posible configurar la consola virtual mediante la interfaz web de iDRAC o la interfaz de línea de comandos RACADM.

Configuración de la consola virtual mediante la interfaz web

Para configurar la consola virtual mediante la interfaz web de iDRAC:

1. Vaya a **Configuration (Configuración)** > **Virtual Console (Consola virtual)**. Aparece la página **Consola virtual**.
2. Active la consola virtual y especifique los valores necesarios. Para obtener más información acerca de estas opciones, consulte la *Ayuda en línea de iDRAC*.

   NOTA: Si está utilizando el sistema operativo Nano, inhabilite la función de bloqueo automático del sistema en la página de la consola virtual.
3. Haga clic en **Aplicar**. Se configura la consola virtual.

Configuración de la consola virtual mediante RACADM

Para configurar la consola virtual, utilice los el comando **set** con los objetos en el grupo **iDRAC.VirtualConsole**.

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

Vista previa de la consola virtual

Antes de iniciar la Consola virtual, puede obtener una vista previa del estado de la consola virtual en la página **Sistema** > **Propiedades** > **Resumen del sistema**. La sección **Vista previa de la consola virtual** muestra una imagen que indica el estado de la Consola virtual. La imagen se actualiza cada 30 segundos. Esta es una función con licencia.

NOTA: La imagen de la consola virtual está disponible únicamente si se ha activado la consola virtual.

Inicio de la consola virtual

Es posible iniciar la consola virtual mediante la interfaz web de iDRAC o un URL:

NOTA: No inicie la sesión se 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 HTML5, Java o ActiveX.
- Hay un ancho de banda de red mínimo de 1 MB/seg.

NOTA: Si la controladora de vídeo integrada se desactiva en el BIOS e inicia la consola virtual, el visor de la consola virtual aparece en blanco.

Cuando inicia la consola virtual mediante exploradores de IE de 32 o 64 bits, utilice HTML5 o el complemento necesario (Java o ActiveX) disponible en el explorador correspondiente. Los valores de configuración de Opciones de Internet son comunes a todos los exploradores.

Cuando se inicia la consola virtual mediante el complemento Java, es posible que de vez en cuando se produzca un error de recopilación de Java. Para resolver este problema, vaya a **Panel de control de Java** > **General** > **Configuración de 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.

Para iniciar la consola virtual mediante el complemento HTML5, debe desactivar el bloqueador de elementos emergentes.

Inicio de la consola virtual mediante la interfaz web

Puede iniciar la consola virtual de las maneras siguientes:

- Vaya a **Configuración** > **Consola virtual**. Aparece la página **Consola virtual**. Haga clic en **Iniciar consola virtual**. Se inicia el **Visor de la consola virtual**.

En el **Visor de la consola virtual**, se muestra el escritorio del sistema remoto. Por medio de este visor, se pueden controlar las funciones del mouse y el teclado del sistema remoto desde la estación de administración.

Es posible que aparezcan varias casillas de mensaje después de iniciar la aplicación. Para evitar un acceso no autorizado a la aplicación, desplácese por estos cuadros de mensaje dentro de un plazo de tres minutos. De lo contrario, se le solicitará que reinicie la aplicación.

Si aparecen una o más ventanas de alerta de seguridad mientras se inicia el visor, haga clic en Sí para continuar.

Es posible que aparezcan dos punteros del mouse en la ventana del visor: uno para el servidor administrado y otro para la estación de administración. Para sincronizar los cursores, consulte Sincronización de los punteros del mouse.

Inicio de la consola virtual mediante URL

Para iniciar la consola virtual mediante el URL:

1. Abra un explorador web compatible y, en el cuadro de dirección, escriba la siguiente URL en minúsculas: **https://iDRAC_ip/console**
2. Según la configuración de inicio de sesión, aparecerá la página **Inicio de sesión** correspondiente:

- Si está desactivado el inicio de sesión único y está activado el inicio de sesión local, de Active Directory, de LDAP o mediante tarjeta inteligente, aparecerá la página **Inicio de sesión** correspondiente.
- Si está activado el inicio de sesión único, se iniciará el **Visor de la consola virtual** y la página **Consola virtual** se muestra en segundo plano.

NOTA: Internet Explorer admite el inicio de sesión local, de Active Directory, de LDAP y mediante tarjeta inteligente (SC), así como el inicio de sesión único (SSO). Firefox admite el inicio de sesión local, de AD y SSO en sistemas operativos basados en Windows y el inicio de sesión local, de Active Directory y de LDAP en sistemas operativos basados en Linux.

NOTA: Si no dispone de privilegios de acceso a la consola virtual, pero sí a los medios virtuales, al utilizar el URL se iniciarán los medios virtuales en lugar de la consola virtual.

Desactivación de mensajes de advertencia mientras se inicia la consola virtual o los medios virtuales mediante el complemento de Java o ActiveX

Puede desactivar los mensajes de advertencia mientras inicia la consola virtual o los medios virtuales mediante el complemento de Java.

NOTA: Para usar esta función e iniciar la consola virtual de iDRAC en una red IPv6 se requiere Java 8 o superior.

1 Inicialmente, al iniciar la consola virtual o los medios virtuales mediante el complemento de Java, aparece el indicador para verificar el publicador. Haga clic en **Yes (Sí)**.

Aparece un mensaje de advertencia de certificado que indica que no se ha encontrado un certificado de confianza.

NOTA: Si el certificado se encuentra en el almacén de certificados del sistema operativo o en una ubicación especificada anteriormente por el usuario, este mensaje de advertencia no se muestra.

2 Haga clic en **Continue (Continuar)**.

Se inicia el visor de la consola virtual o el visor de medios virtuales.

NOTA: El visor de medios virtuales se inicia si la consola virtual está desactivada.

3 En el menú **Herramientas**, haga clic en **Opciones de sesión** y, a continuación, en la ficha **Certificado**.

4 Haga clic en **Examinar ruta de acceso**, especifique la ubicación para almacenar el certificado del usuario, haga clic en **Aplicar**, haga clic en **Aceptar** y salga del visor.

5 Inicie la consola virtual de nuevo.

6 En el mensaje de advertencia del certificado, seleccione la opción **Confiar siempre en este certificado** y, a continuación, haga clic en **Continuar**.

7 Salga del visor.

8 Cuando vuelva a iniciar la consola virtual, el mensaje de advertencia no aparecerá.

Uso del visor de la consola virtual

El Visor de la consola virtual proporciona diversos controles como la sincronización del mouse, el ajuste de escala de la consola virtual, opciones de chat, macros para el teclado, acciones relacionadas con la alimentación, dispositivos para el siguiente inicio y acceso a medios virtuales. Para obtener información sobre cómo usar estas funciones, consulte iDRAC Online Help (Ayuda en línea de iDRAC).

NOTA: Si el servidor remoto está apagado, se mostrará el mensaje "Sin señal".

En la barra de título del Visor de la consola virtual se muestra el nombre DNS o la dirección IP del iDRAC al que se encuentra conectado desde la estación de administración. Si iDRAC no cuenta con un nombre DNS, se mostrará la dirección IP. El formato es:

- Servidores tipo bastidor y torre:

<DNS name / IPv6 address / IPv4 address>, <Model>, User: <username>, <fps>

- Servidores Blade:
  <DNS name / IPv6 address / IPv4 address>, <Model>, <Slot number>, User: <username>, <fps>

En algunas oportunidades, el Visor de la consola virtual puede mostrar un 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 de video y subsecuentemente 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**.

Consola virtual basada en HTML5

NOTA: Compruebe las notas de la versión para el soporte extendido del sistema operativo para HTML5.

NOTA: Mientras se utiliza HTML5 para acceder a la consola virtual, el idioma debe ser coherente en todo el diseño de teclado del cliente y el destino, el sistema operativo y el explorador. Por ejemplo, todos deben estar en inglés (EE. UU.) o en cualquiera de los idiomas admitidos.

Para iniciar la consola virtual de HTML5, debe activar la función de consola virtual desde la página Consola virtual de iDRAC y establecer la opción **Tipo de consola virtual** en HTML5.

Puede iniciar la consola virtual como una ventana emergente mediante uno de los métodos siguientes:

- En la página de inicio del iDRAC, haga clic en el enlace **Iniciar** disponible en la sesión Vista previa de consola
- En la página Consola virtual del iDRAC, haga clic en **Iniciar consola virtual**.
- De la página de inicio de sesión de iDRAC, escriba **https//<IP de iDRAC> /consola**. Este método se denomina inicio directo.

En la consola virtual de HTML5 están disponibles las siguientes opciones de menú:

- Añadir control de alimentación
- Orden de inicio
- Charla
- Teclado
- Captura de pantalla
- Actualizar
- Pantalla completa
- Desconectar visor
- Control de la consola
- Soportes virtuales

La opción **Pasar todas las pulsaciones de teclas al servidor** no se admite en la consola virtual HTML5. Utilice el teclado y macros de teclado para todas las teclas de función.

- Control de consola: tiene las siguientes opciones de configuración:
  - Teclado
  - Macros de teclado
  - Relación de aspecto
  - Modo táctil
  - Aceleración del mouse
- Teclado: este teclado utiliza código de origen abierto. La diferencia con el teclado físico es que las teclas numéricas pasan a caracteres especiales cuando la clave de **Bloqueo de mayúsculas** está activada. La funcionalidad sigue siendo la misma y se ingresa el número si presiona el caracter especial cuando la clave de **Bloqueo de mayúsculas** está activada.

- Macros de teclado: estos son compatibles con la consola virtual HTML5 y aparecen como las siguientes opciones del menú desplegable. Haga clic en **Aplicar** para aplicar la combinación de claves seleccionada en el servidor.
  - Ctrl+Alt+Supr
  - Alt+Tab
  - Alt+ESC
  - Ctrl+ESC
  - Alt+Espacio
  - Alt+Intro
  - Alt+Guión
  - Alt+F4
  - PrntScrn
  - Alt+PrntScrn
  - F1
  - Pausa
  - Lengüeta
  - Ctrl+Intro
  - PetSis
  - Alt+SysReq
- Relación de aspecto: la imagen de video de la consola virtual HTML5 ajusta automáticamente el tamaño para hacer la imagen visible. Las siguientes opciones de configuración se muestran en forma de lista desplegable:
  - Mantener
  - No mantener

  Haga clic en **Aplicar** para aplicar los valores seleccionados en el servidor.
- Modo táctil: la consola virtual HTML5 admite la función de Modo Táctil. Las siguientes opciones de configuración se muestran en forma de lista desplegable:
  - Directo
  - Relativa

  Haga clic en **Aplicar** para aplicar los valores seleccionados en el servidor.
- Aceleración del mouse: seleccione la aceleración del mouse en base al sistema operativo. Las siguientes opciones de configuración se muestran en forma de lista desplegable:
  - Absoluta (Windows, versiones más recientes de Linux, Mac OS-X)
  - Relativa, sin aceleración
  - Relativa (RHEL, versiones anteriores de Linux)
  - Linux RHEL 6.x y SUSE Linux Enterprise Server 11 o posterior

  Haga clic en **Aplicar** para aplicar los valores seleccionados en el servidor.
- Medios virtuales: haga clic en la opción **Conectar medios virtuales** para iniciar la sesión de medios virtuales. El menú de medios virtuales muestra la opción **Examinar** para examinar y asignar los archivos ISO e IMG.

  NOTA: No puede asignar medios físicos, como por ejemplo las unidades USB, CD o DVD mediante la consola virtual basada en HTML5.

Exploradores compatibles

La consola virtual de HTML5 se admite en los siguientes exploradores:

- Internet Explorer 11
- Chrome 36
- Firefox 30

- Safari 7.0

  NOTA: Se recomienda tener el sistema operativo Mac Versión 10.10.2 (o posterior) instalado en el sistema.

Para obtener más detalles sobre los exploradores y las versiones admitidos, consulte las *Notas de la versión de iDRAC* disponibles en **dell.com/idracmanuals**.

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.

Al utilizar 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 de mouse predeterminada del sistema operativo se utiliza para controlar la flecha del mouse en el visor de la Consola virtual.

Cuando se ven dos cursores de mouse en el visor de la Consola virtual del cliente, esto indica que el sistema operativo del servidor admite Posicionamiento relativo. Esto es típico para sistemas operativos Linux o Lifecycle Controller y genera dos cursores del mouse si los valores de aceleración del mouse del servidor son diferentes de los valores de aceleración del mouse en el cliente de la Consola virtual. Para resolver esto, cambie a un cursor único o haga coincidir la aceleración del mouse en el sistema administrado y la estación de administración:

- Para cambiar a un cursor único, en el menú **Herramientas**, seleccione **Cursor único**.
- Para establecer la aceleración del mouse, vaya a **Herramientas** > **Opciones de sesión** > **Mouse**. En la pestaña **Aceleración del mouse**, seleccione **Windows** o **Linux** en función del sistema operativo.

Para salir del modo de cursor único, presione <Esc> o la tecla de terminación configurada.

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

Si se utiliza la consola virtual para conectarse a un sistema administrado con un sistema operativo de distribución Linux recientemente instalado, es posible que se produzcan problemas de sincronización con el mouse. Esto puede deberse a la función Aceleración previsible de puntero del escritorio GNOME. Para lograr una sincronización adecuada con el mouse en la consola virtual de iDRAC, se debe desactivar esta función. Para ello, en la sección de mouse en el archivo **/etc/X11/xorg.conf**, agregue lo siguiente:

```
Option "AccelerationScheme" "lightweight".
```

Si se siguen produciendo problemas de sincronización, realice el siguiente cambio adicional en el archivo **<inicio de usuario>/.gconf/desktop/gnome/peripherals/mouse/%gconf.xml**:

Cambie los valores para `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 pestaña **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**.

Paso de las pulsaciones de tecla a través de la consola virtual para complemento de Java o ActiveX

Puede activar la opción **Pass all keystrokes to server (Pasar todas las pulsaciones de tecla al servidor)** y enviar todas las pulsaciones de tecla y combinaciones de teclas de la estación de administración al sistema administrado a través del visor de la consola virtual. Si está desactivada, dirige todas las combinaciones de teclas a la estación de administración en donde se ejecuta la sesión de la consola virtual.

Para pasar todas las pulsaciones de tecla al servidor, en el visor de la consola virtual, vaya a **Tools (Herramientas)** > **Session Options (Opciones de sesión)** > **General** y seleccione la opción **Pass all keystrokes to server (Pasar todas las pulsaciones de tecla al servidor)** para pasar las pulsaciones de tecla de la estación de administración al sistema administrado.

El comportamiento de la función Pasar todas las pulsaciones de tecla al servidor depende de lo siguiente:

- Tipo de complemento (Java o ActiveX) según la sesión de consola virtual que se inicia.

  Para el cliente Java, se debe cargar la biblioteca nativa para que funcionen tanto la opción Pass all keystrokes to server (Pasar todas las pulsaciones de tecla al servidor) como el modo Single Cursor (Cursor único). Si no se cargan las bibliotecas nativas, las opciones **Pass all keystrokes to server (Pasar todas las pulsaciones de tecla al servidor)** y **Single Cursor (Cursor único)** se muestran desactivadas. Si intenta seleccionar una de estas opciones, se mostrará un mensaje de error que indica que no se admiten las opciones seleccionadas.

  Para el cliente ActiveX, se debe cargar la biblioteca nativa para que funcionen tanto la opción Pass all keystrokes to server (Pasar todas las pulsaciones de tecla al servidor). Si no se cargan las bibliotecas nativas, la opción **Pass all keystrokes to server (Pasar todas las pulsaciones de tecla al servidor)** se muestra desactivada. Si intenta seleccionar esta opción, se mostrará un mensaje de error que indica que no se admite la opción seleccionada.

  En los sistemas operativos MAC, active la opción **Activar acceso de dispositivos de asistencia** en **Acceso universal** para que funcione la opción "Pasar todas las pulsaciones de tecla al servidor".
- El sistema operativo que se ejecuta en la estación de administración y el sistema administrado. Las combinaciones de teclas que son importantes para el sistema operativo en 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.

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 teclas) siempre se envían al sistema administrado. Esto incluye todas las teclas de función, las teclas Shift, Alt y Ctrl, y las teclas de menú. Algunas de estas teclas afectan tanto a la estación de administración como al sistema administrado.

  Por ejemplo, si la estación de administración y el sistema administrado ejecutan el sistema operativo Windows y la opción Pasar todas las teclas está desactivada, al presionar la tecla Windows para abrir el menú **Inicio**, este se abre tanto en la estación de administración como en el sistema administrado. Sin embargo, si la opción Pasar todas las teclas está activada, el menú **Inicio** se abrirá solamente en el sistema administrado y no en la estación de administración.
- Cuando la opción Pasar todas las pulsaciones de teclas está desactivada, el comportamiento depende en las combinaciones de teclas pulsadas y las combinaciones especiales que interprete el sistema operativo en la estación de administración.

Sesión de consola virtual basada en Java que se ejecuta en el sistema operativo Linux

El comportamiento mencionado para el sistema operativo Windows también se aplica al sistema operativo Linux con las excepciones siguientes:

- Cuando la opción Pasar todas las pulsaciones de teclas al servidor está activada, <Ctrl+Alt+Del> se pasa al sistema operativo en el sistema administrado.
- Las teclas mágicas SysRq son combinaciones de teclas que interpreta el núcleo de Linux. Son útiles 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 el sistema operativo Linux utilizando uno de los siguientes métodos:
  - 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 SysRq se envían al sistema operativo en el sistema administrado. El comportamiento de la secuencia de teclas para restablecer el sistema operativo, es decir, reiniciar sin desmontar ni sincronizar, depende de si las teclas mágicas SysRq están activadas o desactivadas en la estación de administración:
  - Si SysRq está activado en la estación de administración, <Ctrl+Alt+SysRq+b> o <Alt+SysRq+b> restablece la estación de administración, independientemente del estado del sistema.
  - Si SysRq está activado en la estación de administración, <Ctrl+Alt+SysRq+b> o <Alt+SysRq+b> restablece el sistema operativo del sistema administrado.
  - Otras combinación de teclas SysRq (por ejemplo, <Alt+SysRq+k>, <Ctrl+Alt+SysRq+m>, etc.) se pasan al sistema administrado, independientemente de si las teclas SysRq están activadas o no en la estación de administración.

Uso de teclas máginas de SysRq a través de la consola remota

Puede activar las teclas mágicas de SysRq a través de la consola remota mediante cualquiera de los métodos siguientes:

- Herramienta IPMI de código abierto
- Uso de SSH/Telnet o conector serie externo

Uso de la herramienta IPMI de código abierto

Asegúrese de que la configuración del BIOS/iDRAC admite la redirección de consola mediante SOL.

1 En el indicador de comandos, ejecute el comando activate SOL:

```
Ipmitool –I lanplus –H <ipaddr> -U <username> -P <passwd> sol activate
```

Se activa la sesión de SOL.

2 Después de que el servidor se inicia en el sistema operativo, aparece el indicador de inicio de sesión `localhost.localdomain`. Inicie sesión mediante el nombre de usuario y la contraseña del sistema operativo.

3 Si SysRq no está habilitado, habilítelo mediante `echo 1 >/proc/sys/kernel/sysrq`.

4 Ejecute la secuencia de interrupción `~B`.

5 Use la tecla mágica SysRq para habilitar la función SysRq. Por ejemplo, el siguiente comando muestra la información de memoria en la consola:

```
echo m > /proc/sysrq-trigger displays
```

Uso de SSH/Telnet o conector serie externo (conexión directa a través de un cable serie)

1 Para las sesiones Telnet/SSH, después de iniciar sesión mediante el nombre de usuario y la contraseña del iDRAC, en la solicitud `/admin>`, ejecute el comando `console com2`. Aparecerá la petición `localhost.localdomain` .

2 Para la redirección de la consola mediante el conector de serie externo conectado directamente al sistema mediante un cable de serie, la solicitud de inicio de sesión `localhost.localdomain` aparece después de que el servidor se inicia en el sistema operativo.

3 Inicie sesión mediante el nombre de usuario y la contraseña del sistema operativo.

4 Si SysRq no está habilitado, habilítelo mediante `echo 1 >/proc/sys/kernel/sysrq`.

5 Use la tecla mágica para habilitar la función SysRq. Por ejemplo, el siguiente comando reinicia el servidor:

```
echo b > /proc/sysrq-trigger
```

NOTA: No es necesario ejecutar la secuencia de interrupción antes de usar las teclas mágicas de SysRq.

Sesión de consola virtual basada en ActiveX que se ejecuta en el sistema operativo Windows

El comportamiento de la opción de pasar todas las pulsaciones de teclas al servidor en una sesión de consola virtual basada en ActiveX que se ejecuta en un sistema operativo de Windows es similar al comportamiento explicado para una sesión de consola virtual basada en Java que se ejecuta en la estación de administración de Windows con las excepciones siguientes:

- Cuando la opción Pasar todas las pulsaciones de teclas está desactivada, si presiona F1 se iniciará la ayuda de la aplicación tanto en la estación de administración como en el sistema administrado. También se mostrará el mensaje siguiente:

  ```
  Click Help on the Virtual Console page to view the online Help
  ```

- Es posible que las teclas multimedia no se bloqueen explícitamente.
- Las combinaciones <Alt + Espacio>, <Ctrl + Alt + +>, <Ctrl + Alt + -> no se envían al sistema administrado y son interpretadas por el sistema operativo en la estación de administración.

18

Uso del módulo de servicio del iDRAC

El Módulo de servicio del iDRAC es una aplicación de software que se recomienda instalar en el servidor (no está instalada de manera predeterminada). Complementa el iDRAC con información de supervisión del sistema operativo. Complementa al iDRAC al proporcionar datos adicionales para trabajar con las interfaces de iDRAC, como la interfaz web, Redfish, RACADM y WSMan. Puede configurar las funciones supervisadas por el módulo de servicio del iDRAC para controlar la CPU y la memoria utilizada en el sistema operativo del servidor. La interfaz de línea de comandos del sistema operativo del host se ha introducido para activar o desactivar la condición de ciclo de encendido completo de todos los componentes del sistema, excepto la unidad de suministro de energía.

NOTA: El iDRAC9 utiliza iSM versión 3.01 y superior.

NOTA: Puede utilizar el módulo de servicio del iDRAC solo si ha instalado la licencia Express o Enterprise del iDRAC.

Antes de utilizar el módulo de servicio de iDRAC, asegúrese de que:

- Tiene privilegios de Inicio de sesión, Configurar y Control del servidor en el iDRAC para activar o desactivar las funciones del módulo de servicio del iDRAC.
- No desactiva a opción **Configuración de iDRAC mediante RACADM local**.
- El canal de paso del SO a iDRAC está activada a través del bus USB interno en iDRAC.

  NOTA:
  - Cuando el módulo de servicio del iDRAC se ejecuta por primera vez, activa de manera predeterminada el canal de paso del sistema operativo al iDRAC en el iDRAC. Si desactiva esta función después de instalar el módulo de servicio del iDRAC, debe activarla manualmente en el iDRAC.
  - Si el canal de paso del sistema operativo al iDRAC se activa a través de LOM en iDRAC, no se puede utilizar el módulo de servicio de iDRAC.

Temas:

Instalación del módulo de servicio del iDRAC

Puede descargar e instalar el módulo de servicio del iDRAC desde **dell.com/support**. Debe tener privilegio de administrador en el sistema operativo del servidor para instalar el módulo de servicio del iDRAC. Para obtener información acerca de la instalación, consulte la *iDRAC Service Module Installation Guide (Guía de instalación del módulo de servicio del iDRAC)* disponible en **dell.com/support/manuals**.

NOTA: Esta función no es aplicable para los sistemas Dell Precision PR7910.

Instalación del módulo de servicio de iDRAC Express y Basic

En la página de **Configuración del módulo de servicios de iDRAC**, haga clic en **Instalar Módulo de servicios**.

1 El instalador del Módulo de servicios está disponible para el sistema operativo del host y se crea un trabajo en el iDRAC.

Para un sistema operativo Microsoft Windows o Linux, inicie sesión en el servidor local o remotamente.

2 Encuentre el volumen montado etiquetado como "**SMINST**" en su lista de dispositivos y ejecute la secuencia de comandos correspondiente:

- En Windows, abra el símbolo del sistema y ejecute el archivo por lotes **ISM-Win.bat**.
- En Linux, abra el símbolo del shell y ejecute el archivo de secuencias de comandos **ISM-Lx.sh**.

3 Una vez finalizada la instalación, el iDRAC muestra el Módulo de servicios como **instalado** y la fecha de instalación.

> **NOTA: El instalador estará disponible para el sistema operativo del host durante 30 minutos. Si la instalación no se inicia en un máximo de 30 minutos, debe reiniciar la instalación del Módulo de servicios.**

Instalación del módulo de servicio de iDRAC desde iDRAC Enterprise

1 En el asistente de **Registro de SupportAssist**, haga clic en **Siguiente**.

2 En la página de **Configuración del módulo de servicios de iDRAC**, haga clic en **Instalar Módulo de servicios**.

3 Haga clic en **Iniciar la consola virtual** y luego en **Continuar** en el cuadro de diálogo de advertencia de seguridad.

4 Para localizar el archivo del instalador de iSM, inicie sesión en el servidor en forma local o remota.

> **NOTA: El instalador estará disponible para el sistema operativo del host durante 30 minutos. Si la instalación no se inicia en un máximo de 30 minutos, debe reiniciar la instalación.**

5 Encuentre el volumen montado etiquetado como "**SMINST**" en su lista de dispositivos y ejecute la secuencia de comandos correspondiente:

- En Windows, abra el símbolo del sistema y ejecute el archivo por lotes **ISM-win.bat**.
- En Linux, abra el símbolo del shell y ejecute el archivo de secuencias de comandos **ISM-Lx.sh**.

6 Siga las instrucciones que aparecen en la pantalla para completar la instalación.

En la página **Configuración del módulo de servicios de iDRAC**, el botón de **Módulo de instalación de servicios** se desactiva una vez finalizada la instalación y el estado del Módulo de servicios se muestra **en ejecución**.

Sistemas operativos admitidos para el módulo de servicio de iDRAC

Para obtener la lista de sistemas operativos admitidos por el módulo de servicio de iDRAC, consulte *iDRAC Service Module Installation Guide* (Guía de instalación del módulo de servicio de iDRAC) disponible en **dell.com/openmanagemanuals**.

Funciones de supervisión del módulo de servicio del iDRAC

El módulo de servicio del iDRAC (iSM) proporciona las siguientes funciones de supervisión:

- Compatibilidad de perfil de Redfish para atributos de red
- Restablecimiento forzado del iDRAC

- Acceso al iDRAC a través del sistema operativo host (función experimental)
- Alertas SNMP de iDRAC en banda
- Ver información sobre el sistema operativo (SO)
- Replicar los registros de Lifecycle Controller en los registros del sistema operativo
- Opciones de recuperación automática del sistema
- Llenado del Instrumental de administración de Windows (WMI) Proveedores de administración
- Integración con SupportAssist Collection. Esto se aplica únicamente si se ha instalado el Módulo de servicio de iDRAC, versión 2.0 o posterior.
- Preparación para quitar una unidad SSD PCIe NVMe. Para obtener más información.
- Ciclo de encendido y apagado del servidor remoto.

Compatibilidad de perfil de Redfish para atributos de red

El Módulo de servicio de iDRAC v2.3 o posterior proporciona los atributos de red adicionales en iDRAC, que pueden obtenerse a través de los clientes REST desde iDRAC. Para obtener más detalles, consulte la compatibilidad de perfil de Redfish de iDRAC.

Información sobre el sistema operativo

OpenManage Server Administrator actualmente comparte la información del sistema operativo y el nombre de host con iDRAC. El módulo de servicio del iDRAC proporciona información similar, como el nombre del sistema operativo, la versión del sistema operativo y el nombre de dominio completamente calificado (FQDN) con iDRAC. De manera predeterminada, la función de supervisión está activada. No se desactiva si OpenManage Server Administrator está instalado en el sistema operativo host.

En el Módulo de servicio de iDRAC, versión 2.0 o posterior, se ha modificado la función de información del sistema operativo con la supervisión de la interfaz de red del sistema operativo. Cuando el Módulo de servicio de iDRAC, versión 2.0 o posterior, se utiliza con iDRAC 2.00.00.00, inicia la supervisión de las interfaces de red del sistema operativo. Puede ver esta información mediante la interfaz web de iDRAC, RACADM o WSMan.

Replicar registros de Lifecycle en el registro del sistema operativo

Puede replicar los registros de Lifecycle Controller en los registros del sistema operativo desde el momento en que la función se activa en el iDRAC. Es similar a la replicación del registro de sucesos del sistema (SEL) que realiza OpenManage Server Administrator. Todos los sucesos que tienen la opción **OS Log (Registro del sistema operativo)** seleccionada como destino (en la página **Alerts (Alertas)** o en las interfaces equivalentes de RACADM o WSMan) se replican en el registro del sistema operativo mediante el Módulo de servicio de iDRAC. El conjunto predeterminado de registros que se va a incluir en los registros del sistema operativo es igual que el valor configurado para las alertas o capturas de SNMP.

El módulo de servicio del iDRAC también registra los sucesos ocurridos cuando el sistema operativo no funciona. Los registros del sistema operativo realizados por el Módulo de servicio de iDRAC siguen los estándares de registro del sistema IETF para los sistemas operativos basados en Linux.

NOTA: A partir de la versión 2.1 del Módulo de servicio de iDRAC, la ubicación de la replicación de los registros de Lifecycle Controller en los registros del sistema operativo Windows puede configurarse mediante el uso del instalador del Módulo de servicio de iDRAC. Puede configurar la ubicación al instalar el Módulo de servicio de iDRAC o modificar el instalador del Módulo de servicio de iDRAC.

Si OpenManage Server Administrator está instalado, esta función de supervisión se desactiva para evitar duplicar las anotaciones de SEL en el registro del sistema operativo.

NOTA: En Microsoft Windows, si los sucesos de iSM se registran en los registros del sistema en lugar de registros de la aplicación, reinicie el servicio de registro de eventos de Windows o reinicie el sistema operativo del host.

Opciones de recuperación automática del sistema

La función de recuperación automática del sistema es un temporizador basado en hardware. Si se produce una falla de hardware, es posible que no se invoque el supervisor de la condición, pero el servidor se restablece como si el interruptor de alimentación estuviera activado. La opción ASR se implementa mediante un temporizador de "pulso" que continuamente cuenta en forma descendente. El supervisor de la condición con frecuencia recarga el contador para evitar la cuenta regresiva a cero. Si la opción ASR cuenta en forma descendente hasta cero, se supone que el sistema operativo se ha bloqueado y el sistema intenta reiniciarse automáticamente.

Puede realizar operaciones de recuperación automática del sistema, tales como reinicio, ciclo de encendido o apagado del servidor después de un intervalo de tiempo especificado. Esta función está activada solo si el temporizador de vigilancia del sistema operativo está desactivado. Si OpenManage Server Administrator está instalado, esta función de supervisión se desactiva para evitar la duplicación de los temporizadores de vigilancia.

Proveedores del Instrumental de administración de Windows

El WMI es un conjunto de extensiones para el modelo de controlador de Windows que proporciona una interfaz de sistema operativo a través de la cual los componentes instrumentados proporcionan información y notificaciones. El WMI es la implementación de Microsoft de los estándares de administración empresarial basada en la web (WBEM) y el modelo común de información (CIM) de Distributed Management Task Force (DMTF) para administrar el hardware del servidor, los sistemas operativos y las aplicaciones. Los proveedores de WMI permiten la integración con consolas de administración de sistemas como Microsoft System Center y permiten las secuencias de comandos para administrar Microsoft Windows Server.

Es posible activar o desactivar la opción de WMI en el iDRAC. El iDRAC expone las clases de WMI a través del módulo de servicio del iDRAC y proporciona la información sobre la condición del servidor. De manera predeterminada, se activa la función de información sobre WMI. El Módulo de servicio de iDRAC expone las clases supervisadas de WSMan en la iDRAC a través de WMI. Las clases se exponen en el espacio de nombres **root/cimv2/dcim**.

Es posible acceder a las clases mediante cualquiera de las interfaces de cliente de WMI estándar. Para obtener más información, consulte los documentos de perfiles.

En los ejemplos siguientes, se utiliza la clase DCIM_account para ilustrar la capacidad que proporciona la función de información sobre WMI en el Módulo de servicio de iDRAC. Para conocer los detalles de las clases y los perfiles compatibles, consulte la documentación sobre perfiles WSMan disponible en Dell TechCenter.

Interfaz CIM	WinRM	WMIC	PowerShell
Enumere las instancias de una clase	`winrm e wmi/root/cimv2/dcim/dcim_account`	`wmic /namespace:\\root\cimv2\dcim PATH dcim_account`	`Get-WmiObject dcim_account -namespace root/cimv2/dcim`
Obtenga una instancia específica de una clase	`winrm g wmi/root/cimv2/dcim/DCIM_Account?CreationClassName=DCIM_Account+Name=iDRAC.Embedded.1#Users.2+SystemCreationClassName=DCIM_SPComputerSystem+SystemName=systemmc`	`wmic /namespace:\\root\cimv2\dcim PATH dcim_account where Name="iDRAC.Embedded.1#Users.16"`	`Get-WmiObject -Namespace root\cimv2\dcim -Class dcim_account -filter "Name='iDRAC.Embedded.1#Users.16'"`
Obtenga instancias asociadas de una instancia	`winrm e wmi/root/cimv2/dcim/* -`	`wmic /namespace:\\root\cimv2\dcim PATH`	`Get-Wmiobject -Query "ASSOCIATORS OF`

Interfaz CIM	WinRM	WMIC	PowerShell
	`dialect:association -filter: {object=DCIM_Account? CreationClassName=DCIM_Account +Name=iDRAC.Embedded.1#Users.1+SystemCreationClassName=DCIM_SPComputerSystem+SystemName=systemmc}`	`dcim_account where Name='iDRAC.Embedded.1#Users.2' ASSOC`	`{DCIM_Account.CreationClassName='DCIM_Account',Name='iDRAC.Embedded.1#Users.2',SystemCreationClassName='DCIM_SPComputerSystem',SystemName='systemmc'}" -namespace root/cimv2/dcim`
Obtenga referencias de una instancia	`winrm e wmi/root/cimv2/dcim/* -dialect:association -associations -filter: {object=DCIM_Account? CreationClassName=DCIM_Account +Name=iDRAC.Embedded.1#Users.1+SystemCreationClassName=DCIM_SPComputerSystem+SystemName=systemmc}`	No aplicable	`Get-Wmiobject -Query "REFERENCES OF {DCIM_Account.CreationClassName='DCIM_Account',Name='iDRAC.Embedded.1#Users.2',SystemCreationClassName='DCIM_SPComputerSystem',SystemName='systemmc'}" -namespace root/cimv2/dcim`

Restablecimiento forzado remoto del iDRAC

Mediante iDRAC, puede supervisar los servidores admitidos para los problemas críticos de software, firmware o hardware del sistema. A veces, es posible que iDRAC deje de responder debido a diversas razones. Durante estos casos, deberá apagar el servidor y restablecer iDRAC. Para restablecer la CPU de iDRAC, debe apagar y encender el servidor o realizar un ciclo de apagado y encendido de CA.

Mediante la función de restablecimiento forzado de iDRAC remoto, cada vez que iDRAC no responde, puede realizar una operación de restablecimiento de iDRAC remoto sin un ciclo de apagado y encendido de CA. Para restablecer la iDRAC de manera remota, asegúrese de tener privilegios de administrador en el sistema operativo host. De manera predeterminada, la función de restablecimiento forzado de iDRAC remoto está activada. Puede realizar un restablecimiento forzado de iDRAC remoto mediante la interfaz web de iDRAC, RACADM y WSMan.

Uso del comando

En esta sección se proporcionan los usos del comando para sistemas operativos Windows, Linux y ESXi para llevar a cabo el restablecimiento forzado del iDRAC.

- **Windows**
  - Mediante el Instrumental de administración de Windows (WMI) local:

    ```
    winrm i iDRACHardReset wmi/root/cimv2/dcim/DCIM_iSMService?
    InstanceID="iSMExportedFunctions"
    ```

  - Mediante la interfaz remota de WMI:

    ```
    winrm i iDRACHardReset wmi/root/cimv2/dcim/dcim_ismservice -u:<admin-username> -p:<admin-passwd> -r: http://<remote-hostname OR IP>/wsman -a:Basic -encoding:utf-8 -skipCACheck -skipCNCheck
    ```

  - Mediante la secuencia de comandos de Windows PowerShell con y sin fuerza:

    ```
    Invoke-iDRACHardReset -force
    ```

    ```
    Invoke-iDRACHardReset
    ```

  - Mediante el acceso directo **Menú de programación**:

Por razones de simplicidad, iSM proporciona un acceso directo en el **menú de programación** del sistema operativo Windows. Al seleccionar la opción **Remote iDRAC Hard Reset (Restablecimiento forzado de iDRAC remoto)**, se le solicitará una confirmación para restablecer iDRAC. Después de confirmar todo, iDRAC se restablecerá y se mostrará el resultado de la operación.

NOTA: Aparecerá el siguiente mensaje de advertencia en Event Viewer (Visor de sucesos) en la categoría Application Logs (Registros de la aplicación). Esta advertencia no requiere ninguna otra acción.

```
A provider, ismserviceprovider, has been registered in the Windows Management Instrumentation namespace Root\CIMV2\DCIM to use the LocalSystem account. This account is privileged and the provider may cause a security violation if it does not correctly impersonate user requests.
```

- **Linux**

  El Módulo de servicio de iDRAC (iSM) proporciona un comando ejecutable en todos los sistemas operativos Linux compatibles con iSM. Puede ejecutar este comando mediante un inicio de sesión en el sistema operativo con SSH o un equivalente.

  ```
  Invoke-iDRACHardReset
  ```

  ```
  Invoke-iDRACHardReset -f
  ```

- **ESXi**

  En todos los sistemas operativos ESXi compatibles con iSM, iSM v2.3 admite un proveedor del método de interfaz de programación común de administración (CMPI) para restablecer el iDRAC de manera remota mediante los comandos remotos WinRM.

  ```
  winrm i iDRACHardReset http://schemas.dell.com/wbem/wscim/1/cim-schema/2/root/cimv2/dcim/DCIM_iSMService?__cimnamespace=root/cimv2/dcim+InstanceID=iSMExportedFunctions -u:<root-username> -p:<passwd> -r:https://<Host-IP>:443/WSMan -a:basic -encoding:utf-8 -skipCNCheck -skipCACheck -skipRevocationcheck
  ```

NOTA: El sistema operativo ESXi VMware no le pedirá confirmación antes de restablecer el iDRAC.

NOTA: Debido a las limitaciones en el sistema operativo VMware ESXi, la conectividad de iDRAC no se restaura por completo después del restablecimiento. Asegúrese de restablecer iDRAC manualmente.

Gestión de errores

Tabla 37. Gestión de errores

Resultado	Descripción
0	Ejecución satisfactoria
1	Versión del BIOS admitida para restablecimiento del iDRAC
2	Plataforma no admitida
3	Acceso denegado
4	Falló el restablecimiento del iDRAC

Compatibilidad dentro de banda para las alertas SNMP del iDRAC

Al usar el módulo de servicio del iDRAC 2.3, puede recibir alertas SNMP desde el sistema operativo host, que es similar a las alertas generadas por el iDRAC.

También puede supervisar las alertas de SNMP de iDRAC sin configurar iDRAC y administrar el servidor de manera remota al configurar las capturas de SNMP y el destino en el sistema operativo host. En el Módulo de servicio de iDRAC v2.3 o posterior, esta función convierte todos los registros de Lifecycle replicado en registros del sistema operativo en las capturas de SNMP.

NOTA: Esta función se activa solamente cuando la función de replicación de los registros de Lifecycle está activada.

NOTA: En los sistemas operativos Linux, esta función requiere un SNMP maestro o del sistema operativo activado con el protocolo de multiplexación de SNMP (SMUX).

De forma predeterminada, esta función está desactivada. A pesar de que el mecanismo de alertas de SNMP dentro de banda puede coexistir junto con el mecanismo de alertas de SNMP de iDRAC, los registros podrían tener alertas de SNMP redundantes de ambos orígenes. Se recomienda utilizar la opción dentro de banda o la opción fuera de banda, en lugar de usar ambas.

Uso del comando

En esta sección se proporcionan los usos del comando para los sistemas operativos Windows, Linux y ESXi.

- **Sistema operativo Windows**
  - Mediante el Instrumental de administración de Windows (WMI) local:

    ```
    winrm i EnableInBandSNMPTraps
    wmi/root/cimv2/dcim/DCIM_iSMService?InstanceID="iSMExportedFunctions" @{state="[0/1]"}
    ```

  - Mediante la interfaz remota de WMI:

    ```
    winrm i EnableInBandSNMPTraps wmi/root/cimv2/dcim/DCIM_iSMService?
    InstanceID="iSMExportedFunctions" @{state="[0/1]"}
    -u:<admin-username> -p:<admin-passwd> -r:http://<remote-hostname OR IP>/WSMan  -a:Basic -
    encoding:utf-8 -skipCACheck -skipCNCheck
    ```

- **Sistema operativo Linux**

  En todos los sistemas operativos Linux compatibles con iSM, iSM proporciona un comando ejecutable. Puede ejecutar este comando mediante un inicio de sesión en el sistema operativo con SSH o un equivalente.

  A partir de iSM 2.4.0, se puede configurar Agent-x como el protocolo predeterminado para las alertas de SNMP de iDRAC en banda mediante el comando siguiente:

  ```
  ./Enable-iDRACSNMPTrap.sh 1/agentx –force
  ```

  Si `–force` no se especifica, asegúrese de que net-SNMP esté configurado y reinicie el servicio snmpd.

  - Para activar esta función:

    ```
    Enable-iDRACSNMPTrap.sh 1
    ```

    ```
    Enable-iDRACSNMPTrap.sh enable
    ```

  - Para desactivar esta función:

    ```
    Enable-iDRACSNMPTrap.sh 0
    ```

    ```
    Enable-iDRACSNMPTrap.sh disable
    ```

    NOTA: La opción --force configura Net-SNMP para reenviar las capturas. No obstante, debe configurar el destino de las capturas.

- **Sistema operativo ESXi VMware**

  En todos los sistemas operativos ESXi compatibles con iSM, iSM v2.3 admite un proveedor del método de interfaz de programación común de administración (CMPI) para activar esta función de manera remota mediante los comandos remotos WinRM.

  ```
  winrm i EnableInBandSNMPTraps http://schemas.dell.com/wbem/wscim/1/cim-schema/2/root/cimv2/
  dcim/DCIM_iSMService?
  __cimnamespace=root/cimv2/dcim+InstanceID=iSMExportedFunctions -u:<user-name> -p:<passwd> -
  r:https://<remote-host-name
  ```

  ```
  ip-address>:443/WSMan -a:basic -encoding:utf-8 -skipCNCheck -skipCACheck -skipRevocationcheck
  @{state="[0/1]"}
  ```

  NOTA: Se debe revisar y configurar todos los valores SNMP del sistema ESXi VMware para las capturas.

NOTA: Para obtener más detalles, consulte el documento técnico In-BandSNMPAlerts disponible en http://en.community.dell.com/techcenter/extras/m/white_papers.

Acceso al iDRAC a través del sistema operativo host

Con el uso de esta función, puede configurar y supervisar los parámetros de hardware a través de la interfaz web de iDRAC, WSMan y Redfish utilizando la dirección IP del host sin configurar la dirección IP de iDRAC. Puede utilizar las credenciales de iDRAC predeterminadas si el servidor de iDRAC no está configurado o continuar usando las mismas credenciales de iDRAC si el servidor de iDRAC haya se ha configurado previamente.

Acceso al iDRAC a través de los sistemas operativos Windows

Puede realizar esta tarea mediante alguno de los siguientes métodos:

- Instale la función del acceso al iDRAC mediante el paquete web.
- Configure con la secuencia de comandos PowerShell de iSM

Instalación mediante MSI

Puede instalar esta función mediante web-pack. Esta función está desactivada en la instalación típica de iSM. Si está activada, el número de puerto de escucha predeterminado es 1266 Puede modificar este número de puerto dentro del rango de 1024 a 65535. El iSM redirige la conexión a iDRAC. El iSM, a continuación, crea una regla de servidor de seguridad entrante, OS2iDRAC. El número de puerto de escucha se agrega a la regla de servidor de seguridad OS2iDRAC en el sistema operativo host, que permite las conexiones entrantes. La regla de servidor de seguridad se activa automáticamente cuando se activa esta función.

A partir de iSM 2.4.0, puede recuperar el estado actual y la configuración de puerto de escucha mediante el siguiente Powershell cmdlet:

```
Enable-iDRACAccessHostRoute -status get
```

La salida de este comando indica si esta función está activada o desactivada. Cuando la función está activada, se muestra el número de puerto de escucha.

NOTA: Asegúrese de que los servicios Microsoft IP Helper se estén ejecutando en su sistema para que esta función funcione.

Para acceder a la interfaz web de iDRAC, utilice el formato `https://<host-name>` o `OS-IP>:443/login.html` en el navegador, donde:

- `<host-name>`: nombre de host completo del servidor en el que iSM está instalado y configurado para el acceso de iDRAC a través del SO. Puede utilizar la dirección IP del sistema operativo si el nombre de host no está presente.
- `443`: número de puerto de iDRAC predeterminado. Se denomina el número de puerto de conexión al que se redirigen todas las conexiones de entrada en número de puerto de escucha. Puede modificar el número de puerto a través de la interfaz web de iDRAC, WSMan y RACADM.

Configuración mediante iSM PowerShell cmdlet

Si esta función está desactivada al instalar iSM, puede activarla función mediante el siguiente comando de Windows PowerShell proporcionado por iSM:

```
Enable-iDRACAccessHostRoute
```

Si la función ya está configurada, puede desactivarla o modificarla con el comando PowerShell y las opciones correspondientes. Las opciones disponibles son las siguientes:

- **Status (Estado)**: este parámetro es obligatorio. Los valores no distinguen entre mayúsculas y minúsculas, y el valor puede ser **true**, **false** o **get**.
- **Port (Puerto)**: es el número de puerto de escucha. Si no proporciona un número de puerto, se usará el número de puerto predeterminado (1266). Si el valor del parámetro **Status (Estado)** es FALSE, podrá ignorar el resto de los parámetros. Debe introducir un nuevo número de puerto que no esté ya configurado para esta función. La configuración del nuevo número de puerto sobrescribe la

regla de servidor de seguridad entrante OS2iDRAC existente, y usted podrá utilizar el nuevo número de puerto para conectarse con iDRAC. El rango de valores es de 1024 a 65535.

- **IpRange (Rango de IP)**: este parámetro es opcional y proporciona un rango de direcciones IP que pueden conectarse con iDRAC a través del sistema operativo host. El formato del rango de direcciones IP es el formato de enrutamiento interdominios sin clases (CIDR), que es una combinación de dirección IP y máscara de subred. Por ejemplo: 10.94.111.21:24. El acceso a iDRAC está restringido para direcciones IP que no se encuentren dentro de dicho rango.

  NOTA: Esta función solo admite direcciones IPv4.

Acceso al iDRAC a través de los sistemas operativos Linux

Puede instalar esta función mediante el archivo **setup.sh** que está disponible en el paquete web. Esta función está desactivada en una instalación predeterminada o típica de iSM. Para obtener el estado de esta función, utilice el siguiente comando:

```
Enable-iDRACAccessHostRoute get-status
```

Para instalar, activar y configurar esta función, utilice el comando siguiente:

```
./Enable-iDRACAccessHostRoute <Enable-Flag> [ <source-port> <source-IP-range/source-ip-range-mask>]
```

<Enable-Flag>=0	Deshabilitar No se requieren `<source-port>` y `<source-IP-range/source-ip-range-mask>`.
<Enable-Flag>=1	Activar Se requiere `<source-port>` y `<source-ip-range-mask>` es opcional.
<source-IP-range>	Rango de IP en formato *<IP-Address/subnet-mask>*. Por ejemplo: 10.95.146.98/24.

Coexistencia de OpenManage Server Administrator y módulo de servicio del iDRAC

En un sistema, OpenManage Server Administrator y el módulo de servicio del iDRAC pueden coexistir y seguir funcionando de manera correcta e independiente.

Si ha activado las funciones de supervisión durante la instalación del módulo de servicio del iDRAC, una vez finalizada la instalación y si el módulo de servicio del iDRAC detecta la presencia de OpenManage Server Administrator, el conjunto de funciones de supervisión que se superponen se desactivan. Si OpenManage Server Administrator se está ejecutando, el módulo de servicio del iDRAC desactiva las funciones de supervisión que se superponen después de iniciar sesión en el sistema operativo y en el iDRAC.

Cuando vuelva a activar estas funciones de supervisión a través de las interfaces de iDRAC después, se realizan las mismas comprobaciones y las funciones se activan según si OpenManage Server Administrator se está ejecutando o no.

Uso del módulo de servicio del iDRAC desde la interfaz web del iDRAC

Para utilizar el módulo del servicio del iDRAC desde la interfaz web del iDRAC:

1. Vaya a **Configuración de IDRAC** > **Descripción general** > **Módulo de servicio de iDRAC** > **Configurar Módulo de servicio**. Aparece la página **Configuración del módulo de servicio del iDRAC**.
2. Puede ver lo siguiente:
   - Versión del módulo de servicio del iDRAC instalado en el sistema operativo host.

- Estado de conexión del módulo de servicio del iDRAC con el iDRAC.

3 Para llevar a cabo funciones de supervisión fuera de banda, seleccione una o más de las siguientes opciones:
   - **Información de sistema operativo**: vea la información del sistema operativo.
   - **Replicar registro de Lifecycle en el registro del sistema operativo**: incluya los registros de Lifecycle Controller en los registros del sistema operativo. Esta opción está desactivada si OpenManage Server Administrator está instalado en el sistema.
   - **Información sobre WMI**: incluya la información de WMI.
   - **Acción de recuperación automática del sistema**: realice opciones de recuperación automática en el sistema después de un período de tiempo especificado (en segundos):
     - **Reiniciar**
     - **Apagar el sistema**
     - **Realizar ciclo de encendido del sistema**

     Esta opción está desactivada si OpenManage Server Administrator está instalado en el sistema.

Uso del módulo de servicio del iDRAC desde RACADM

Para utilizar el módulo de servicio de iDRAC desde RACADM, use los objetos en el grupo **ServiceModule**.

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

Utilización del módulo de servicio de iDRAC en el sistema operativo Windows Nano

Para obtener las instrucciones de instalación, consulte la *guía de instalación del módulo de servicio de iDRAC*.

Para comprobar si el servicio iSM está en ejecución, utilice el siguiente comando cmdlet:

```
Get-Service "iDRAC Service Module"
```

Puede ver los registros de Lifecycle replicados con la consulta de WMI o Windows PowerShell:

```
GetCimInstance –Namespace root/cimv2 – className win32_NTLogEvent
```

De manera predeterminada, los registros están disponibles en **Visor de eventos** > **Registros de aplicaciones y servicios** > **Sistema**.

19

Uso de un puerto USB para la administración del servidor

En los servidores de 13ª generación y posteriores supervisados por el iDRAC, puede realizar las siguientes funciones en un puerto USB y una unidad USB:

- Configure un servidor mediante los archivos almacenados en una unidad USB colocada en un puerto USB, que es supervisado por un iDRAC.

  NOTA: El puerto USB Micro B es compatible con iDRAC9.

  NOTA:

  - Para administrar un puerto USB o configurar un servidor mediante la importación de archivos de configuración XML en una unidad USB, debe tener el privilegio de Control del sistema. Para obtener más información acerca de la administración de un puerto USB, consulte la documentación técnica Asignación de puertos USB y Administración de unidades USB en servidores de la 13a generación y posteriores.

  Introduzca lo siguiente y haga clic en Aplicar.

  Modo de puerto de administración USB: en servidores de la 14a generación, iDRAC directo solamente le permite configurar el modo de puerto USB:

  - iDRAC directo solamente: seleccione esta opción para indicar que solo un iDRAC debe usar un puerto USB. Cuando un iDRAC usa un puerto USB, no puede reasignarlo al sistema operativo.

  iDRAC administrado:

  iDRAC directo solamente: seleccione esta opción para indicar que solo un iDRAC debe usar un puerto USB. Cuando un iDRAC usa un puerto USB, no puede reasignarlo al sistema operativo.

  - Deshabilitado: seleccione esta opción para indicar que los archivos del Perfil de configuración del servidor no se deben importar.

NOTA: iDRAC9 le permite proteger con contraseña el archivo comprimido después de utilizar Habilitado solamente para archivos de configuración comprimidos para comprimir el archivo antes de realizar la importación. Puede introducir una contraseña para proteger el archivo mediante la opción Contraseña para archivo zip.

Temas:

Acceso a la interfaz de iDRAC por medio de la conexión USB directa

La función de iDRAC directo permite conectar directamente el puerto USB de su equipo de escritorio o equipo portátil al puerto USB de iDRAC. Esto le permite interactuar directamente con las interfaces de iDRAC (por ejemplo, la interfaz web, RACADM y WSMan) para lograr una administración y un mantenimiento avanzados de los servidores.

Para acceder a la interfaz de iDRAC por medio del puerto USB:

1 Apague las redes inalámbricas y desconéctelas de cualquier otra red de conexión permanente.
2 Asegúrese de que el puerto USB esté activado. Para obtener más información, consulte el Configuración de los valores de puerto de administración USB .
3 Espere a que se asigne la dirección IP a su equipo portátil (169.254.0.3) y al iDRAC (169.254.0.3). Esta acción puede demorar varios segundos.
4 Empiece a utilizar las interfaces de red de iDRAC, como la interfaz web, RACADM, Redfish o WSMan.
5 Cuando iDRAC utiliza el puerto USB, el indicador LED parpadea indicando actividad. La frecuencia es de cuatro parpadeos por segundo.
6 Después del uso, desconecte el cable.

El LED se apagará.

Configuración de iDRAC mediante el perfil de configuración del servidor en un dispositivo USB

Con la nueva función de iDRAC directo, se puede configurar iDRAC en el servidor. En primer lugar, configure los valores del puerto de administración USB en iDRAC, inserte el dispositivo USB que contiene el perfil de configuración del servidor y, a continuación, importe el perfil de configuración del servidor del dispositivo USB a iDRAC.

NOTA: Puede establecer los valores del puerto de administración USB mediante las interfaces de iDRAC solo si no hay ningún dispositivo USB conectado al servidor.

NOTA: Los sistemas PowerEdge que no tienen el LCD y el panel de LED no admiten la memoria USB.

Configuración de los valores de puerto de administración USB

Es posible configurar el puerto USB en iDRAC de la siguiente manera:

- Active o desactive el puerto USB del servidor con la configuración del BIOS. Cuando iDRAC se establece en **Todos los puertos apagados** o **Puertos frontales apagados**, también se desactiva el puerto USB administrado. El estado del puerto se puede ver por medio de las interfaces de iDRAC. Si se indica el estado desactivado:
  - iDRAC no procesa un dispositivo USB o el host conectado al puerto USB administrado.
  - Es posible modificar la configuración del puerto USB administrado, pero la configuración no se aplicará hasta que los puertos USB en el panel anterior se activen en el BIOS.
- Establezca el modo de puerto de administración USB que determina si el puerto USB debe ser utilizado por iDRAC o el sistema operativo del servidor:
  - Automático (predeterminado): si un dispositivo USB no es compatible con iDRAC o si el perfil de configuración del servidor no está presente en el dispositivo, el puerto USB se desconecta de iDRAC y se conecta al servidor. Cuando se extrae un dispositivo del servidor, la configuración del puerto se restablece y su uso queda destinado para iDRAC.
  - Uso estándar del sistema operativo: el dispositivo USB siempre es utilizado por el sistema operativo.
  - iDRAC directo solamente: el dispositivo USB siempre es utilizado por iDRAC.

Es necesario contar con el privilegio de control de servidor para configurar el puerto de administración USB.

Cuando existe un dispositivo USB conectado, la página Inventario del sistema muestra la información del dispositivo USB en la sección Inventario de hardware.

Se registra un suceso en los registros de Lifecycle Controller en las siguientes situaciones:

- El dispositivo se encuentra en modo automático o modo iDRAC y se inserta o se extrae el dispositivo USB.
- El modo de puerto de administración USB se modifica.
- El dispositivo se conmuta automáticamente de iDRAC a sistema operativo.

- El dispositivo se expulsa de iDRAC o de su sistema operativo.

Cuando un dispositivo excede los requisitos de alimentación según lo permitido por la especificación USB, el dispositivo se desconecta y se genera un suceso de sobrecarga con las siguientes propiedades:

- Categoría: condición del sistema
- Tipo: dispositivo USB
- Gravedad: advertencia
- Notificaciones permitidas: correo electrónico, captura SNMP, syslog remoto y sucesos WS.
- Acciones: ninguna

Se muestra un mensaje de error y se registra en el registro de Lifecycle Controller en las siguientes situaciones:

- Se intenta configurar el puerto de administración USB sin el privilegio de usuario de control del servidor.
- iDRAC está usando un dispositivo USB y se intenta modificar el modo de puerto de administración USB.
- iDRAC está usando un dispositivo USB y se extrae el dispositivo.

Configuración de puerto de administración USB mediante la interfaz web

Para configurar el puerto USB:

1 En la interfaz web de iDRAC, vaya a **Configuración** > **Configuración del sistema** > **Configuración de hardware** > **Configuración de administración USB** .

2 El **Modo de puerto de administración de USB** está establecido en iDRAC directo solamente.

3 Desde el iDRAC administrado: en el menú desplegable de Configuración XML de USB, seleccione opciones para configurar un servidor mediante la importación de archivos del Perfil de configuración del servidor almacenados en una unidad USB:

- **Desactivado**
- **Activado solamente cuando el servidor contiene configuraciones de credenciales predeterminadas.**
- **Activado**

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

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

Configuración de puerto de administración USB mediante RACADM

Para configurar el puerto de administración USB, utilice los siguientes objetos y subcomandos RACADM:

- Para ver el estado del puerto USB:
  ```
  racadm get iDRAC.USB.ManagementPortStatus
  ```
- Para ver la configuración del puerto USB:
  ```
  racadm get iDRAC.USB.ManagementPortMode
  ```
- Para modificar la configuración del puerto USB:
  ```
  racadm set iDRAC.USB.ManagementPortMode <Automatic|Standard OS Use|iDRAC|>
  ```

  NOTA: Asegúrese de especificar el atributo Uso del sistema operativo estándar dentro de comillas simples mientras se utiliza el comando set de RACADM.
- Para ver el inventario del dispositivo USB:
  ```
  racadm hwinventory
  ```
- Para configurar por medio de la configuración de alertas actual:
  ```
  racadm eventfilters
  ```

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

Configuración del puerto de administración de USB mediante la utilidad de configuración de iDRAC

Para configurar el puerto USB:

1 En la utilidad de configuración de iDRAC, vaya a **Configuración de medios y puertos USB**.

Se mostrará la página **Configuración de iDRAC.Configuración de medios y puertos USB**.

2 En el menú desplegable **Modo de puerto de administración de USB**, haga lo siguiente:

- **Automático**: iDRAC o el sistema operativo del servidor utilizan el puerto USB.
- **Uso estándar del sistema operativo**: el sistema operativo del servidor utiliza el puerto USB.
- **iDRAC directo solamente**: iDRAC utiliza el puerto USB.

3 En el menú desplegable **iDRAC directo: XML de configuración USB**, seleccione opciones para configurar un servidor mediante la importación del perfil de configuración del servidor almacenado en una unidad USB:

- **Desactivado**
- **Activado mientras el servidor contiene configuraciones de credenciales predeterminadas solamente**
- **Activado**

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

4 Haga clic en **Atrás**, después en **Terminar** y, a continuación, en **Sí** para aplicar la configuración.

Importación de un perfil de configuración del servidor desde un dispositivo USB

Asegúrese de crear un directorio en la raíz de un dispositivo USB denominado System_Configuration_XML donde se encuentren los archivos config.xml / config.json y control.xml:

- El perfil de configuración del servidor se encuentra en el subdirectorio System_Configuration_XML bajo el directorio raíz del dispositivo USB. Este archivo contiene todos los pares valor-atributo del servidor. Esto incluye atributos de iDRAC, PERC, RAID y BIOS. Es posible editar este archivo para configurar cualquier atributo en el servidor. El nombre del archivo puede ser <servicetag>-config.xml, <servicetag>-config.json, <modelnumber>-config.xml, <modelnumber>-config.json, config.xml o config.json.
- Archivo XML de control: incluye parámetros para controlar la operación de importación y no contiene atributos de iDRAC ni de ningún otro componente del sistema. El archivo de control contiene tres parámetros:
  - Tipo de apagado: ordenado, forzado, sin reinicio.
  - Tiempo de espera (en segundos): 300 como mínimo y 3600 como máximo.
  - Estado de alimentación del host final: encendido o apagado.

Ejemplo de archivo control.xml:

```
<InstructionTable>       <InstructionRow>                 <InstructionType>Configuration XML
import Host control Instruction</InstructionType>                  <Instruction>ShutdownType</
Instruction>                 <Value>NoReboot</Value>
<ValuePossibilities>Graceful,Forced,NoReboot</ValuePossibilities>       </InstructionRow>
<InstructionRow>                  <InstructionType>Configuration XML import Host control
Instruction</InstructionType>                 <Instruction>TimeToWait</
Instruction>                 <Value>300</Value>                 <ValuePossibilities>Minimum
value is 300 -Maximum value is 3600 seconds.</ValuePossibilities>       </
InstructionRow>       <InstructionRow>                 <InstructionType>Configuration XML
import Host control Instruction</InstructionType>
<Instruction>EndHostPowerState</Instruction>                <Value>On</Value>
<ValuePossibilities>On,Off</ValuePossibilities>      </InstructionRow></InstructionTable>
```

Es necesario contar con el privilegio de control del servidor para realizar esta operación.

NOTA: Al importar el perfil de configuración del servidor, el cambio de los valores de administración de USB en el archivo XML da como resultado un trabajo fallido o completado con errores. Puede comentar los atributos en el XML para evitar los errores.

Para importar el perfil de configuración del servidor desde el dispositivo USB hacia iDRAC:

1 Configure el módulo de administración USB:
   - Establezca **Modo de puerto de administración USB** en **Automático** o **iDRAC**.
   - Establezca el valor de **iDRAC administrado: configuración XML USB** en **Activado con credenciales predeterminadas** o **Activado**.
2 Inserte la memoria USB (que contiene los archivos **configuration.xml** y **control.xml**) en el puerto USB del iDRAC.
3 El perfil de configuración del servidor se descubre en el dispositivo USB en el subdirectorio System_Configuration_XML bajo el directorio raíz del dispositivo USB. Se descubre en la secuencia que se indica a continuación:
   - <servicetag>-config.xml / <servicetag>-config.json
   - <modelnum>-config.xml / <modelnum>-config.json
   - config.xml / config.json
4 Se inicia un trabajo de importación del perfil de configuración del servidor.

   Si el perfil no se descubre, la operación se detiene.

   Si **iDRAC administrado: configuración XML USB** se establece en **Activado con credenciales predeterminadas** y la contraseña de configuración del BIOS no es nula o si una de las cuentas de usuario de iDRAC se ha modificado, se muestra un mensaje de error y la operación se detiene.
5 El panel LCD y el indicador LED (si está presente) muestran el estado que indica que se ha iniciado un trabajo de importación.
6 Si existe una configuración que debe organizarse y **Tipo de apagado** se especifica como **Sin reinicio** en el archivo de control, se debe reiniciar el servidor para que los valores se configuren. De lo contrario, el servidor se reinicia y la configuración se aplica. Solo cuando el servidor ya está apagado, se aplica la configuración organizada en etapas aunque se establezca la opción **Sin reinicio**.
7 Una vez que se completa el trabajo de importación, el panel LCD o LED indica que el trabajo está completo. Si es necesario reiniciar el sistema, el panel LCD muestra el estado del trabajo como “En pausa, a la espera de reinicio”.
8 Si el dispositivo USB queda insertado en el servidor, el resultado de la operación de importación se registra en el archivo **results.xml** en el dispositivo USB.

Mensajes de LCD

Si el panel LCD está disponible, se muestran los siguientes mensajes en una secuencia:

1 Importación: cuando el perfil de configuración del servidor se copia desde el dispositivo USB.
2 Aplicación: cuando el trabajo está en progreso.
3 Completado: cuando el trabajo se ha completado correctamente.
4 Completado con errores: cuando el trabajo se ha completado con errores.
5 Fallido: cuando el trabajo ha fallado.

Para obtener más detalles, consulte el archivo de resultados en el dispositivo USB.

Comportamiento de parpadeo de LED

Si el LED USB está presente, indica lo siguiente:

- Luz verde fija: cuando el perfil de configuración del servidor se copia desde el dispositivo USB.
- Luz verde parpadeante: cuando el trabajo está en progreso.
- Luz verde fija: cuando el trabajo se ha completado correctamente.

Archivo de resultados y registros

Se registra la siguiente información para la operación de importación:

- La importación automática desde USB se registra en el archivo de registro de Lifecycle Controller.
- Si el dispositivo USB queda insertado, los resultados del trabajo se registran en el archivo de resultados que se encuentra en la memoria USB.

Un archivo de resultados denominado **Results.xml** se actualiza o se crea en el subdirectorio con la siguiente información:

- Etiqueta de servicio: los datos se registran después de que la operación de importación ha devuelto un error o una identificación de trabajo.
- ID de trabajo: los datos se registran después de que la operación de importación ha devuelto una identificación de trabajo.
- Fecha de inicio y hora del trabajo: los datos se registran después de que la operación de importación ha devuelto una identificación de trabajo.
- Estado: los datos se registran cuando la operación de importación devuelve un error o cuando los resultados del trabajo están disponibles.

20

Uso de la Sincronización rápida de iDRAC

Con Dell OpenManage Mobile ejecutándose en un dispositivo móvil Android o iOS, se puede acceder fácilmente al servidor de manera directa o a través de la consola de OME. Le permite revisar los detalles del servidor y el inventario, ver los registros de LC y sucesos del sistema, obtener notificaciones automáticas en un dispositivo móvil desde una consola de OME, asignar la dirección IP y modificar la contraseña de iDRAC, configurar los atributos clave del BIOS y tomar medidas correctivas, según sea necesario. También puede aplicar un ciclo de encendido en un servidor, acceder a la consola del sistema o acceder a la GUI de iDRAC.

OMM se puede descargar en forma gratuita desde la Apple App Store o la Google Play Store.

Se debe instalar la aplicación OpenManage Mobile en el dispositivo móvil (compatible con dispositivos móviles Android 5.0+ e iOS 9.0+) para administrar el servidor mediante la interfaz de Sincronización rápida 2 de iDRAC.

NOTA: Esta sección aparece solo en los servidores que cuentan con el módulo Sincronización rápida 2 en la orejeta izquierda del bastidor.

NOTA: Esta función se admite actualmente en dispositivos móviles con los sistemas operativos Android y Apple iOS.

En la versión actual, esta función está disponible en todos los servidores PowerEdge de 14a generación. Se requiere un Panel de control izquierdo de Sincronización rápida 2 (incorporado en la **orejeta izquierda del bastidor**) y dispositivos móviles con Bluetooth de bajo consumo (y, opcionalmente, Wi-Fi) habilitados. Por lo tanto, es una venta incremental de hardware y las funcionalidades no dependen de las licencias de software de iDRAC.

Procedimientos de configuración de la Sincronización rápida 2 de iDRAC:

- - Configuración de acceso a la Sincronización rápida de iDRAC (mediante GUI de iDRAC, iDRAC HII, racadm, WSMan)
  a **>Acceso a la sincronización rápida**: configure a modo de lectura-escritura. Esta es la opción predeterminada.
  b **>Temporizador de inactividad de la sincronización rápida**: configure como activado. Esta es la opción predeterminada.
  c **>Tiempo de espera de inactividad de la Sincronización rápida**: indica la hora después de la cual se desactiva el modo de Sincronización rápida 2. De forma predeterminada, se seleccionan segundos. El valor predeterminado es 120 segundos. El rango válido es de 120 a 3600 segundos.
  d **>Autenticación de lectura de sincronización rápida**: se configura como activada. Esta es la opción predeterminada.
  e **WiFi de sincronización rápida**: se configura como activado. Esta es la opción predeterminada.

Una vez configurado, active el botón de Sincronización rápida 2 en el panel de control izquierdo. Asegúrese de que se encienda la luz de Sincronización rápida 2. Acceda a la información de Sincronización rápida 2 a través de un dispositivo móvil (Android 5.0+ o IOS 9.0+, OMM 2.0 o superior).

Con OpenManage Assistant, es posible:

- Ver información de inventario
- Ver información de monitoreo
- Configurar los valores de red básicos de iDRAC

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

Temas:

Configuración de la sincronización rápida 2 de iDRAC

Con la interfaz web de iDRAC, RACADM, WSMan y iDRAC HII, se puede configurar la función de sincronización rápida 2 de iDRAC para permitir el acceso al dispositivo móvil:

- **Acceso a la sincronización rápida**: configure a modo de lectura-escritura. Esta es la opción predeterminada.
- **Temporizador de inactividad de la sincronización rápida**: configure a modo de lectura-escritura. Esta es la opción predeterminada.
- **Tiempo de espera de inactividad de la sincronización rápida**: indica la hora después de la cual se desactiva el modo de Quick Sync 2. De forma predeterminada, se seleccionan segundos. El valor predeterminado es 120 segundos. El rango válido es de 120 a 3600 segundos.
  a Si se activa, permite especificar una hora después de la cual el modo de sincronización rápida 2 se apaga. Para activarlo, pulse el botón de activación de nuevo.
  b Si está desactivado, el temporizador no le permite introducir un período de tiempo de espera.
- **Autenticación de lectura de sincronización rápida**: se configura como habilitada. Esta es la opción predeterminada.
- **WiFi de sincronización rápida**: se configura como habilitado. Esta es la opción predeterminada.

Es necesario contar con el privilegio de control del servidor para configurar los valores. No se requiere el reinicio del servidor para que la configuración surta efecto. Una vez configurado, puede activar el botón de sincronización rápida 2 en el panel de control izquierdo. Asegúrese de que la luz de sincronización rápida se encienda. Posteriormente, acceda a la información de sincronización rápida a través de un dispositivo móvil.

Se registra una entrada en el registro de Lifecycle Controller cuando se modifica la configuración.

Configuración de los ajustes de Quick Sync 2 de iDRAC mediante la interfaz web

Para configurar Quick Sync 2 de iDRAC:

1 En la interfaz web de iDRAC, vaya a **Configuration (Configuración)** > **System Settings (Configuración del sistema)** > **Hardware Settings (Configuración de hardware)** > **iDRAC Quick Sync (Quick Sync de iDRAC)**.
2 En la sección **iDRAC Quick Sync (Quick Sync de iDRAC)**, en el menú desplegable **Access (Acceso)**, seleccione una de las opciones siguientes para proporcionar acceso al dispositivo móvil Android o iOS:
   - Lectura/escritura
   - Solo lectura
   - Desactivado
3 Active el temporizador.
4 Especifique el valor del límite de tiempo de espera.
   Para obtener más información acerca de los campos, consulte la *Ayuda en línea de iDRAC*.
5 Haga clic en **Aplicar** para aplicar la configuración.

Configuración de los valores de sincronización rápida 2 de iDRAC mediante RACADM

Para configurar la función 2 de la sincronización rápida de iDRAC, utilice los objetos racadm en el grupo **System.QuickSync.** Para obtener más información, consulte *iDRAC RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de iDRAC)* disponible en **dell.com/esmmanuals**.

Configuración de los valores de sincronización rápida 2 del iDRAC mediante la utilidad de configuración de iDRAC

Para configurar la sincronización rápida 2 del iDRAC:

1 En la GUI del iDRAC, vaya a **Configuración** > **Configuración del sistema** > **Configuración de hardware** > **Sincronización rápida del iDRAC**.

2 En la sección **Sincronización rápida del iDRAC**:

- Especifique el nivel de acceso.
- Active el tiempo de espera.
- Especifique el límite de tiempo de espera definido por el usuario (el rango va de 15 a 3600 segundos).

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

3 Haga clic en **Atrás**, en **Terminar** y, a continuación, en **Sí**.

Se aplica la configuración.

Uso de dispositivos móviles para ver información de iDRAC

Para ver la información de iDRAC desde el dispositivo móvil, consulte *OpenManage Mobile User's Guide* (Guía del usuario de OpenManage Mobile) disponible en **dell.com/support/manuals** para consultar los pasos.

21

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
- Instalara aplicaciones
- Actualizar controladores
- Instalar un sistema operativo en el sistema administrado

Esta es una función con licencia para los servidores tipo bastidor y torre. 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 incluye una imagen de disco flexible o una unidad de disco flexible disponible. Entre las unidades ópticas compatibles se incluye un máximo de una unidad óptica disponible o un archivo de imagen ISO.

  En la figura siguiente se muestra una configuración típica de medios virtuales.
- No puede accederse a los medios de disco flexible virtuales de iDRAC desde máquinas virtuales.
- Todo medio virtual emula un dispositivo físico del sistema administrado.
- En sistemas administrados basados en Windows, las unidades de medios virtuales se montan automáticamente si están conectados y configurados con una letra de unidad.
- Con algunas configuraciones, en los sistemas administrados basados en Linux, las unidades de medios virtuales no se montan automáticamente. Para montarlas manualmente, utilice el comando de montaje.
- 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.

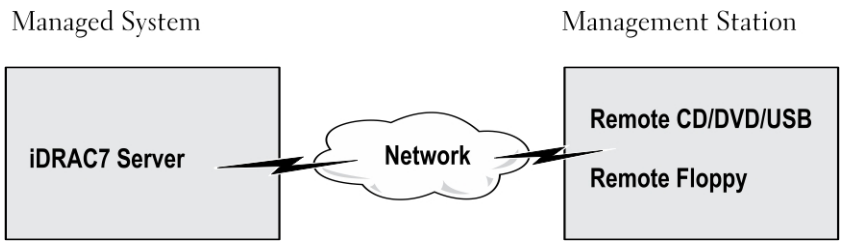


Ilustración 4. Configuración de medios virtuales

Temas:

Unidades y dispositivos compatibles

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

Tabla 38. Unidades y dispositivos compatibles

Unidad	Medios de almacenamiento compatibles
Unidades ópticas virtuales	• 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	• Archivo de imagen de CD-ROM/DVD en el formato ISO9660 • Archivo de imagen de disco flexible en el formato ISO9660
Unidades Flash USB	• 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.

Configuración de medios virtuales mediante la interfaz web de iDRAC

Para configurar los valores de medios virtuales:

PRECAUCIÓN: No restablezca iDRAC mientras ejecuta una sesión de medios virtuales. De lo contrario, es posible que se produzcan resultados no deseados, incluida la pérdida de datos.

1 En la interfaz web de iDRAC, vaya a **Configuración** > **Medios virtuales** > **Medios conectados**.
2 Especifique la configuración obligatoria. Para obtener más información, consulte la *Ayuda en línea de iDRAC*.
3 Haga clic en **Aplicar** para guardar la configuración.

Configuración de medios virtuales mediante RACADM

Para configurar los medios virtuales, utilice el comando **set** con los objetos en el grupo **iDRAC.VirtualMedia**.

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

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 hacerlo:

1 En la utilidad de configuración de iDRAC, vaya a **Configuración de medios y puertos USB**.
Se mostrará la página **Configuración de iDRAC.Configuración de medios y puertos USB**.
2 En la sección **Medios virtuales**, seleccione **Desconectar**, **Conectar**, o **Conectar automáticamente** en función de los requisitos. Para obtener más información acerca de las opciones, consulte la *Ayuda en línea de la utilidad de configuración de iDRAC*.
3 Haga clic en **Atrás**, en **Terminar** y, a continuación, en **Sí**.
Se configuran los valores de los medios virtuales.

Estado de medios conectados y respuesta del sistema

En la tabla siguiente se describe la respuesta del sistema en función de la configuración de medios conectados.

Tabla 39. Estado de medios conectados y respuesta del sistema

Estado de los medios conectados	Respuesta del sistema
Desconectar	No se puede asignar una imagen al sistema.
Conectar	Los medios se asignan, incluso cuando se cierre la **Vista de cliente**.
Conexión automática	Los medios se asignan cuando se abre la **Vista de cliente** y su asignación se anula cuando se cierra la **Vista de cliente**.

Configuración del servidor para ver los dispositivos virtuales en los medios virtuales

Debe configurar los siguientes valores en la estación de administración para permitir la visibilidad de las unidades vacías. Para ello, en Windows Explorer, desde el menú **Organizar**, haga clic en **Opciones de carpeta y búsqueda**. En la pestaña **Ver**, deseleccione la opción **Ocultar unidades vacías en la carpeta Equipo** y haga clic en **Aceptar**.

Acceso a medios virtuales

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

Los medios virtuales y RFS son mutuamente exclusivos. Si la conexión del RFS está activa e intenta iniciar el cliente de Medios virtuales, se muestra el siguiente mensaje de error: *Los medios virtuales no están disponibles actualmente. Hay una sesión de medios virtuales o recurso compartido de archivos remoto en uso.*

Si la conexión del RFS no está activa e intenta iniciar el cliente de medios virtuales, el cliente se inicia satisfactoriamente. Luego puede usar el cliente de medios virtuales para asignar dispositivos y archivos a las unidades virtuales de medios virtuales.

Inicio de medios virtuales mediante la consola virtual

Antes de iniciar medios virtuales a través de la consola virtual, asegúrese de lo siguiente:

- La consola virtual está activada.
- El sistema está configurado para no ocultar unidades vacías: En el Explorador de Windows, vaya a **Opciones de carpeta**, borre la opción **Ocultar unidades vacías en la carpeta Equipo** y haga clic en **Aceptar**.

Para acceder a los medios virtuales mediante la consola virtual:

1 En la interfaz web de iDRAC, vaya a **Configuración** > **Consola virtual**.
Aparece la página **Consola virtual**.
2 Haga clic en **Iniciar consola virtual**.
Se inicia el **Visor de la consola virtual**.

NOTA: En Linux, Java es el tipo de complemento predeterminado para acceder a la consola virtual. En Windows, abra el archivo .jnlp para iniciar la consola virtual mediante Java.

3 Haga clic en **Medios virtuales** > **Conectar medios virtuales**.
La sesión de medios virtuales se establece y el menú **Medios virtuales** muestra la lista de dispositivos disponibles para la asignación.

NOTA: La aplicación de la ventana Visor de consola virtual debe permanecer activa mientras accede a los medios virtuales.

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 el Explorador de Windows, vaya a **Opciones de carpeta**, desactive la opción **Ocultar las unidades vacías en la carpeta Mi PC** y haga clic en **Aceptar**.

Para iniciar los medios virtuales cuando la consola virtual está desactivada:

1 En la interfaz web de iDRAC, vaya a **Configuration (Configuración)** > **Virtual Console (Consola virtual)**.
2 Haga clic en **Launch Virtual Console (Iniciar consola virtual)**.
Aparece el siguiente mensaje:

```
Virtual Console has been disabled. Do you want to continue using Virtual Media redirection?
```

3 Haga clic en **OK** (Aceptar).
Aparece la ventana **Medios virtuales**.
4 Desde el menú **Medios virtuales**, haga clic en **Asignar CD/DVD** o **Asignar disco extraíble**.
Para obtener más información, consulte Asignación de unidad virtual.

NOTA: Las letras de unidad de los dispositivos virtuales en el sistema administrado no coinciden con las letras de unidades físicas en la estación de administración.

NOTA: Es posible que los medios virtuales no funcionen correctamente en clientes de sistema operativo 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.

NOTA: El complemento HTML5 no se admite en los medios virtuales independientes.

Adición de imágenes de medios virtuales

Puede crear una imagen de medios de la carpeta remota y montarla como un dispositivo USB conectado al sistema operativo del servidor. Para agregar las imágenes de medios virtuales:

1 Haga clic en **Medios virtuales** > **Crear imagen...**.

2 En el campo **Carpeta de origen**, haga clic en **Examinar** y vaya a la carpeta o al directorio que se utilizará como origen para el archivo de imagen. El archivo de imagen se encuentra en la estación de administración o en la unidad C: del sistema administrado.

3 En el campo **Nombre de archivo de imagen** aparecerá la ruta de acceso predeterminada para almacenar los archivos de imagen creados (por lo general, el directorio del escritorio). Para cambiar esta ubicación, haga clic en **Examinar** y especifique una ubicación.

4 Haga clic en **Crear imagen**.

Se inicia el proceso de creación de la imagen. Si la ubicación del archivo de imagen está dentro de la carpeta de origen, aparecerá un mensaje de advertencia para indicar que la creación de la imagen no puede continuar porque la ubicación del archivo de imagen dentro de la carpeta de origen provocará un lazo infinito. Si la ubicación del archivo de imagen no está dentro de la carpeta de origen, la creación de la imagen continúa.

Cuando se cree la imagen, aparecerá un mensaje para indicarlo.

5 Haga clic en **Finalizar**.

Se crea la imagen.

Cuando una carpeta se agrega como imagen, se crea un archivo **.img** en el escritorio de la estación de administración desde la que se utiliza esta función. Si se mueve o elimina este archivo **.img**, la anotación correspondiente para esta carpeta en el menú **Medios virtuales** no funciona. Por tanto, es recomendable no mover ni eliminar el archivo **.img** mientras se usa la *imagen*. No obstante, el archivo **.img** se puede eliminar después de que se deselecciona la entrada pertinente y esta se quita mediante la opción **Quitar imagen** para quitar la anotación.

Visualización de los detalles del dispositivo virtual

Para ver los detalles del dispositivo virtual, en el visor de la consola virtual, haga clic en **Herramientas** > **Estadísticas**. En la ventana **Estadísticas**, la sección **Medios virtuales** muestra los dispositivos virtuales asignados y la actividad de lectura/escritura de cada dispositivo. Si los medios virtuales están conectados, se visualiza esta información. Si los medios virtuales no están conectados, aparece el mensaje "Medios virtuales no conectados".

Si los medios virtuales se inician sin utilizar la consola virtual, la sección **Medios virtuales** aparece como un cuadro de diálogo. Proporciona información acerca de los dispositivos asignados.

Restablecimiento de USB

Para restablecer el dispositivo USB:

1 En el visor de la consola virtual, haga clic en **Herramientas** > **Estadísticas**.

Aparece la ventana **Estadísticas**.

2 En **Medios virtuales**, haga clic en **Restablecimiento de USB**.

Aparece un mensaje que indica al usuario que el restablecimiento de la conexión USB puede afectar a todas las entradas del dispositivo de entrada, incluidos los medios virtuales, el teclado y el mouse.

3 Haga clic en **Yes (Sí)**.

Se restablece el USB.

NOTA: Los medios virtuales de iDRAC no finalizan ni siquiera después de cerrar la sesión de la interfaz web de iDRAC.

Asignación de la unidad virtual

Para asignar la unidad virtual:

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

1 Para establecer una sesión de medios virtuales, en el menú **Medios virtuales** haga clic en **Conectar medios virtuales**.

Por cada dispositivo disponible para asignar desde el servidor host, aparecerá un elemento en el menú **Medios virtuales**. El elemento de menú recibe un nombre acorde al tipo de dispositivo, por ejemplo:

- Asignar CD/DVD
- Asignar disco extraíble
- Asignar disquete

NOTA: Aparece el elemento de menú Asignar disco flexible en la lista si la opción Emulación de disco flexible está activada en la página Medios conectados. Cuando se activa Emulación de disco flexible, Asignar disco extraíble se reemplaza con Asignar disco flexible.

La opción **Asignar DVD/CD** se puede usar para archivos ISO y la opción de **Asignar disco extraíble** puede utilizarse para imágenes.

NOTA: No puede asignar medios físicos, como por ejemplo las unidades USB, CD o DVD mediante la consola virtual basada en HTML5.

NOTA: No puede asignar las memorias USB como discos de medios virtuales mediante la consola virtual o los medios virtuales a través de una sesión RDP.

2 Haga clic en el tipo de dispositivo que desea asignar.

NOTA: Se muestra la sesión activa si hay una sesión de medios virtuales activa actualmente desde la sesión de la interfaz web actual, desde otra sesión de interfaz web o desde VMCLI.

3 En el campo **Unidad/archivo de imagen**, seleccione el dispositivo de la lista desplegable.

La lista contiene todos los dispositivos disponibles (no asignados) que puede asignar (CD/DVD, disco extraíble, disco flexible) y los tipos de archivo de imagen que puede asignar (ISO o IMG). Los archivos de imagen están ubicados en el directorio predeterminado de archivos de imagen (por lo general, el escritorio del usuario). Si el dispositivo no está disponible en la lista desplegable, haga clic en **Explorar** para especificar el dispositivo.

El tipo de archivo correcto para CD/DVD es ISO y para disco extraíble y disco flexible es IMG.

Si la imagen se crea en la ruta de acceso predeterminada (Escritorio), cuando seleccione **Asignar disco extraíble**, la imagen creada estará disponible para la selección en el menú desplegable.

Si crea la imagen en una ubicación diferente, cuando seleccione **Asignar disco extraíble**, la imagen creada no estará disponible para la selección en el menú desplegable. Haga clic en **Examinar** para especificar la imagen.

4 Seleccione **Solo lectura** para asignar dispositivos aptos para escritura como de solo lectura.

Para los dispositivos de CD/DVD, esta opción está activada de manera predeterminada y no puede desactivarla.

NOTA: Los archivos ISO e IMG se asignan como archivos de solo lectura si los asigna mediante la consola virtual de HTML5.

5 Haga clic en **Asignar dispositivo** para asignar el dispositivo al servidor host.

Después de asignar el dispositivo/archivp, el nombre de su elemento de menú de **Medios virtuales** cambia para indicar el nombre del dispositivo. Por ejemplo, si el dispositivo de CD/DVD se asigna a un archivo de imagen llamado **foo.iso**, el elemento de menú de CD/DVD del menú de Medios virtuales se denomina **foo.iso asignado a CD/DVD**. La marca de verificación en dicho menú indica que está asignado.

Visualización de las unidades virtuales correctas para la asignación

En una estación de administración basada en Linux, la ventana de **Cliente** de los medios virtuales puede mostrar discos extraíbles y discos flexibles que no forman parte de la estación de administración. Para asegurarse de que las unidades virtuales correctas están disponibles para su asignación, debe activar la configuración de puertos para el disco duro SATA conectado. Para hacerlo:

1 Reinicie el sistema operativo de la estación de administración. Durante la POST, presione <F2> para acceder a la **Configuración del sistema**.
2 Vaya a la **Configuración de SATA**. Aparecerán los detalles del puerto.
3 Active los puertos que están presentes en el disco duro y conectados a él.
4 Acceda a la ventana de **Cliente** de los medios virtuales. Se mostrarán las unidades correctas que se pueden asignar.

Anulación de la asignación de la unidad virtual

Para anular la asignación de la unidad virtual:

1 Desde el menú **Medios virtuales** realice cualquiera de las siguientes acciones:
   - Haga clic en el dispositivo que desea desasignar.
   - Haga clic en **Desconectar medios virtuales**.

   Aparecerá un mensaje solicitando confirmación.
2 Haga clic en **Yes (Sí)**.
   La marca de verificación para ese elemento de menú desaparecerá para indicar que no está asignado al servidor host.

   NOTA: Después de desasignar un dispositivo USB conectado a vKVM desde un sistema cliente que ejecuta el sistema operativo de Macintosh, es posible que el dispositivo no asignado no esté disponible en el cliente. Reinicie el sistema o monte manualmente el dispositivo en el sistema cliente para ver ese dispositivo.

NOTA: Para desasignar una unidad de DVD virtual en un sistema operativo Linux, desmonte la unidad y expúlsela.

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 iniciarse desde un dispositivo de inicio según el orden de inicio establecido. Si el dispositivo virtual está conectado y se cuenta con un medio de inicio, el sistema se inicia con el dispositivo virtual. De lo contrario, el sistema omitirá el dispositivo, de manera similar a un dispositivo físico sin medios de inicio.

Activación del inicio único para medios virtuales

Puede cambiar el orden de inicio solamente después de conectar un dispositivo de medios virtuales remoto.

Antes de activar la opción de inicio único, asegúrese de lo siguiente:

- Dispone del privilegio *Configurar usuario*.
- Asigne las unidades locales o virtuales (CD/DVD, disco flexible o dispositivo Flash USB) con los medios o la imagen de inicio mediante las opciones de medios virtuales
- Los medios virtuales deben estar en el estado *Conectado* para que las unidades virtuales aparezcan en la secuencia de inicio.

Para activar la opción de inicio único e iniciar el sistema administrado desde los medios virtuales:

1 En la interfaz web de iDRAC, vaya a **Información general** > **Servidor** > **Medios conectados**.
2 En **Medios virtuales**, seleccione la opción **Activar el inicio una vez** y haga clic en **Aplicar**.
3 Encienda el sistema administrado y presione **<F2>** durante el inicio.
4 Cambie la secuencia de inicio para iniciar desde el dispositivo de medios virtuales remoto.
5 Reinicie el servidor.

El sistema administrado se inicia una vez desde los medios virtuales.

22

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 de la estación de administración a iDRAC en el sistema administrado. Al usar esta utilidad, puede acceder a 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.

La utilidad VMCLI proporciona las siguientes funciones:

- Administración de dispositivos extraíbles o imágenes accesibles a través de medios virtuales.
- Finalización automática de la sesión cuando se activa la opción **Iniciar una vez** en el firmware de iDRAC.
- Comunicaciones seguras con iDRAC mediante la capa de sockets seguros (SSL).
- Ejecute comandos VMCLI hasta que:
  - se terminen automáticamente las conexiones.
  - un sistema operativo termine el proceso.

    NOTA: Para terminar el proceso en Windows, utilice el Administrador de tareas.

Temas:

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. Después de una instalación correcta, verifique la carpeta **install\Dell\SysMgt\rac5** para asegurarse de que existe **vmcli.exe**. De manera similar, compruebe la respectiva ruta 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 los sistemas Linux, para acceder al iDRAC, 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 de VMCLI. No obstante, para agregar o editar usuarios en el grupo de administradores de VMCLI, utilice el comando `visudo`.

Sintaxis de VMCLI

La interfaz VMCLI es idéntica en los sistemas Windows y Linux. La sintaxis de VMCLI es:

```
VMCLI [parameter] [operating_system_shell_options]
```

Por ejemplo: `vmcli -r iDRAC-IP-address:iDRAC-SSL-port`

Con el valor *parameter*, la interfaz VMCLI puede conectarse al servidor especificado, acceder a iDRAC y asignarse a los medios virtuales especificados.

NOTA: La sintaxis de VMCLI distingue entre mayúsculas y minúsculas.

Para garantizar la seguridad, es recomendable utilizar los siguientes parámetros de VMCLI:

- `vmcli -i` : permite un método interactivo para iniciar VMCLI. Garantiza que el nombre de usuario y la contraseña no estén visibles cuando otros usuarios examinan los procesos.
- vmcli `-r <iDRAC-IP-address[:iDRAC-SSL-port]> -S -u <iDRAC-user-name> -p <iDRAC-user-password> -c {<device-name> | <image-file>}` — Indica si el certificado de CA de iDRAC es válido. Si el certificado no es válido, se muestra un mensaje de advertencia cuando ejecuta este comando. Sin embargo, el comando se ejecuta correctamente y se establece una sesión VMCLI. Para obtener más información sobre los parámetros de VMCLI, consulte la *Ayuda de VMCLI* o las *páginas Man 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 40. Comandos VMCLI

Soportes virtuales	Comando
Unidad de disco flexible	`vmcli -r [RAC IP or hostname] -u [iDRAC user name] -p [iDRAC user password] -f [device name]`
Disco flexible o imagen de memoria de USB de inicio	`vmcli -r [iDRAC IP address] [iDRAC user name] -p [iDRAC password] -f [floppy.img]`
Unidad CD mediante la opción -f	`vmcli -r [iDRAC IP address] -u [iDRAC user name] -p [iDRAC password] -f [device name]|[image file]-f [cdrom - dev ]`
Imagen CD/DVD de inicio	`vmcli -r [iDRAC IP address] -u [iDRAC user name] -p [iDRAC password] -c [DVD.img]`

Si el archivo no está protegido contra escritura, es posible que los medios virtuales escriban en el archivo de imagen. Para evitar que los medios virtuales no escriban en los medios, 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: redirige 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 desde 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 comando del sistema operativo para que la utilidad se ejecute en segundo plano.

  Por ejemplo, en un sistema operativo Linux, el caracter "et" (&) después del comando hace que el programa se genere como un nuevo proceso de segundo plano. Esta técnica es útil en programas de secuencia de comandos, ya que permite a la secuencia de comandos continuar después de que se inicia un nuevo proceso para el comando VMCLI (de lo contrario, la secuencia de comandos se bloquea hasta que se finalice el programa VMCLI).

  Cuando se inicial varias sesiones de VMCLI, utilice las prestaciones específicas del sistema operativo para enumerar y terminar los procesos.

23

Administración de la tarjeta vFlash SD

La tarjeta vFlash SD es una tarjeta digital segura (SD) que puede solicitar e instalar desde la fábrica. 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. vFLash es una función que requiere licencia.

NOTA: No existe ninguna limitación de tamaño de la tarjeta SD, puede abrir y reemplazar la tarjeta SD instalada de fábrica por una tarjeta SD de mayor capacidad. Debido a que vFlash utiliza el sistema de archivos FAT32, el tamaño del archivo está limitado a 4 GB.

Si la tarjeta no está disponible en la ranura de tarjeta vFlash SD del sistema, aparecerá el siguiente mensaje de error en la interfaz web de iDRAC, en **Información general** > **Servidor** > **vFlash**:

```
SD card not detected. Please insert an SD card of size 256MB or greater.
```

NOTA: Asegúrese de insertar únicamente una tarjeta SD compatible con vFlash en la ranura de la tarjeta vFlash de iDRAC. Si inserta una tarjeta SD no compatible, aparecerá el siguiente mensaje de error al inicializar la tarjeta: *Se ha producido un error al inicializar la tarjeta SD.*

Las características claves son las siguientes:

- Proporciona espacio de almacenamiento y emula dispositivos USB.
- Se pueden crear hasta 16 particiones. Cuando se conectan, estas particiones se exponen al sistema como una unidad de disco flexible, una unidad de disco duro o una unidad de CD/DVD que depende del modo de emulación seleccionado.
- Se pueden crear particiones desde tipos de sistemas 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.

NOTA: Si está activado el modo FIPS, no es posible realizar acciones vFlash.

Temas:

Configuración de la tarjeta SD vFlash

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 de propietario* de *hardware* del sistema en **dell.com/support/manuals**.

NOTA: Es necesario tener privilegios de acceso a los medios virtuales para activar o desactivar la funcionalidad vFlash y para inicializar la tarjeta.

Visualización de las propiedades de la tarjeta vFlash SD

Una vez activada la función vFlash, se pueden ver las propiedades de la tarjeta SD mediante la interfaz web de iDRAC o RACADM.

Visualización de las propiedades de la tarjeta vFlash SD mediante la interfaz web

Para ver las propiedades de la tarjeta vFlash SD, en la interfaz web de iDRAC, vaya a **Configuración** > **Configuración del sistema** > **Configuración de hardware** > **vFlash**. Aparece la página Propiedades de la tarjeta. Para obtener información acerca de las propiedades que se muestran, consulte la *Ayuda en línea de iDRAC*.

Visualización de las propiedades de la tarjeta vFlash SD mediante RACADM

Para ver las propiedades de la tarjeta vFlash SD mediante RACADM, utilice el comando `get` con los siguientes objetos:

- iDRAC.vflashsd.AvailableSize
- iDRAC.vflashsd.Health
- iDRAC.vflashsd.Licensed
- iDRAC.vflashsd.Size
- iDRAC.vflashsd.WriteProtect

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

Visualización de las propiedades de la tarjeta vFlash SD mediante la utilidad de configuración de iDRAC

Para ver las propiedades de la tarjeta vFlash SD en la **utilidad de configuración de iDRAC**, vaya a **Configuración de medios y puertos USB**. En la página **Configuración de medios y puertos USB** se muestran las propiedades. Para obtener información acerca de las propiedades exhibidas, consulte la *Ayuda en línea de la utilidad de configuración de iDRAC*.

Activación o desactivación de la funcionalidad vFlash

Debe activar la funcionalidad vFlash para realizar la administración de particiones.

Activación o desactivación de la funcionalidad vFlash mediante la interfaz web

Para activar o desactivar la funcionalidad vFlash:

1. En la interfaz web de iDRAC, vaya a **Configuración** > **Configuración del sistema** > **Configuración de hardware** > **vFlash**.
   Aparece la página **Propiedades de la tarjeta SD**.
2. Seleccione o anule la opción de **vFlash activado** para activar o desactivar la funcionalidad vFlash. Si una partición vFlash está conectada, no podrá desactivar vFlash y aparecerá 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:

```
racadm set iDRAC.vflashsd.Enable [n]
```

n=0	Desactivado
n=1	Activado

NOTA: El comando RACADM sólo funcionará si se cuenta con una tarjeta vFlash SD. Si no se cuenta con una tarjeta, se muestra el siguiente mensaje: *ERROR: Tarjeta SD ausente*.

Activación o desactivación de la funcionalidad vFlash mediante la utilidad de configuración de iDRAC

Para activar o desactivar la funcionalidad vFlash:

1. En la utilidad de configuración de iDRAC, vaya a **Configuración de medios y puertos USB**.
   La **Configuración de iDRAC.** Se mostrará la página **Configuración de medios y puertos USB**.
2. En la sección **Medios vFlash** , seleccione **Activado** para activar la funcionalidad vFlash o **Desactivado** para desactivarla.
3. Haga clic en **Atrás**, en **Terminar** y, a continuación, en **Sí**.
   La funcionalidad vFlash se activa o desactiva según la opción seleccionada.

Inicialización de la tarjeta vFlash SD

La operación de inicialización reformatea la tarjeta SD y configura la información inicial vFlash en la tarjeta.

NOTA: Si la tarjeta SD está protegida contra escritura, la opción Inicializar estará desactivada.

Inicialización de la tarjeta vFlash SD mediante la interfaz web

Para iniciar la tarjeta vFlash SD:

1. En la interfaz web de iDRAC, vaya a **Configuración** > **Configuración del sistema** > **Configuración de hardware** > **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:

```
racadm set iDRAC.vflashsd.Initialized 1
```

Se eliminan todas las particiones existentes y la tarjeta se reformatea.

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

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 **Configuración de medios y puertos USB**.

La **Configuración de iDRAC.** Se muestra la página **Configuración de medios y puertos USB**.

2 Haga clic en **Inicializar vFlash**.

3 Haga clic en **Yes (Sí)**. Se inicia la operación de inicialización.

4 Haga clic en **Atrás** y vaya a la misma **Configuración de iDRAC .** Página **Configuración de medios y puertos USB** 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 Ingrese 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 específica, utilice el comando: `racadm vflashpartition status -i (index)`

NOTA: Si se reinicia iDRAC, se perderá el estado de la última operación de partición.

Administración de las particiones vFlash

Puede realizar lo siguiente mediante la interfaz web de iDRAC o RACADM:

NOTA: Un administrador puede realizar todas las operaciones en las particiones vFlash. De lo contrario, debe disponer del privilegio Acceder a los medios virtuales para crear, eliminar, formatear, conectar, desconectar o copiar el contenido para la partición.

- Creación de una partición vacía
- Creación de una partición mediante un archivo de imagen
- Formateo de una partición
- Visualización de las particiones disponibles
- Modificación de una partición
- Conexión o desconexión de particiones
- Eliminación de las particiones existentes
- Descarga del contenido de una partición
- Inicio de una partición

NOTA: Si hace clic en cualquier opción de las páginas vFlash cuando una aplicación utiliza vFlash, tal como WSMan, la utilidad de configuración de iDRAC o RACADM, o si desea desplazarse a otra página de la GUI, es posible que iDRAC muestre el siguiente mensaje: `vFlash is currently in use by another process. Try again after some time`

VFlash es capaz de crear particiones en forma rápida cuando no hay otras operaciones vFlash en curso, como ser, formateo, conexión de particiones, etc. Por lo tanto, se recomienda primero crear todas 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. Es posible crear particiones del tipo *Disco flexible* o *Disco duro*. La partición tipo CD solo se admite cuando se crean particiones mediante imágenes.

Antes de crear una partición vacía, asegúrese de lo siguiente:

- Dispone de privilegios **Acceder a los medios virtuales**.
- La tarjeta está inicializada.
- La tarjeta no está protegida contra escritura.
- No se está realizando una operación de inicialización en la tarjeta.

Creación de una partición vacía mediante la interfaz web

Para crear una partición vFlash vacía:

1 En la interfaz web de iDRAC, vaya a **Configuration (Configuración)** > **System Settings (Configuración del sistema)** > **Hardware Settings (Configuración de hardware)** > **vFlash** > **Create Empty Partition (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 estas opciones, consulte la *Ayuda en línea de iDRAC*.

Se crea una nueva partición vacía sin formato que es de solo lectura de manera predeterminada. Aparece una página que indica el porcentaje de progreso. Aparece un mensaje de error si:

- La tarjeta está protegida contra escritura.
- El nombre de la etiqueta coincide con la etiqueta de una partición existente.
- Se 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:

1 Inicie sesión en el sistema por medio de telnet, SSH o una consola en serie.

2 Ingrese el comando:

```
racadm vflashpartition create -i 1 -o drive1 -t empty -e HDD -f fat16 -s [n]
```

donde `[n]` es el tamaño de la partición.

De manera predeterminada, se crea una partición vacía con derechos de lectura y escritura.

Creación de una partición mediante un archivo de imagen

Puede crear una partición nueva en la tarjeta vFlash SD mediante un archivo de imagen (disponible en el formato **.img** o **.iso**). Las particiones son de tipos de emulación: disco flexible (**.img**), disco duro (**.img**) o CD (**.iso**). El tamaño de la partición creada es igual al tamaño del archivo de imagen.

Antes de crear una partición a partir de un archivo de 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.
- El tipo de imagen y el tipo de emulación coinciden.

  NOTA: El tipo de imagen cargada y el tipo de emulación deben coincidir. Surgen problemas cuando iDRAC emula un dispositivo con un tipo de imagen incorrecto. Por ejemplo, si la partición se crea mediante una imagen ISO y el tipo de emulación se especifica como Disco duro, el BIOS no puede arrancar 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 que, o equivalente a, 4 GB. El tamaño máximo admitido de la partición es 4 GB. No obstante, cuando se crea una partición mediante un explorador web, el tamaño del archivo de imagen debe ser menor que 2 GB.

NOTA: La partición de vFlash es un archivo de imagen que se encuentra en un sistema de archivos FAT32. Por lo tanto, el archivo de imagen tiene la limitación de 4 GB.

Creación de una partición mediante un archivo de imagen mediante la interfaz web

Para crear una partición vFlash mediante un archivo de imagen:

1 En la interfaz web de iDRAC, vaya a **Configuración** > **Configuración del sistema** > **Configuración de hardware** > **vFlash** > **Crear desde la 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 estas opciones, consulte la *Ayuda en línea de iDRAC*.

Se crea una nueva partición. Para el tipo de emulación de CD, se crea una partición de solo lectura. Para el tipo de emulación de disco flexible o disco duro, se crea una partición de lectura/escritura. Aparece un mensaje de error si:

- La tarjeta está protegida contra escritura.
- El nombre de la etiqueta coincide con la etiqueta de una partición existente.
- El tamaño del archivo de imagen es mayor de 4 GB o excede el espacio disponible en la tarjeta.
- El archivo de imagen no existe o la extensión del archivo de imagen no es .img ni .iso.
- Ya se está realizando una operación de inicialización en la tarjeta.

Creación de una partición desde un archivo de imagen mediante RACADM

Para crear una partición a partir de un archivo de imagen mediante RACADM:

1 Inicie sesión en el sistema por medio de telnet, SSH o una consola en serie.

2 Ingrese el comando

```
racadm vflashpartition create -i 1 -o drive1 -e HDD -t image -l //myserver/sharedfolder/
foo.iso -u root -p mypassword
```

De manera predeterminada, la partición creada es de sólo lectura. Este comando distingue entre mayúsculas y minúsculas en la extensión del nombre del archivo de la imagen. Si la extensión del nombre del archivo está en mayúsculas, por ejemplo FOO.ISO en vez de FOO.iso, el comando informa 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 de sistema de archivos. Los tipos de sistema de archivos compatibles son EXT2, EXT3, FAT16 y FAT32. Solo puede formatear particiones del tipo Disco duro o Disco flexible, no del tipo CD. No es posible formatear particiones de solo lectura.

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.

Para formatear la partición vFlash:

1 En la interfaz web de iDRAC, vaya a **Configuración** > **Configuración del sistema** > **Configuración de hardware** > **vFlash** > **Formato**.
Aparece la página **Formatear partición**.

2 Introduzca la información necesaria y haga clic en **Aplicar**.
Para obtener más información acerca de estas opciones, consulte la *Ayuda en línea de iDRAC*.

Aparece un mensaje de advertencia que indica que todos los datos de la partición se borrarán.

3 Haga clic en **OK** (Aceptar).
La partición seleccionada se formatea en el tipo de sistema de archivos especificado. Aparece un mensaje de error si:
- La tarjeta está protegida contra escritura.
- Ya se está realizando una operación de inicialización en la tarjeta.

Visualización de las particiones disponibles

Asegúrese de que la función vFlash esté activada para ver la lista de particiones disponibles.

Visualización de las particiones disponibles mediante la interfaz web

Para ver las particiones vFlash disponibles, en la interfaz web de iDRAC, vaya a **Configuración** > **Configuración del sistema** > **Configuración de hardware** > **vFlash** > **Administrar**. Se muestra la página **Administrar particiones** , la cual enumera las particiones disponibles y la información relacionada para cada partición. Para obtener información acerca de las particiones, consulte la *Ayuda en línea de iDRAC*.

Visualización de las particiones disponibles mediante RACADM

Para ver las particiones disponibles y sus propiedades en mediante RACADM:

1 Abra una consola Telnet, SSH o de comunicación en serie al sistema e inicie sesión.

2 Introduzca los comandos siguientes:
- Para enumerar todas las particiones existentes y sus propiedades:
```
racadm vflashpartition list
```
- Para obtener el estado operativo en la partición 1:
```
racadm vflashpartition status -i 1
```
- Para obtener el estado de todas las particiones existentes:

```
racadm vflashpartition status -a
```

NOTA: La opción -a solo es válida con la acción status.

Modificación de una partición

Puede cambiar una partición de solo lectura a lectura y escritura, o viceversa. Antes de modificar la partición, asegúrese de lo siguiente:

- La funcionalidad vFlash está activada.
- Dispone de privilegios **Acceder a los medios virtuales**.

NOTA: De manera predeterminada, se crea una partición de solo lectura.

Modificación de una partición mediante la interfaz web

Para modificar una partición:

1. En la interfaz web de iDRAC, vaya a **Configuration (Configuración)** > **System Settings (Configuración del sistema)** > **Hardware Settings (Configuración de hardware)** > **vFlash** > **Manage (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. El estado no se puede cambiar a lectura y escritura. Si la partición está conectada, la casilla de verificación aparecerá en gris.

Modificación de una partición mediante RACADM

Para ver las particiones disponibles y sus propiedades en la tarjeta:

1. Inicie sesión en el sistema por medio de telnet, SSH o una consola en serie.
2. Utilice uno de los siguientes:
   - Mediante el comando `set` para cambiar el estado de lectura y escritura de la partición:
     - Para cambiar una partición de solo lectura a lectura y escritura:
       ```
       racadm set iDRAC.vflashpartition.<index>.AccessType 1
       ```
     - Para cambiar una partición de lectura y escritura a solo lectura:
       ```
       racadm set iDRAC.vflashpartition.<index>.AccessType 0
       ```
   - Mediante el comando `set` para especificar el tipo de emulación:
     ```
     racadm set iDRAC.vflashpartition.<index>.EmulationType <HDD, Floppy, or CD-DVD>
     ```

Conexión o desconexión de particiones

Cuando conecta una o más particiones, estas estarán visibles para el sistema operativo y el BIOS como dispositivos de almacenamiento masivo USB. Cuando conecta varias particiones en función del índice asignado, estas se enumeran en orden ascendiente en el sistema operativo y en el menú del orden de inicio de BIOS.

Si desconecta una partición, esta dejará de ser visible en el sistema operativo y en el menú de orden de inicio del BIOS.

Al conectar o desconectar una partición, se restablece el bus USB del sistema administrado. Esto afecta a las aplicaciones que utilizan vFlash y desconecta las sesiones de medios virtuales de iDRAC.

Antes de conectar o desconectar una partición, asegúrese de lo siguiente:

- La funcionalidad vFlash está activada.
- No se está realizando una operación de inicialización en la tarjeta.
- Dispone de privilegios **Acceder a los medios virtuales**.

Conexión o desconexión de particiones mediante la interfaz web

Para conectar o desconectar particiones:

1 En la interfaz web de iDRAC, vaya a **Configuration (Configuración)** > **System Settings (Configuración del sistema)** > **Hardware Settings (Configuración de hardware)** > **vFlash** > **Manage (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 Inicie sesión en el sistema por medio de telnet, SSH o una consola en serie.

2 Use los siguientes comandos:
- Para conectar una partición:
```
racadm set iDRAC.vflashpartition.<index>.AttachState 1
```
- Para desconectar una partición:
```
racadm set iDRAC.vflashpartition.<index>.AttachState 0
```

Comportamiento del sistema operativo para particiones conectadas

Para los sistemas operativos Windows y Linux:

- El sistema operativo controla y asigna las letras de unidad a las particiones conectadas.
- Las particiones se 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 el tipo de partición EXT2, que es nativo de Linux. Por ejemplo, en un entorno de Linux, el sistema operativo no puede leer el tipo de partición NTFS que es nativo de Windows.
- La etiqueta de la partición vFlash es diferente del nombre del volumen del 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 se modifica el nombre de la etiqueta de partición almacenada en iDRAC.

Eliminación de las particiones existentes

Antes de eliminar el contenido de una partición, asegúrese de lo siguiente:

- La funcionalidad vFlash está activada.

- La tarjeta no está protegida contra escritura.
- La partición no está conectada.
- No se está realizando una operación de inicialización en la tarjeta.

Eliminación de las particiones disponibles mediante la interfaz web

Para eliminar una partición existente:

1 En la interfaz web de iDRAC, vaya a **Configuración** > **Configuración del sistema** > **Configuración de hardware** > **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 **OK** (Aceptar).
Se elimina la partición.

Eliminación de las particiones existentes mediante RACADM

Para eliminar particiones:

1 Abra una consola Telnet, SSH o de comunicación en serie al sistema e inicie sesión.

2 Introduzca los comandos siguientes:
- Para eliminar una partición:
```
racadm vflashpartition delete -i 1
```
- Para eliminar todas las particiones, vuelva a inicializar la tarjeta vFlash SD.

Descarga del contenido de una partición

Puede descargar el contenido de una partición vFlash en el formato **.img** o **.iso** en las ubicaciones siguientes:

- Sistema administrado (desde el que se opera iDRAC)
- Ubicación de red asignada a una estación de administración

Antes de descargar el contenido de una partición, asegúrese de lo siguiente:

- Dispone de privilegios Acceder a los medios virtuales.
- La funcionalidad vFlash está activada.
- No se está realizando una operación de inicialización en la tarjeta.
- En el caso de una partición de lectura y escritura, no debe estar conectada.

Para descargar el contenido de la partición vFlash:

1 En la interfaz web de iDRAC, vaya a **Configuración** > **Configuración del sistema** > **Configuración de hardware** > **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: Todas las particiones existentes (excepto las particiones conectadas) aparecen en la lista. La primera partición se selecciona en forma predeterminada.**

3 Especifique la ubicación donde desea guardar el archivo.
El contenido de la partición seleccionada se descarga en la ubicación especificada.

NOTA: Si solo se especifica la ubicación de la carpeta, se utilizará la etiqueta de partición como nombre de archivo, junto con la extensión .iso para particiones de CD y disco duro e .img para particiones de disco flexible y disco duro.

Inicio de una partición

Se puede establecer una partición vFlash conectada como el dispositivo de inicio para la siguiente operación de inicio.

Antes de iniciar una partición, asegúrese de lo siguiente:

- La partición vFlash contiene una imagen de inicio (en formato **.img** o **.iso**) para realizar el inicio desde el dispositivo.
- La funcionalidad vFlash está activada.
- Dispone de privilegios Acceder a los medios virtuales.

Inicio de una partición mediante la interfaz web

Para establecer la partición vFlash como primer dispositivo de inicio, consulte Inicio de una partición mediante la interfaz web.

NOTA: Si las particiones vFlash conectadas no figuran en el menú desplegable Primer dispositivo de inicio, asegúrese de que el BIOS se haya actualizado a la versión más reciente.

Inicio de una partición mediante RACADM

Para establecer una partición vFlash como el primer dispositivo de inicio, utilice el objeto **iDRAC.ServerBoot**.

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

NOTA: Cuando se ejecuta este comando, la etiqueta de la partición vFlash se establece automáticamente en inicio único (`iDRAC.ServerBoot.BootOnce` se establece como `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.

24

Uso de SMCLP

La especificación Protocolo de la línea de comandos de administración del servidor (SMCLP) permite una 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 del modelo de información común (CIMOM) mediante un conjunto de comandos orientados a humanos. SMCLP es un subcomponente de la iniciativa SMASH del Grupo operativo de gestión distribuida (DMTF) para optimizar la administración de sistemas en varias plataformas. La especificación SMCLP, junto con la especificación de abordaje de elementos administrados y varios perfiles a especificaciones de asignación SMCLP, describe los verbos y destinos estándares de las distintas ejecuciones de tareas de administración.

NOTA: Se presupone que el usuario está familiarizado con la iniciativa Arquitectura de administración de sistemas para el hardware de servidor (SMASH) y las especificaciones SMCLP para el grupo de trabajos de administración (SMWG).

El SM-CLP es un subcomponente de la iniciativa SMASH del Grupo operativo de gestión distribuida (DMTF) para optimizar la administración de servidores en varias plataformas. La especificación SM-CLP, junto con la especificación de abordaje de elementos administrados y varios perfiles a especificaciones de asignación SM-CLP, describe los verbos y destinos estándares de las distintas ejecuciones de tareas de administración.

La SMCLP se aloja desde el firmware de la controladora iDRAC y admite interfaces Telnet, SSH y en serie. La interfaz SMCLP de iDRAC se basa en la especificación SMCLP Versión 1.0 provista por la organización DMTF.

NOTA: Es posible acceder a la información acerca de los perfiles, las extensiones y los MOF en delltechcenter.com y a toda la información sobre DMTF disponible en dmtf.org/standards/profiles/.

Los comandos SM-CLP implementan un subconjunto de comandos RACADM locales. Los comandos son útiles 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 comandos en formatos bien definidos, incluido XML, lo que facilita la creación de secuencias de comandos y la integración con herramientas de informes y administración existentes.

Temas:

Capacidades de System Management mediante SMCLP

SMCLP de iDRAC permite:

- Administración de la alimentación del servidor: encender, apagar o reiniciar el sistema
- Administración de registro de sucesos del sistema (SEL): mostrar o borrar las anotaciones del registro de sucesos del sistema
- Vea las cuentas de usuario del iDRAC

- Ver las propiedades del sistema

Ejecución de los comandos SMCLP

Puede ejecutar los comandos SMCLP mediante la interfaz SSH o Telnet. Abra una interfaz SSH o Telnet e inicie sesión en iDRAC como administrador. Aparece el símbolo del sistema SMCLP (admin ->).

Símbolos del sistema de SMCLP:

- Los servidores Blade yx1x utilizan `-$`.
- Los servidores tipo bastidor y torre yx1x utilizan `admin->`.
- Los servidores Blade, bastidor y torre yx2x utilizan `admin->`.

donde, y es un carácter alfanumérico, tal como M (para servidores Blade), R (para servidores tipo bastidor) y T (para servidores tipo torre) y x es un número. Esto indica la generación de servidores Dell PowerEdge.

NOTA: Las secuencias de comandos `-$` puede utilizar estos para sistemas yx1x. Sin embargo, a partir de los sistemas yx2x se puede utilizar una secuencia de comandos con `admin->` para los servidores tipo Blade, bastidor y torre.

Sintaxis SMCLP de iDRAC

El SMCLP de iDRAC utiliza el concepto de verbos y destinos para proporcionar a los sistemas capacidades de administración a través de la CLI. El verbo indica la operación que se debe realizar y el destino determina la entidad (u objeto) que ejecuta la operación.

La sintaxis de la línea de comandos de SMCLP es la siguiente:

```
<verb> [<options>] [<target>] [<properties>]
```

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

Tabla 41. Verbos de SMCLP

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

En la tabla siguiente se proporciona una lista de destinos.

Tabla 42. Destinos de SMCLP

Destino	Definiciones
admin1	Dominio de admin
admin1/profiles1	Perfiles registrados en iDRAC
admin1/hdwr1	Hardware
admin1/system1	Destino del sistema administrado
admin1/system1/capabilities1	Capacidades de recopilación del sistema administrado SMASH
admin1/system1/capabilities1/elecap1	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/pwrmgtcap1	Capacidades del servicio de administración del estado de la alimentación en el sistema
admin1/system1/sp1/capabilities1/acctmgtcap*	Capacidades del servicio de administración de cuentas
admin1/system1/sp1/capabilities1/rolemgtcap*	Capacidades de administración basada en funciones locales
admin1/system1/sp1/capabilities1/elecap1	Capacidades de autentificación
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

Destino	Definiciones
admin1/system1/sp1/jobq1	Cola de trabajo del protocolo del servicio CLP
admin1/system1/sp1/jobq1/job*	Trabajo del protocolo del servicio CLP
admin1/system1/sp1/pwrmgtsvc1	Servicio de administración del estado de la alimentación
admin1/system1/sp1/account1-16	Cuenta de usuario local
admin1/sysetm1/sp1/account1-16/identity1	Cuenta de identidad de usuario local
admin1/sysetm1/sp1/account1-16/identity2	Cuenta de identidad de IPMI (LAN)
admin1/sysetm1/sp1/account1-16/identity3	Cuenta de identidad de IPMI (conexión serie)
admin1/sysetm1/sp1/account1-16/identity4	Cuenta de identidad CLP
admin1/system1/sp1/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

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 espacio de direcciones de Punto de acceso administrable (MAP). Una ruta de acceso de direcciones especifica la ruta de acceso desde la raíz del espacio de direcciones a un objeto de este.

El destino de raíz está representado mediante una barra diagonal (/) o una barra diagonal invertida (\). Se trata del punto de inicio predeterminado al iniciar sesión en iDRAC. Desplácese desde 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, si aparece una barra diagonal invertida 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 encontrar su ubicación actual en el espacio de direcciones. Las abreviaciones `..` y `.` funcionan de la misma forma que en Windows y Linux: `..` se refiere al nivel superior inmediato y `.` se refiere al nivel actual.

Uso del verbo Show

Para obtener más información acerca de un destino, utilice el verbo `show` . 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` le 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` lleva a cabo `show` a través de 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 los cuatro formatos para la salida de los verbos de SM-CLP: **text**, **clpcsv**, **keyword** y **clpxml**.

El formato predeterminado es **text**, y es la salida que se lee con mayor facilidad. El formato **clpcsv** es un formato de valores separados por coma adecuado para cargar en un programa de hoja de cálculo. El formato **keyword** genera información como una lista de pares de palabras clave=valor en modo de uno por línea. El formato **clpxml** es un documento XML que contiene un elemento XML **response**. El DMTF ha especificado los formatos **clpcsv** y **clpxml** y sus especificaciones se encuentran disponibles en el sitio web de DMTF en **dmtf.org**.

El siguiente ejemplo muestra cómo incluir el contenido del registro de sucesos del sistema en el mensaje de salida de XML:

```
show -l all -output format=clpxml /admin1/system1/logs1/log1
```

Ejemplos de uso

En esta sección se proporcionan escenarios prácticos para SMCLP:

- Administración de la alimentación del servidor
- Administración de SEL
- Navegación en MAP del destino

Administración de la alimentación del servidor

En los ejemplos siguientes se muestra cómo utilizar SMCLP para realizar operaciones de administración de la alimentación en un sistema administrado.

Escriba los comandos siguientes en el símbolo del sistema SMCLP:

- Para apagar el servidor:
  ```
  stop /system1
  ```
  Aparece el siguiente mensaje:
  ```
  system1 has been stopped successfully
  ```
- Para activar el servidor:
  ```
  start /system1
  ```
  Aparece el siguiente mensaje:
  ```
  system1 has been started successfully
  ```
- Para reiniciar el servidor:
  ```
  reset /system1
  ```
  Aparece el siguiente mensaje:
  ```
  system1 has been reset successfully
  ```

Administración de SEL

En los ejemplos siguientes se muestra cómo utilizar SMCLP para realizar operaciones relacionadas con SEL en el sistema administrado. Escriba los comandos siguientes en el símbolo del sistema SMCLP:

- Para ver el SEL:
  ```
  show/system1/logs1/log1
  ```
  Aparece la siguiente información:
  ```
  /system1/logs1/log1

  Targets:

  Record1

  Record2

  Record3

  Record4

  Record5

  Properties:
  ```

```
InstanceID = IPMI:BMC1 SEL Log

MaxNumberOfRecords = 512

CurrentNumberOfRecords = 5

Name = IPMI SEL

EnabledState = 2

OperationalState = 2

HealthState = 2

Caption = IPMI SEL

Description = IPMI SEL

ElementName = IPMI SEL

Commands:

cd

show

help

exit

version
```

- Para ver la anotación SEL:
  `show/system1/logs1/log1`

  Aparece la siguiente información:

```
/system1/logs1/log1/record4


Properties:

LogCreationClassName= CIM_RecordLog

CreationClassName= CIM_LogRecord

LogName= IPMI SEL

RecordID= 1

MessageTimeStamp= 20050620100512.000000-000

Description= FAN 7 RPM: fan sensor, detected a failure

ElementName= IPMI SEL Record


Commands:
```

```
cd

show

help

exit

version
```

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:
  tipo `cd .`
- Para subir un nivel:
  tipo `cd ..`
- Para salir:
  `exit`

25

Implementación de los sistemas operativos

Puede utilizar cualquiera de las utilidades siguientes para implementar sistemas operativos en sistemas administrados:

- Recurso compartido de archivos remotos
- Consola de medios virtuales

Temas:

Implementación del sistema operativo mediante recurso compartido de archivos remotos

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

- Los privilegios **Configurar Usuario** y **Acceder a los medios virtuales** para iDRAC están activados para el usuario.
- El recurso compartido de red contiene controladores y el archivo de imagen iniciable de sistema operativo tiene un formato estándar del sector, tal como **.img** o **.iso**.

  NOTA: Al crear el archivo de imagen, siga los procedimientos de instalación en red estándares y marque la imagen de implementación como de solo lectura para asegurarse de que cada sistema de destino inicie y ejecute el mismo procedimiento de implementación.

Para implementar un sistema operativo mediante RFS:

1. Con el recurso compartido de archivos remotos (RFS), coloque la imagen ISO o IMG en el sistema administrado a través de NFS o CIFS.
2. Vaya a **Configuración** > **Configuración del sistema** > **Configuración de hardware** > **Primer dispositivo de inicio**.
3. Establezca el orden de inicio en la lista desplegable **Primer dispositivo de inicio** para seleccionar un medio virtual, como por ejemplo disquete, CD, DVD o ISO.
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.

Administración de recursos compartidos de archivos remotos

Mediante la función de recursos compartidos de archivos remotos (RFS), puede establecer un archivo de imagen ISO o IMG en un recurso compartido de red y ponerlo a disposición del sistema operativo del servidor administrado como una unidad virtual. Para ello, móntelo como un CD o DVD mediante NFS o CIFS. Esta función requiere licencia.

El recurso compartido de archivos remotos solo admite los formatos de archivos de imagen **.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.

Las funciones RFS y Medios virtuales son mutuamente exclusivas.

- Si el cliente de medios virtuales no está activo e intenta establecer una conexión con RFS, la conexión se establecerá y la imagen remota estará disponible para el sistema operativo host.
- Si el cliente de medios virtuales está activo e intenta establecer una conexión con RFS, aparecerá el siguiente mensaje de error:

  Los medios virtuales están desconectados o redirigidos para la unidad virtual seleccionada.

El estado de conexión RFS está disponible en el registro de iDRAC. Una vez conectada, una unidad virtual montada mediante RFS no se desconecta aunque cierre sesión de iDRAC. La conexión RFS se cierra si iDRAC se reinicia o si se interrumpe la conexión de red. También están disponibles las opciones de Interfaz web y línea de comandos en CMC e iDRAC para cerrar la conexión de RFS. La conexión RFS de CMC siempre invalida una unidad montada mediante RFS existente en iDRAC.

NOTA:

- CIFS admite las direcciones IPv4 e IPv6 pero NFS admite solamente la dirección IPv4.
- Si está utilizando CIFS y forma parte de un dominio de Active Directory, introduzca el nombre de dominio con la dirección IP en la ruta de acceso de un archivo de imagen.
- Si desea acceder a un archivo desde un recurso compartido NFS, configure los siguientes permisos de recursos compartidos. Estos permisos son necesarios debido a que las interfaces de iDRAC se ejecutan en un modo que no es raíz.
  - Linux: asegúrese de que los permisos de los recursos compartidos se establezcan al menos en **Lectura** para la cuenta **Otros**.
  - Windows: Vaya a la pestaña **Seguridad** de las propiedades del recurso compartido y agregue **Todos** al campo **Nombres de grupos o usuarios** con el privilegio **Leer y ejecutar**.

  ,
- Si ESXi se está ejecutando en el sistema administrado y monta una imagen de disco flexible (**.img**) mediante RFS, la imagen del disco flexible conectado no está disponible para el sistema operativo ESXi.
- La función vFlash de iDRAC y RFS no tienen relación.

Configuración de recursos compartidos de archivos remotos mediante la interfaz web

Para activar el uso compartido de archivos remotos:

1 En la interfaz web del iDRAC, vaya a **Configuración** > **Medios virtuales** > **Medios conectados**.

Aparece la página **Medios conectados**.

2 En **Medios conectados**, seleccione **Conectar** o **Conectar automáticamente**.

3 En **Recurso compartido de archivos remoto**, especifique la ruta de acceso del archivo de imagen, el nombre de dominio, el nombre de usuario y la contraseña. Para obtener información acerca de los campos, consulte la *Ayuda en línea de iDRAC7*.

Ejemplo de ruta de acceso de un archivo de imagen:

- CIFS: //<IP para conexión para sistema de archivos CIFS>/<ruta de archivo>/<nombre de imagen>
- NFS: <IP para conexión para sistema de archivos NFS>:/<ruta de archivo>/<nombre de imagen>

NOTA: Para evitar errores de E/S cuando se utilizan los recursos compartidos CIFS alojados en sistemas Windows 7, modifique las siguientes claves de registro:

- Configure HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\LargeSystemCache para 1
- Configure HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\Size en 3

NOTA: Los caracteres '/' o '\' se pueden utilizar para la ruta de archivo.

CIFS admite las dos direcciones IPv4 e IPv6 pero NFS admite solamente la dirección IPv4.

Si está utilizando un recurso compartido de NFS, asegúrese de introducir la <ruta de acceso del archivo> y el <nombre de la imagen> exactos ya que distingue mayúsculas de minúsculas.

NOTA: Para obtener más información sobre los caracteres recomendados para los nombres de usuario y las contraseñas, consulte Caracteres recomendados para nombres de usuario y contraseñas.

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

4 Haga clic en **Aplicar** y, después, en **Conectar**.

Una vez establecida la conexión, la opción **Estado de conexión** muestra la opción **Conectado**.

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

Para los distribuidores de Linux, es posible que esta función requiera un comando de montaje manual cuando se trabaja en el nivel de ejecución init 3. La sintaxis del comando es la siguiente:

```
mount /dev/OS_specific_device / user_defined_mount_point
```

donde, `user_defined_mount_point` es cualquier directorio que decida utilizar para el montaje similar a cualquier comando de montaje.

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 conectar el dispositivo virtual, en el sistema operativo Linux debe ejecutar el comando siguiente inmediatamente:

```
tail /var/log/messages | grep SCSI
```

Esto muestra el texto que identifica el dispositivo (por ejemplo, sdc del dispositivo SCSI). Este procedimiento también se aplica a los medios virtuales cuando utiliza distribuciones de Linux en el nivel de ejecución init 3. De manera predeterminada, los medios virtuales no se montan automáticamente en init 3.

Configuración de recursos compartidos de archivos remotos mediante RACADM

Para configurar el uso compartido de archivos remotos mediante RACADM, utilice los comandos siguientes:

`racadm remoteimage`

`racadm remoteimage <options>`

Las opciones disponibles son:

`-c`: conectar imagen

`-d`: desconectar imagen

`-u` <nombre de usuario>: 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 Consulte ejemplos de ruta de acceso de un archivo de imagen en la sección Configuración de recursos compartidos de archivos remotos mediante la interfaz web

`-s`: mostrar el estado actual

NOTA: Todos los caracteres, incluidos los especiales y alfanuméricos, están permitidos para nombre de usuario, contraseña y ubicación_de_imagen excepto los siguientes caracteres: ' (comilla simple), " (comillas), , (comas), < (signo de menor que) y > (signo de mayor que).

NOTA: Para evitar errores de E/S cuando se utilizan los recursos compartidos CIFS alojados en sistemas Windows 7, modifique las siguientes claves de registro:

- Configure HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\LargeSystemCache para `1`
- Configure HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\Size en `3`

Implementación del sistema operativo mediante medios virtuales

Antes de implementar el sistema operativo mediante medios virtuales, asegúrese de lo siguiente:

- Los medios virtuales deben estar en el estado *Conectado* para que las unidades virtuales aparezcan en la secuencia de inicio.
- Si los medios virtuales se encuentran en modo *Conectado automáticamente*, la aplicación de medios virtuales debe iniciarse antes de iniciar el sistema.
- El recurso compartido de red contiene controladores y el archivo de imagen iniciable de sistema operativo tiene un formato estándar del sector, tal como **.img** o **.iso**.

Para implementar un sistema operativo mediante medios virtuales:

1 Pruebe una de las siguientes acciones: S
   - Inserte el CD o DVD de instalación del sistema operativo en la unidad correspondiente de la estación de administración.
   - Conecte la imagen del sistema operativo.
2 Seleccione la unidad en la estación de administración con la imagen necesaria para asignarla.
3 Utilice uno de los métodos siguientes para iniciar el dispositivo necesario:
   - Establezca el orden de inicio de inicio único desde **Disco flexible virtual** o **CD/DVD/ISO virtual** mediante la interfaz web de iDRAC.
   - Establezca el orden de inicio a través de **Configuración del sistema** > **Configuración del BIOS del sistema** presionando <F2> durante el inicio.
4 Reinicie el sistema administrado y siga las instrucciones en pantalla para completar la implementación.

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.

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 el **Puerto USB interno** como **Encendido**. Si se establece como **Apagado**, el IDSDM no estará disponible como dispositivo de inicio.
4 Si no se necesita redundancia (una sola tarjeta SD), configure la opción **Puerto de tarjeta SD interno** como **Activado** y la opción **Redundancia de la tarjeta SD interna** como **Desactivado**.
5 Si se necesita redundancia (dos tarjetas SD), establezca la opción **Puerto de tarjeta SD interno** en **Activado** y la opción **Redundancia de la tarjeta SD interna** en **Reflejar**.
6 Haga clic en **Atrás** y luego en **Terminar**.
7 Haga clic en **Sí** para guardar la configuración y presione <Esc> para salir de **Configuración del sistema**.

Acerca de IDSDM

El módulo SD dual interno (IDSDM) sólo está disponible en determinadas plataformas. IDSDM proporciona redundancia en la tarjeta SD del hipervisor utilizando otra tarjeta SD que refleja el contenido de la primera tarjeta SD.

Cualquiera de las dos tarjetas SD puede ser la tarjeta maestra. 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 en cualquier momento, la tarjeta SD1 falla o se elimina, la tarjeta SD2 se convierte automáticamente en la tarjeta activa (maestra).

Es posible ver el estado, la condición y la disponibilidad de IDSDM mediante la interfaz web de iDRAC o RACADM. El estado de redundancia de la tarjeta SD y los sucesos de falla se registran en SEL, el cual se muestra en el panel frontal, y las alertas PET se generan si están activadas.

26

Solución de problemas de Managed System mediante iDRAC

Puede diagnosticar y solucionar los problemas de un sistema administrado mediante los elementos siguientes:

- Consola de diagnósticos
- Código de la POST
- Videos de captura de inicio y bloqueo
- Pantalla de último bloqueo del sistema
- Registros de sucesos del sistema
- Registros de Lifecycle
- Estado del panel frontal
- Indicadores de problemas
- Condición del sistema

Temas:

Uso de la consola de diagnósticos

iDRAC ofrece un conjunto estándar de herramientas de diagnóstico de red similares a las herramientas que se incluyen con sistemas basados en Microsoft Windows o Linux. Mediante la interfaz web de iDRAC, es posible acceder a las herramientas de depuración de la red.

Para acceder a la consola de diagnósticos:

1 En la interfaz web de iDRAC, vaya a **Mantenimiento** > **Diagnósticos**.

Se muestra la página **Comando de la consola de diagnósticos**.

2 En el cuadro de texto **Comando**, escriba un comando y haga clic en **Enviar**. Para obtener información acerca de los comandos, consulte *iDRAC Online Help (Ayuda en línea para iDRAC)*.

Los resultados se muestran en la misma página.

Restablecer el iDRAC y Restablecer el iDRAC a los valores predeterminados

1 En la interfaz web de iDRAC, vaya a **Mantenimiento** > **Diagnóstico**.

Tiene las siguientes opciones:

- Haga clic en **Restablecer iDRAC** para restablecer el iDRAC. Se ejecutará una operación de reinicio normal en el iDRAC. Después del reinicio, actualice el explorador para volver a conectarse e iniciar sesión con iDRAC.
- Haga clic en **Restablecer el iDRAC a los valores predeterminados** para restablecer el iDRAC a los valores predeterminados. Después de hacer clic en **Restablecer el iDRAC a los valores predeterminados**, aparece la ventana **Restablecer el iDRAC a los valores predeterminados de fábrica**. Esta acción restablece el iDRAC a los valores predeterminados de fábrica. Seleccione cualquiera de las opciones siguientes:
  1 Descarte todos los valores, pero conserve el usuario y la configuración de red.
  2 Descartar todos los valores y restablecer el nombre de usuario predeterminado a raíz y la contraseña al valor de envío (raíz/valor de envío).
  3 Descartar todos los valores y restablecer el nombre de usuario predeterminado a raíz y la contraseña a calvin (raíz/calvin).

2 Haga clic en **Continue (Continuar)**.

Programación del diagnóstico automatizado remoto

Puede invocar en forma remota el diagnóstico automatizado fuera de línea en un servidor como un suceso de una sola vez y devolver los resultados. Si el diagnóstico requiere un reinicio, puede reiniciar inmediatamente o apilarlo para un ciclo de reinicio o mantenimiento subsiguiente (similar a las actualizaciones). Cuando se ejecutan los diagnósticos, los resultados se recopilan y almacenan en el almacenamiento interno del iDRAC. A continuación, puede exportar los resultados en un recurso compartido de red CIFS o NFS mediante el comando racadm `diagnostics export`. También puede ejecutar los diagnósticos mediante los comandos adecuados de WSMan. Para obtener más información, consulte la documentación de WSMan.

Es necesario tener la licencia iDRAC Express para usar los diagnósticos automatizados remotos.

Puede realizar los diagnósticos inmediatamente o programarlos para un día y horario determinados y especificar el tipo de diagnóstico y el tipo de reinicio.

Para el programa debe especificar lo siguiente:

- Hora de inicio: ejecute el diagnóstico en un día y horario futuros. Si especifica TIME NOW, el diagnóstico se ejecuta en el próximo reinicio.
- Hora de finalización: ejecute el diagnóstico hasta un día y horario posterior a la hora de inicio. Si no se inicia en la hora de finalización, se marca como fallido con Hora de finalización caducada. Si especifica TIME NA, no se aplica el tiempo de espera.

Los tipos de pruebas de diagnóstico son:

- Prueba rápida
- Prueba extendida
- Ambas en una secuencia

Los tipos de reinicio son:

- Realice un ciclo de encendido del sistema.
- Apagado ordenado (se espera a que se apague o reinicie el sistema operativo)
- Apagado ordenado forzado (le indica al sistema operativo que debe apagarse y espera 10 minutos. Si no se apaga, el iDRAC realiza un ciclo de encendido del sistema)

Solo puede programarse o ejecutarse un trabajo de diagnóstico a la vez. Un trabajo de diagnóstico puede finalizar satisfactoriamente, finalizar con errores o finalizar de manera incorrecta. Los sucesos de diagnóstico y los resultados se graban en el registro de Lifecycle Controller. Puede recuperar los resultados de la última ejecución del diagnóstico mediante RACADM remoto o WSMan.

Puede exportar los resultados del diagnóstico de los últimos diagnósticos finalizados que se programaron en forma remota a un recurso compartido de red como CIFS, NFS, HTTP o HTTPS. El tamaño máximo del archivo es de 5 MB.

Puede cancelar un trabajo de diagnóstico cuando el estado del trabajo es No programado o Programado. Si el diagnóstico se está ejecutando, reinicie el sistema para cancelarlo.

Antes de ejecutar el diagnóstico remoto, asegúrese de lo siguiente:

- Lifecycle Controller está activado.
- Cuenta con privilegios de Inicio de sesión y Control del servidor.

Programación de diagnóstico automatizado remoto mediante RACADM

- Para ejecutar los diagnósticos remotos y guardar los resultados en el sistema local, utilice el siguiente comando:
  ```
  racadm diagnostics run -m <Mode> -r <reboot type> -s <Start Time> -e <Expiration Time>
  ```
- Para exportar los resultados del último diagnóstico remoto ejecutado, utilice el siguiente comando:
  ```
  racadm diagnostics export -f <file name> -l <NFS / CIFS share> -u <username> -p <password>
  ```

Para obtener más información acerca de las opciones, consulte *iDRAC RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC) disponible en **dell.com/idracmanuals**.

Visualización de los códigos de la POST

Los códigos de la POST son indicadores de progreso del BIOS del sistema, los cuales indican las distintas etapas de la secuencia de inicio a partir del reinicio durante el encendido y le permiten diagnosticar los errores relacionados con el inicio del sistema. La página **Códigos de la POST** muestra el último código de la POST del sistema antes de iniciar el sistema operativo.

Para ver los códigos de la POST, vaya a **Mantenimiento** > **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 video de ciclo de inicio registra la secuencia de sucesos para un ciclo de inicio. Los vídeos de ciclos de inicio están organizados en el orden del más reciente al más viejo.
- Último video de bloqueo: un video de bloqueo registra la secuencia de sucesos que llevan al error.

Esta es una función con licencia.

iDRAC registra cincuenta marcos durante el tiempo de inicio. La reproducción de las pantallas de inicio se realiza a una velocidad de 1 marco por segundo. Si se restablece iDRAC, el video de captura de inicio no estará disponible, ya que se almacena en la memoria RAM y se luego se elimina.

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.
- La hora de captura de video que se muestra en el reproductor de video de la GUI de iDRAC puede diferir de la hora de captura de video que se muestra en otros reproductores de video. El reproductor de video de la GUI de iDRAC muestra la hora en la zona horaria de iDRAC mientras que los demás reproductores de video muestran la hora en las zonas horarias del respectivo sistema operativo.

NOTA: Los archivos de captura de inicio de DVC no son videos. Es una secuencia de pantallas (en una resolución particular) tomada durante el transcurso del inicio del servidor. El reproductor de DVC convierte estas pantallas en forma conjunta para crear el video de inicio. Cuando exporta el video de DVC (instantánea continua y diferencias) al formato .mov (video real), se espera que utilice la misma resolución, o una resolución similar, con la que el video se codificó inicialmente. Los videos deben ser exportados en una resolución similar a la resolución con la que fueron capturados.

NOTA: El retraso en la disponibilidad del archivo de captura de inicio se debe a que el búfer de captura de inicio no está completo después del inicio del host.

Para ver la pantalla **Captura de inicio**, haga clic en **Mantenimiento** > **Resolución de problemas** > **Captura de video**.

La pantalla de **Captura de video** muestra las grabaciones del video. Para obtener más información, consulte la *Ayuda en línea de iDRAC*.

Configuración de los valores de captura de video

Para configurar los valores de captura de video:

1 En la interfaz web de iDRAC, vaya a **Mantenimiento** > **Solución de problemas** > **Captura de video**.
Aparecerá la página **Captura de video**.
2 En el menú desplegable **Configuración de captura de video**, seleccione cualquiera de las opciones siguientes:
- **Desactivar**: se desactiva la captura de inicio.
- **Capturar hasta que el búfer esté completo**: la secuencia de inicio se captura hasta que haya alcanzado el tamaño del búfer.
- **Capturar hasta el final de POST**: la secuencia de inicio se captura hasta el final de POST.

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

Visualización de registros

Es posible visualizar los registros de sucesos del sistema (SEL) y los registros de Lifecycle. Para obtener más información, consulte Visualización del registro de sucesos del sistema y Visualización del registro de Lifecycle.

Visualización de la pantalla de último bloqueo del sistema

La función de la pantalla de último bloqueo captura una pantalla del bloqueo del sistema más reciente, la guarda y la muestra en iDRAC. Esta es una función con licencia.

Para ver la pantalla de último bloqueo:

1 Asegúrese de que la función de pantalla de último bloqueo esté activada.
2 En la interfaz web de iDRAC, vaya a **Descripción general** > **Servidor** > **Solución de problemas** > **Pantalla de último bloqueo**.
La página **Pantalla de último bloqueo** muestra la pantalla de último bloqueo guardada desde el sistema administrado.

Haga clic en **Borrar** para eliminar la pantalla de último bloqueo.

NOTA: Una vez que se restablece el iDRAC o se produce un suceso de ciclo de alimentación de CA, se borran los datos de captura de bloqueo.

Visualización de estado del sistema

El estado del sistema resume el estado de los siguientes componentes del sistema:

- Resumen
- Baterías
- Refrigeración
- CPU
- Panel frontal
- Intrusión
- Memoria
- Dispositivos de red
- Sistemas de alimentación
- Voltajes
- Medios flash extraíbles
- Controladora del chasis

Se puede ver el estado del sistema gestionado:

- Servidores tipo bastidor y torre: estado del LED de ID del sistema y del panel frontal LCD o el estado del LED de ID del sistema de panel frontal LED.
- Servidores Blade: solo los LED de ID del sistema.

Visualización del estado del LCD del panel frontal del sistema

Para ver el estado de panel anterior LCD para los servidores tipo bastidor y torre aplicables, en la interfaz web de iDRAC, vaya a **Sistema** > **Descripción general** > **Panel frontal**. Se muestra la página **Panel frontal**.

La sección **Panel frontal** muestra la transmisión en directo de los mensajes que aparecen actualmente en el panel frontal de LCD. Cuando el sistema funciona correctamente (indicado por un color azul sólido en el panel frontal de LCD), las opciones **Ocultar error** y **Mostrar error** aparecen en gris.

NOTA: Puede ocultar o mostrar los errores solamente para los servidores tipo bastidor y torre.

Basándose en la selección, el cuadro de texto muestra el valor actual. Si selecciona Definido por el usuario, introduzca el mensaje necesario en el cuadro de texto. El límite de caracteres es 62. Si selecciona Ninguno, el mensaje de inicio no se muestra en el LCD.

Para ver el estado de panel anterior LCD con RACADM, utilice los objetos en el grupo System.LCD. Para obtener más información, consulte *iDRAC RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM de iDRAC), disponible en **dell.com/idracmanuals**.

Visualización del estado del LED del panel frontal del sistema

Para ver el estado actual de un LED de ID del sistema, en la interfaz web de iDRAC, vaya a **Sistema** > **Descripción general** > **Panel frontal**. En la sección **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 ícono de estado azul en el panel frontal de LCD), las opciones **Ocultar error** y **Mostrar error** aparecen en gris. Puede ocultar o mostrar los errores solamente para los servidores tipo bastidor y torre.

Para ver el estado de un LED de identificación del sistema mediante RACADM, utilice el comando **getled**.

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

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: El usuario debe llevar a cabo únicamente las tareas de solución de problemas y las reparaciones sencillas autorizadas en la documentación del producto o indicadas por el personal de servicio y de asistencia en línea o telefónica. Los daños causados por reparaciones no autorizadas por Dell no están cubiertos por la garantía. Lea y siga las instrucciones de seguridad que se incluyen con el producto.

Visualización de la condición del sistema

Las interfaces web de iDRAC y CMC (para servidores blade) muestran el estado de los elementos siguientes:

- Baterías
- CPU
- Refrigeración
- Intrusión
- Memoria
- Sistemas de alimentación
- Medios flash extraíbles
- Voltajes
- Varios

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 un LED con luz ámbar parpadea, y un servidor particular tiene un error, la principal pantalla de estado del servidor en el LCD resalta en naranja el servidor afectado. Utilice los botones de navegación LCD para resaltar el servidor afectado y luego haga clic en el botón

central. Los mensajes de error y advertencia se mostrarán en la segunda línea. Para obtener la lista de mensajes de error que se muestra en el panel LCD, consulte el manual del propietario del servidor.

Reinicio de iDRAC

Puede realizar un reinicio por hardware o por software de iDRAC sin apagar el servidor:

- Reinicio por hardware: en el servidor, mantenga presionado el botón LED durante 15 segundos.
- Reinicio por software: utilice la interfaz web de iDRAC o RACADM.

Reinicio de iDRAC mediante la interfaz web de iDRAC

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

- Vaya a **Mantenimiento** > **Diagnósticos**. Haga clic en **Restablecer iDRAC**.

Reinicio de iDRAC mediante RACADM

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

Borrado de datos del sistema y del usuario

NOTA: El borrado de datos del sistema y del usuario no se admite desde la GUI iDRAC.

Es posible borrar componentes del sistema y datos del usuario para los siguientes componentes:

- Datos de Lifecycle Controller
- Diagnósticos incorporados
- Driver Pack para el sistema operativo incorporado
- Restablecimiento de los valores predeterminados del BIOS
- Restablecimiento de los valores predeterminados de iDRAC

Antes de llevar a cabo el borrado del sistema, asegúrese de que:

- Cuenta con el privilegio de control del servidor de iDRAC.
- Lifecycle Controller está activado.

La opción Datos de Lifecycle Controller borra cualquier contenido, como el registro de LC, la base de datos de configuración, el firmware de reversión, los registros enviados de fábrica y la información de configuración de FP SPI (o soporte vertical de administración).

NOTA: El registro de Lifecycle Controller contiene la información sobre la solicitud de borrado del sistema y cualquier información generada cuando el iDRAC se reinicia. Toda la información previa se elimina.

Es posible eliminar componentes del sistema individuales o múltiples mediante el comando **SystemErase**:

```
racadm systemErase <BIOS | DIAG | DRVPACK | LCDATA | IDRAC >
```

donde:

- bios: restablecimiento de los valores predeterminados del BIOS
- diag: diagnósticos incorporados
- drvpack: driver pack para el sistema operativo incorporado

- lcdata: se borran los datos de Lifecycle Controller
- iDRAC: restablecimiento de los valores predeterminados de iDRAC
- overwritepd: sobrescribir unidades de disco duro que no admiten borrado seguro instantáneo (ISE)
- percnvcache: restablecimiento del caché del controlador
- vflash: restablecimiento de vFlash
- secureerasepd: borrar unidades de disco duro, SSD y NVMe que admiten ISE
- allapps: borra todas las aplicaciones del sistema operativo

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

NOTA: El enlace del centro tecnológico de Dell aparece en la GUI de iDRAC en sistemas de la marca Dell. Si borra los datos del sistema utilizando el comando de WSMan y desea que el enlace aparezca nuevamente, reinicie el host en forma manual y espere a que CSIOR se ejecute.

NOTA: Una vez ejecutado el borrado del sistema, pueden seguir mostrándose los VD. Ejecute CSIOR después de que se haya completado el borrado del sistema y se haya reiniciado el iDRAC .

Restablecimiento de iDRAC a los valores predeterminados de fábrica

Es posible restablecer iDRAC a la configuración predeterminada de fábrica mediante la utilidad de configuración de iDRAC o la interfaz web de iDRAC.

Restablecimiento de iDRAC a los valores predeterminados de fábrica mediante la interfaz web de iDRAC

Para restablecer iDRAC a los valores predeterminados de fábrica mediante la interfaz web de iDRAC:

1 Vaya a **Mantenimiento** > **Diagnósticos**.
Se muestra la página **Consola de diagnósticos**.
2 Haga clic en **Restablecer iDRAC a los valores predeterminados**.
El estado de finalización se muestra en forma de porcentaje. iDRAC se reinicia y se restablece a los valores predeterminados de fábrica. La IP de iDRAC se restablece pero no es posible acceder a esa dirección. Puede configurar la IP mediante el panel anterior o el BIOS.

Restablecimiento de iDRAC a los valores predeterminados de fábrica mediante la utilidad de configuración de iDRAC

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

1 Vaya a **Restablecer la configuración de iDRAC a los valores predeterminados**.
Aparece la página **Restablecimiento de los valores predeterminado de iDRAC de la configuración de iDRAC**.
2 Haga clic en **Yes (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.

27

Integración de SupportAssist en iDRAC

SupportAssist le permite crear recopilaciones SupportAssist y utilizar otras funciones de SupportAssist para supervisar el sistema y el centro de datos. El iDRAC proporciona interfaces de una aplicación para recopilar información sobre la plataforma que ofrece soporte para resolver problemas de la plataforma y del sistema. iDRAC le permite generar una recopilación SupportAssist del servidor y luego exportarla a una ubicación en la estación de administración (local) o a una ubicación de red compartida como el Sistema de archivos de Internet comunes (CIFS) o el recurso compartido de archivos de red (NFS). La recopilación se genera en formato ZIP estándar, el cual está protegido por contraseña. Puede enviar esta recopilación al soporte técnico para la solución de problemas o la recopilación de inventario.

Temas:

Registro de SupportAssist

Para activar las funciones proactivas y predictivas automatizadas de SupportAssist en el sistema, el usuario necesita registrar el sistema con SupportAssist.

El usuario puede crear y guardar una recopilación en forma local o en el recurso compartido de red sin necesidad de registro.

Información de contacto y envío

Para completar el proceso de registro, los usuarios deben proporcionar datos de los clientes.

Información de contacto principal

Introduzca Nombre*, Apellido*, Número de teléfono*, Número alternativo, Dirección de correo electrónico*, la opción de Dirección del servicio (le permite agregar dirección física, dónde el dispositivo recibirá soporte o donde las piezas de repuesto deben ser enviadas), Nombre de la empresa*, Línea de dirección 1*, Línea de dirección 2, Ciudad*, Estado*, Código postal* y País*. Verifique si los detalles se muestran correctamente y realice cambios si desea editar alguno de los campos.

* Indica que los campos son obligatorios.

Información de contacto secundario

Introduzca Nombre, Apellido, Número de teléfono, Número alternativo y Dirección de correo electrónico, verifique si los detalles se muestran correctamente y efectúe cambios si desea editar alguno de los campos.

NOTA: Puede quitar la información de contacto secundaria en cualquier momento.

Acuerdo de licencia de usuario final

Después de proporcionar toda la información necesaria, debe aceptar el Acuerdo de licencia de usuario final (EULA) para completar el proceso de registro. Tiene la opción de imprimir el EULA con motivo de futura referencia. Puede cancelar y terminar el proceso de registro en cualquier momento.

Instalación del módulo de servicios

Para registrarse y utilizar SupportAssist, debe contar con un Módulo de servicios de iDRAC (iSM) instalado en el sistema. Una vez que haya **iniciado la Instalación del módulo de servicios,** puede ver las instrucciones de instalación. El botón **Siguiente** se mantiene deshabilitado hasta que instale correctamente iSM.

Información de proxy del sistema operativo del servidor

De haber un problema con la conexión, se le solicitará al usuario que proporcione información del proxy del sistema operativo. Introduzca **el servidor, el puerto, el nombre de usuario** y **la contraseña** para configurar los valores del proxy.

SupportAssist

Una vez configurado SupportAssist, puede ver el panel de SupportAssist para **Iniciar una recopilación**, ver **Resumen de solicitudes de servicio, Descripción general de SupportAssist, Solicitudes de servicio** y **Recopilaciones.**

Visite el Portal de asistencia

La **Solicitud de servicio** muestra la información de**Estado** (abierto/cerrado), **Descripción**, **Origen** (evento/teléfono), **ID de solicitud de servicio**, **Envío** (sí/no), **Fecha de apertura** y **Fecha de cierre** para cada evento. Puede seleccionar y ver más detalles de cada suceso. Cuenta con la opción de verificar el Portal de solicitud de servicio para ver información adicional de cualquier caso individual.

Registro de recopilación

El registro de recopilación muestra los detalles de **fecha y hora de recopilación, tipo de recopilación** (manual, programada o basada en sucesos)**, datos recopilados** (Selección personalizada, todos los datos)**, estado de la recopilación** (completa con errores, completa)**, estado de enviado** y **fecha y hora de envío**. Puede enviar la última recopilación que persiste en el iDRAC a DellEMC.

NOTA: Los datos están filtrados para mantener la privacidad del usuario y no contiene el nombre de host, las direcciones mac, los registros o el contenido del Registro.

Generación de SupportAssist

Para generar los registros del sistema operativo y de la aplicación:

- El Módulo de servicio de iDRAC debe estar instalado y en ejecución en el sistema operativo del host.
- Si se elimina OS Collector, el cual viene instalado de fábrica en iDRAC, debe estar instalado en iDRAC.

Si debe trabajar con la Asistencia técnica en un problema con un servidor pero las políticas de seguridad restringen la conexión a Internet, puede proporcionarle a la Asistencia técnica los datos necesarios para facilitar la solución de problemas sin tener que instalar software o descargar herramientas de Dell y sin tener acceso a la Internet desde el sistema operativo del servidor o iDRAC.

Puede generar un informe de estado del servidor y luego exportar la recopilación:

- A una ubicación en la estación de administración (local).
- A una ubicación de red compartida como un sistema de archivos de Internet comunes (CIFS) o recurso compartido de archivos de red (NFS). Para exportar a un recurso compartido de red CIFS o NFS, se necesita conectividad de red directa al puerto de red compartido o dedicado del iDRAC.
- Para DellEMC en un servidor registrado con SupportAssist. Para más información sobre el registro de SupportAssist, consulte la sección Registro con SupportAssist.

La Recopilación de SupportAssist se genera en el formato ZIP estándar. La recopilación contiene la siguiente información:

- La Recopilación de SupportAssist también contiene un visor HTML 5, al cual se puede acceder inmediatamente una vez completada la recopilación.
- Esto puede verse sin cargar en el sitio de asistencia técnica. Esta recopilación proporciona una cantidad masiva de información detallada del sistema y registros en un formato fácil de usar.
- Inventario de hardware para todos los componentes (incluye detalles de firmware y configuración de componentes del sistema, registros de sucesos del sistema de la placa base, información del estado de iDRAC y registros de Lifecycle Controller).
- Sistema operativo e información de las aplicaciones.
- Registros de la controladora de almacenamiento.
- Registros de depuración de iDRAC.

Después de que se generan los datos, podrá verlos. Contiene un conjunto de archivos XML y archivos de registro.

Cada vez que se recopilan datos, se graba un suceso en el registro de Lifecycle Controller. El suceso incluye información como la interfaz utilizada y la fecha y hora de la exportación.

En Windows, si WMI se desactiva, la recopilación de OS Collector se detiene y se muestra un mensaje de error.

Verifique los niveles de privilegio adecuados y asegúrese de que no haya ninguna configuración de Firewall o de seguridad que pueda impedir la obtención de los datos del software o el registro.

Antes de generar el informe de condición, compruebe lo siguiente:

- Lifecycle Controller está activado.
- Collect System Inventory On Reboot (Recopilar inventario del sistema al reiniciar) (CSIOR) está habilitada.
- Cuenta con privilegios de Inicio de sesión y Control del servidor.

Generación de SupportAssist Collection en forma manual mediante la interfaz web del iDRAC

Si el módulo de servicio de iDRAC está instalado y en ejecución en el Sistema operativo del host, puede generar manualmente la Recopilación de SupportAssist. El Módulo de servicios de iDRAC invoca el archivo del Recopilador del sistema operativo correspondiente en

el sistema operativo del host, recopila los datos y los transfiere a iDRAC. Luego, puede guardar los datos en la ubicación requerida. Para generar la recopilación de SupportAssist manualmente:

1 En la interfaz web de iDRAC, vaya a **Mantenimiento** > **SupportAssist**.
2 Si el servidor no está registrado para el flujo de trabajo de SupportAssist, aparece el asistente de registro de SupportAssist. Haga clic en **Cancelar** > **Cancelar registro**.
3 Haga clic en **Iniciar una recopilación**.
4 Seleccione los conjuntos de datos que se incluirán en la Recopilación o deje los valores predeterminados seleccionados.
5 Puede seleccionar los conjuntos de datos que se deben filtrar para la Información de identificación personal (PII).
6 Seleccione el destino en el que la Recopilación se debe guardar.
   a Si el servidor está registrado para el flujo de trabajo SupportAssist y la opción **Enviar ahora** está activada. Al seleccionar esta opción se transmite la Recopilación generada a DellEMC SupportAssist.
   b La opción **Guardar localmente** le permite guardar la Recopilación generada en el sistema local.
   c La opción **Guardar en la red** guarda la Recopilación generada en la ubicación de recurso compartido de CIFS o NFS definida por el usuario.

   Si la opción **Guardar en la red** está seleccionada, la información de red proporcionada por el usuario se guarda con los valores predeterminados (si no se ha guardado ninguna ubicación anterior de recurso compartido de red) para cualquier recopilación futura.
7 Haga clic en **Recopilar** para continuar con la generación de la Recopilación.
8 Acepte el **Acuerdo de nivel usuario final (EULA)** para continuar.

   La opción de datos del sistema operativo y de la aplicación aparecerá en gris y no se podrá seleccionar si:

   - iSM no está instalado o en ejecución en el sistema operativo del host, o
   - El Recopilador del sistema operativo fue eliminado del iDRAC, o
   - El paso directo del SO-BMC está desactivado en el iDRAC, o
   - Los datos de la aplicación del sistema operativo almacenados en caché no están disponibles en iDRAC desde una recopilación anterior

Configuración

Esta página lo ayuda con los detalles de **Configuración de recopilación** e **Información de contacto**.

Configuración de recopilación

Puede guardar las recopilaciones en una ubicación de red preferida. Utilice **Establecer directorio de archivo** para establecer la ubicación de la red.

Puede optar por incluir la información de identificación durante el envío de los datos a Dell en la configuración de recopilación.

Puede activar y programar las opciones de **Recopilación automática** para evitar la intervención manual y mantener una comprobación periódica del sistema De manera predeterminada, cuando se activa un evento y se abre un caso de asistencia, SupportAssist se configura para recopilar automáticamente los registros del sistema desde el dispositivo que generó la alerta y cargarlos a Dell. Puede activar o desactivar la recopilación automática basada en eventos Puede programar las recopilaciones automáticas en función de sus requisitos adecuados. Las opciones disponibles son semanalmente, mensualmente, trimestralmente o nunca. También puede configurar la fecha y hora para los eventos periódicos programados. Tiene la opción de configurar el **Informe de recomendación de ProSupport Plus** durante la configuración de las recopilaciones automáticas. La únca opción para el **Informe de recomendaciones de ProSupport Plus** es encendido o apagado

Valor predeterminado para las recopilaciones

Puede establecer una ubicación de red predeterminada para guardar todas las futuras recopilaciones. De no haber seleccionado una ubicación de red predeterminada, en el futuro no podrá ver sus recopilaciones. Introduzca el tipo de **Protocolo** (CIFS/NFS) que haya

elegido, la **dirección IP, el nombre del recurso compartido, el nombre de dominio, el nombre de usuario** y la **contraseña** antes de **probar la conexión de red.**

Información de contacto

En esta página se muestran los detalles de la información de contacto que ha proporcionado durante el registro de SupportAssist.

28

Preguntas frecuentes

En esta sección se enumeran las preguntas frecuentes para los elementos siguientes:

- Registro de sucesos del sistema
- Seguridad de la red
- Active Directory
- Inicio de sesión único
- Inicio de sesión mediante tarjeta inteligente
- Consola virtual
- Medios virtuales
- Tarjeta vFlash SD
- Autentificación de SNMP
- Dispositivos de almacenamiento
- Módulo de servicios de iDRAC
- RACADM
- Varios

Temas:

Registro de sucesos del sistema

Al utilizar la interfaz web de iDRAC a través de Internet Explorer, ¿por qué el registro SEL no se puede guardar mediante la opción Guardar como?

Esto se debe a un parámetro del explorador. Para resolver esto:

1 En Internet Explorer, vaya a **Herramientas** > **Opciones de Internet** > **Seguridad** y seleccione la zona en la que intenta descargar.

Por ejemplo, si el dispositivo iDRAC se encuentra en la Intranet local, seleccione **Intranet local** y haga clic en **Nivel personalizado...**.

2 En la ventana **Configuración de seguridad**, en **Descargas**, compruebe que las siguientes opciones estén activadas:
   - Preguntar automáticamente si se debe descargar un archivo: (si está disponible)
   - Descarga de archivos

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

Seguridad de la red

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

iDRAC incluye un certificado de servidor de iDRAC predeterminado para garantizar la seguridad de la red cuando se accede a través de la interfaz web y el RACADM remoto. Este certificado no lo emite una CA de confianza. Para resolver esta cuestión, cargue un certificado de servidor iDRAC emitido por una CA de confianza (por ejemplo, Microsoft Certificate Authority, Thawte o Verisign).

¿Por qué el servidor DNS no registra iDRAC?

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

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

iDRAC incluye un certificado de servidor de iDRAC predeterminado para garantizar la seguridad de la red cuando se accede a través de la interfaz web y el RACADM remoto. Cuando se utiliza este certificado, el explorador web muestra una advertencia de seguridad porque el certificado predeterminado que se emite a iDRAC no coincide con el nombre de host de iDRAC (por ejemplo, la dirección IP).

Para solucionar esta cuestión, cargue un certificado de servidor de iDRAC a la dirección IP o el nombre de host de iDRAC. Al generar la CSR (que se utiliza para emitir el certificado), asegúrese de que el nombre común (CN) de la CSR coincide con la dirección IP de iDRAC (si el certificado se ha emitido a la IP) o con el nombre DNS registrado de iDRAC (si el certificado se ha emitido al nombre registrado de iDRAC).

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

1 En la interfaz web de iDRAC, vaya a **Descripción general** > **Configuración de iDRAC** > **Red**. 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 iDRAC.

3 Haga clic en **Aplicar**.

Active Directory

Inicio de sesión fallido de Active Directory. ¿Cómo se resuelve esto?

Para diagnosticar el problema, en la página **Configuración y administración de Active Directory**, haga clic en **Probar configuración**. Revise los resultados de la prueba y corrija el problema. Cambie la configuración y ejecute la prueba hasta que el usuario supere el paso de autorización.

En general, compruebe lo siguiente:

- Al iniciar sesión, asegúrese de usar el nombre de dominio de usuario correcto y no el nombre de NetBIOS. Si tiene una cuenta de usuario de iDRAC local, inicie sesión en iDRAC usando las credenciales locales. Tras iniciar sesión, asegúrese de que:
  - La opción **Active Directory activado** está seleccionada en la página **Configuración y administración de Active Directory**.
  - La configuración de DNS se ha configurado correctamente en la página **Configuración de redes iDRAC**.

- Se ha cargado el certificado de CA raíz de Active Directory correcto en iDRAC si se ha activado la validación de certificados.
- El nombre de iDRAC y el nombre de dominio de iDRAC coinciden con la configuración del entorno de Active Directory si utiliza el esquema extendido.
- El nombre de grupo y el nombre de dominio de grupo coinciden con la configuración del entorno de Active Directory si utiliza el esquema estándar.
- Si el usuario y el objeto iDRAC se encuentran en un dominio diferente, no seleccione la opción **Dominio de usuario desde el inicio de sesión**. En cambio, seleccione la opción **Especificar un dominio** e introduzca el nombre del dominio en el que reside el objeto de iDRAC.

- Verifique los certificados SSL de la controladora de dominio para asegurarse de que la hora de iDRAC se encuentre en el plazo de vigencia del certificado.

El inicio de sesión de Active Directory falla incluso si la validación de certificados está activada. Los resultados de la prueba muestran el siguiente mensaje de error: ¿Por qué sucede esto y cómo se resuelve?

```
ERROR: Can't contact LDAP server, error:14090086:SSL
routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed: Please check the correct
Certificate Authority (CA) certificate has been uploaded to iDRAC. Please also check if the
iDRAC date is within the valid period of the certificates and if the Domain Controller Address
configured in iDRAC matches the subject of the Directory Server Certificate.
```

Si se ha activado la validación de certificados, cuando iDRAC establece la conexión SSL con el servidor de directorios, iDRAC utiliza el certificado de CA cargado para verificar el certificado de servidor de directorios. Los motivos más comunes del fallo de esta validación son los siguientes:

- La fecha de iDRAC no se encuentra en el período de validez del certificado de servidor o de CA. Compruebe la hora de iDRAC y el período de validez del certificado.
- Las direcciones de la controladora de dominio configuradas en iDRAC no coinciden con el asunto o el nombre alternativo del asunto del certificado de servidor de directorios. Si utiliza una dirección IP, lea la siguiente pregunta. Si utiliza FQDN, asegúrese de utilizar el FQDN de la controladora de dominio y no el dominio. Por ejemplo, **servername.example.com** en lugar de **example.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 la 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 la controladora de dominio. Para resolver esto, realice cualquiera de las acciones siguientes:

- Configure el nombre del host (FQDN) de la controladora de dominio como las *direcciones de controladora de dominio* en iDRAC para que coincidan con el Asunto o el Nombre alternativo del asunto del certificado del servidor.
- Vuelva a emitir el certificado del servidor de modo que use una dirección IP en el campo Asunto o Nombre alternativo del asunto y que coincida con la dirección IP configurada en iDRAC.
- Desactive la validación de certificados si prefiere confiar en esta controladora de dominio sin validación de certificados durante el protocolo de enlace SSL.

¿Cómo se configuran las direcciones de controladora de dominio cuando se utiliza el esquema extendido en un entorno de varios dominios?

Debe usar el nombre del host (FQDN) o la dirección IP de las controladoras de dominio que sirven al dominio donde reside el objeto iDRAC.

¿Cuándo deben configurarse las direcciones del catálogo global?

Si está utilizando un esquema estándar y los usuarios y grupos de roles se encuentran en dominios diferentes, las direcciones de catálogo global son necesarias. 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?

En primer lugar, el iDRAC se conecta a las direcciones configuradas de la controladora de dominio. Si el usuario y los grupos de roles se encuentran en ese dominio, se guardarán los privilegios.

Si las direcciones de la controladora global están configuradas, el iDRAC pasa a consultar el catálogo global. Si se recuperan los privilegios adicionales del catálogo global, estos privilegios se acumulan.

¿iDRAC siempre usa LDAP a través de SSL?

Sí. Todo el transporte se realiza a través del puerto seguro 636 y/o 3269. Durante la prueba de la configuración, iDRAC realiza una conexión LDAP para aislar el problema, pero no realiza un enlace LDAP en una conexión no segura.

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

iDRAC aplica una seguridad fuerte para garantizar la identidad de la controladora de dominio a la que se conecta. Sin la validación de certificados, un pirata informático podría falsificar una controladora de dominio y apropiarse de la conexión SSL. Si opta por confiar en todas las controladoras de dominio en el límite de seguridad sin activar la validación de certificados, puede desactivarla a través de la interfaz web o RACADM.

¿Admite iDRAC el nombre NetBIOS?

No en esta versión.

¿Por qué se demora hasta cuatro minutos para iniciar sesión en iDRAC mediante el inicio de sesión único de Active Directory o mediante tarjeta inteligente?

El inicio de sesión único de Active Directory o mediante tarjeta inteligente suele tardar menos de 10 segundos. Sin embargo, puede tardar hasta cuatro minutos si ha especificado el servidor DNS preferido y el servidor DNS alternativo y el primero ha fallado. Se espera que se produzcan tiempos de espera DNS cuando un servidor DNS está fuera de servicio. iDRAC le inicia la sesión mediante el servidor DNS alternativo.

Active Directory está configurado para un dominio presente en Active Directory de Windows Server 2008. Existe un dominio secundario o un subdominio para el dominio, el usuario y el grupo están presentes en el mismo dominio secundario y el usuario es miembro de este grupo. Al intentar iniciar sesión en iDRAC mediante el usuario presente en el dominio secundario, falla el inicio de sesión único de Active Directory.

Esto puede deberse a un tipo de grupo incorrecto. Hay dos tipos de grupo en el servidor de Active Directory:

- Seguridad: los grupos de seguridad permiten administrar el acceso de usuarios y equipos a los recursos compartidos y filtrar la configuración de la política de grupo.
- Distribución: los grupos de distribución tienen la finalidad de utilizarse solo como listas de distribución por correo electrónico.

Asegúrese siempre de que el tipo de grupo sea Seguridad. No es posible utilizar grupos de distribución para asignar permisos para cualquier objeto. Sin embargo, puede usarlos para filtrar la configuración de la política de grupo.

Inicio de sesión único

Se produce una falla en el inicio de sesión de SSO en el 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** para la controladora de dominio y la política de dominio.
2. Configure los equipos para que utilice el conjunto de cifrado DES-CBC-MD5.

   Esta configuración puede afectar la compatibilidad con equipos del cliente o servicios y aplicaciones de su entorno. Los tipos de cifrado de Configuración permitidos para la configuración de la directiva de Kerberos se encuentran en **Configuración del equipo** > **Configuración de seguridad** > **Directivas locales** > **Opciones de seguridad**.
3. Asegúrese de que los clientes del dominio tienen el GPO actualizado.

4 En la línea de comandos, escriba `gpupdate /force` y elimine el archivo keytab antiguo mediante el comando `klist purge`.
5 Una vez actualizado el GPO, cree el nuevo archivo keytab.
6 Cargue el archivo keytab en iDRAC.

Ahora puede iniciar sesión en el iDRAC mediante el inicio de sesión único.

¿Por qué falla el inicio de sesión único para los usuarios de Active Directory en Windows 7 y Windows Server 2008 R2?

Debe activar los tipos de cifrado para Windows 7 y Windows Server 2008 R2. Para ello:

1 Inicie sesión como administrador o como usuario con privilegios administrativos.
2 Vaya a **Inicio** y ejecute **gpedit.msc**. Aparecerá la ventana **Editor de directivas de grupo local**.
3 Vaya a **Configuración del equipo local** > **Configuración de Windows** > **Configuración de seguridad** > **Directivas locales** > **Opciones de seguridad**.
4 Haga clic con el botón derecho del mouse en **Seguridad de la red: Configuración de los tipos de cifrado permitidos para Kerberos** y seleccione **Propiedades**.
5 Active todas las opciones.
6 Haga clic en **OK** (Aceptar). Ahora puede iniciar sesión en el iDRAC mediante el inicio de sesión único.

Indique los siguientes valores adicionales para el esquema extendido:

1 En la ventana **Editor de políticas 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. Aparece la ventana del símbolo del sistema.
5 Ejecute el comando `gpupdate /force`. Se actualizan las directivas de grupo. Cierre la ventana del símbolo del sistema.
6 Vaya a **Inicio** y ejecute el comando regedit. Se mostrará la ventana **Editor del registro**.
7 Vaya a **HKEY_LOCAL_MACHINE** > **Sistema** > **CurrentControlSet** > **Control** > **LSA**.
8 En el panel derecho, haga clic con el botón derecho del mouse y seleccione **Nuevo** > **Valor DWORD (32 bits)**.
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 la ventana **Editor de registro**. Ahora puede iniciar sesión en el iDRAC mediante el inicio de sesión único.

Si ha activado el inicio de sesión único para iDRAC y está utilizando Internet Explorer para iniciar sesión en iDRAC, el inicio de sesión único falla y solicita que se introduzca el nombre de usuario y contraseña. ¿Cómo se resuelve esto?

Asegúrese de que la dirección IP de iDRAC aparezca en **Herramientas** > **Opciones de Internet** > **Seguridad** > **Sitios de confianza**. Si no aparece en la lista, el inicio de sesión único falla y se le solicita que introduzca el nombre de usuario y la contraseña. Haga clic en **Cancelar** y continúe.

Inicio de sesión mediante tarjeta inteligente

Puede tardar hasta cuatro minutos iniciar sesión en iDRAC mediante el inicio de sesión único de Active Directory o mediante tarjeta inteligente.

El inicio de sesión único de Active Directory o mediante tarjeta inteligente suele tardar menos de 10 segundos. Sin embargo, puede tardar hasta cuatro minutos si ha especificado el servidor DNS preferido y el servidor DNS alternativo en la página **Red** y el primero ha fallado. Se espera que se produzcan tiempos de espera DNS cuando un servidor DNS está fuera de servicio. iDRAC le inicia la sesión mediante el servidor DNS alternativo.

El complemento ActiveX no puede detectar el lector de tarjetas inteligentes.

Asegúrese de que la tarjeta inteligente sea 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 inteligente está bloqueada debido a demasiados intentos con un PIN incorrecto. En estos casos, entre en contacto con el emisor de la tarjeta inteligente de la organización para obtener una tarjeta nueva.

Consola virtual

¿Cuál es la versión de Java necesaria para iniciar la consola virtual?

Para usar esta función e iniciar la consola virtual de iDRAC en una red IPv6 se requiere Java 8 o superior.

La sesión de consola virtual se activa aunque se haya cerrado la sesión de la interfaz web de iDRAC. ¿Es este comportamiento 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 iDRAC 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 iDRAC active o desactive el video del servidor local?

Cualquier usuario con privilegios de configuración de iDRAC puede activar o desactivar la consola local.

¿Cómo se puede ver el estado actual del video del servidor local?

El estado se muestra en la página de la consola virtual.

Para mostrar el estado del objeto `iDRAC.VirtualConsole.AttachState`, utilice el comando siguiente:

```
racadm get idrac.virtualconsole.attachstate
```

O bien, utilice el comando siguiente desde una sesión de Telnet, SSH o remota:

```
racadm -r (iDrac IP) -u (username) -p (password) get iDRAC.VirtualConsole.AttachState
```

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 se desactiva, un punto amarillo indica que iDRAC ha bloqueado la consola local.

¿Por qué la parte inferior de la pantalla del sistema no se puede ver desde la ventana de la consola virtual?

Compruebe que la resolución del monitor de la estación de administración sea de 1280 x 1024.

¿Por qué la ventana Visor de la consola virtual está corrupta en el sistema operativo Linux?

El visor de la consola en Linux requiere un conjunto de caracteres UTF-8. Compruebe la configuración regional y restablezca el conjunto de caracteres de ser 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 sólo está disponible para el sistema operativo X-Window. En el visor de la consola virtual, realice cualquiera de las acciones siguientes:

- Vaya a la pestaña **Herramientas** > **Opciones de 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 que la opción **Cursor único** en **Herramientas** en el menú de la consola virtual de iDRAC esté seleccionada en el cliente de la consola virtual de iDRAC. El valor predeterminado es el modo de dos cursores.

¿Se puede usar un teclado o mouse al instalar el sistema operativo Microsoft de forma remota a través de la consola virtual?

No. Cuando se instala de manera remota un sistema operativo Microsoft admitido en un sistema con la consola virtual activada en el BIOS, se envía un mensaje de conexión EMS que le pide que seleccione **Aceptar** en forma remota. Debe seleccionar **Aceptar** en el sistema local o reiniciar el servidor administrado de manera remota, volver a instalar y, a continuación, 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, apague siempre la consola virtual en la utilidad de configuración de iDRAC antes de instalar un sistema operativo de manera remota.

¿Por qué el indicador Bloq Num en la estación de administración no refleja el estado de Bloq Num en el servidor remoto?

Al acceder a través de iDRAC, el indicador Bloq Num en la estación de administración no coincide necesariamente con el estado de Bloq Num en el servidor remoto. El estado de Bloq Num depende de la configuración del servidor remoto cuando se establece la sesión remota, independientemente del estado de Bloq Num en 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?

No. 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 debido a que el complemento Consola virtual de iDRAC no recibe el video de escritorio del servidor remoto. Por lo general, este comportamiento se produce cuando el servidor remoto está apagado. Ocasionalmente, el mensaje puede aparecer debido a un mal funcionamiento de la recepción de video de 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 video está fuera del alcance de captura de video de iDRAC. Parámetros como resolución de visualización o tasa de actualización muy elevada provocan una condición de fuera de alcance. Generalmente, limitaciones físicas, tal como el tamaño de la memoria de video o el ancho de banda, establecen el alcance máximo de los parámetros.

Cuando se inicia una sesión de consola virtual en la interfaz web de iDRAC, ¿por qué aparece una ventana emergente sobre la seguridad de ActiveX?

Es posible que el iDRAC no se encuentre en una lista de sitios de confianza. Para evitar que aparezca la ventana emergente sobre la seguridad cada vez que inicie una sesión de consola virtual, agregue iDRAC a la lista de sitios de confianza en el explorador del cliente:

1 Seleccione **Herramientas** > **Opciones de Internet** > **Seguridad** > **Sitios de confianza**.
2 Haga clic en **Sitios** e introduzca la dirección IP o el nombre DNS de iDRAC.
3 Haga clic en **Add** (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. Debido a su diseño, el mouse PS/2 utiliza la posición relativa para el apuntador del mouse, lo que ocasiona un retraso en la sincronización. El iDRAC tiene un controlador de mouse USB, lo que permite una posición absoluta y un seguimiento más cercano del puntero del mouse. Incluso si iDRAC pasa 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/Diagnóstico 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 se produce si el **Modo de mouse** se establece en **USC/Diagnóstico**. Pulse la tecla de acceso rápido **Alt + M** para utilizar el mouse en el sistema local. Pulse **Alt + M** nuevamente para utilizar el mouse en el Consola virtual.

Cuando la interfaz web de iDRAC se inicia desde la interfaz web de CMC poco después de haberse iniciado la consola virtual, ¿por qué se agota el tiempo de espera de la sesión de la GUI?

Al iniciar la consola virtual en iDRAC desde la interfaz web de CMC, se abre una ventana emergente para iniciar la consola virtual. Esta ventana se cierra poco después de abrirse la consola virtual.

Al iniciar la GUI y la consola virtual en el mismo sistema iDRAC en una estación de administración, se agota el tiempo de espera de la sesión de la GUI de iDRAC si la GUI se inicia antes de que se cierre la ventana emergente. Si la GUI de iDRAC se inicia desde la interfaz web de CMC después de que se cierre la ventana emergente de la consola virtual, este 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 **Imprimir pantalla** y suéltela mientras mantiene presionadas las teclas **Ctrl** y **Alt**. Para enviar la clave SysRq a un servidor Linux remoto a través de iDRAC con 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. La duración es más larga para las tarjetas de 10 Gb y también puede ser excepcionalmente larga si el conmutador de red conectado tiene activado el Protocolo de árbol de expansión (STP). En este caso, se recomienda activar "portfast" para el puerto del conmutador conectado al servidor. En la mayoría de los casos, la consola virtual se restablece sola.

Medios virtuales

¿Por qué a veces se interrumpe la conexión del cliente de medios virtuales?

Cuando se agota el tiempo de espera de la red, el firmware de iDRAC abandona la conexión y desconecta el vínculo entre el servidor y la unidad virtual.

Si cambia el CD en el sistema cliente, es posible que el nuevo CD tenga una función de inicio automático. En dicho caso, el tiempo de espera del firmware puede agotarse y puede que se pierda la conexión si el sistema cliente demora mucho tiempo en leer el CD. Si una conexión se interrumpe, vuelva a conectarse desde la GUI y siga con la operación anterior.

Si los valores de configuración de los medios virtuales se cambian en la interfaz web de iDRAC o mediante los comandos de RACADM local, se desconectarán todos los medios conectados en el momento de aplicar el cambio de configuración.

Para volver a conectar la unidad virtual, utilice la ventana **Vista del cliente** de los medios virtuales.

¿Por qué una instalación del sistema operativo Windows a través de medios virtuales lleva mucho tiempo?

Si instala el sistema operativo Windows mediante el DVD *Herramientas y documentación de Dell Systems Management* y la conexión de red es lenta, el procedimiento de instalación puede demorar más tiempo en acceder a la interfaz web de iDRAC debido a la latencia de red. La ventana de instalación no indica el progreso de instalación.

¿Cómo se configura el dispositivo virtual como dispositivo de inicio?

En el sistema administrado, acceda a la configuración del BIOS y vaya al menú de inicio. Busque el CD virtual, el disco flexible virtual o la tarjeta vFlash y cambie el orden de inicio de los dispositivos según sea necesario. Asimismo, presione la barra espaciadora en la secuencia de inicio de la configuración de CMOS para que el dispositivo virtual pueda iniciarse. Por ejemplo, para iniciar desde una unidad de CD, configure la unidad de CD como el primer dispositivo en el orden de inicio.

¿Cuáles son los tipos de medios que se pueden configurar como disco de inicio?

iDRAC permite iniciar a partir de los siguientes medios de inicio:

- Medios de CDROM/DVD de datos

- Imagen ISO 9660
- Imagen de disco flexible o disco flexible de 1,44
- Una memoria USB a la que el sistema operativo reconoce como disco extraíble
- Una imagen de memoria USB

¿Cómo se configura el dispositivo USB como dispositivo de inicio?

También puede iniciar con un disco de inicio de Windows 98 y copiar los archivos de sistema del disco de inicio al dispositivo USB. Por ejemplo, en el símbolo del sistema, escriba el siguiente comando:

```
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 al 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 esto?

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 del 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 "Virtual Floppy" /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 "Virtual CD" /var/log/messages
```
2 Busque la última entrada de dicho mensaje y anote la hora.
3 En la línea de comandos de Linux, ejecute el siguiente comando:
```
grep "hh:mm:ss" /var/log/messages
```
hh:mm:ss es la fecha y hora del mensaje que devuelve el comando grep en el paso 1.
4 En el paso 3, lea el resultado del comando grep y busque el nombre del dispositivo que se asignó a *CD virtual* de Dell.
5 Asegúrese de que la unidad de CD virtual está conectada.
6 En la línea de comandos de Linux, ejecute el siguiente comando:
```
mount /dev/sdx /mnt/CD
```
donde, `/dev/sdx` es el nombre de dispositivo que se encuentra en el paso 4 y `/mnt/floppy` es el punto de montaje.

¿Por qué las unidades virtuales conectadas al servidor que se quita después de realizar una actualización remota del firmware mediante la interfaz web de iDRAC?

Las actualizaciones del firmware restablecen el iDRAC y hacen que este interrumpa la conexión remota y desmonte las unidades virtuales. Las unidades vuelven a aparecer una vez finalizado el restablecimiento de iDRAC.

¿Por qué todos los dispositivos USB se desconectan después de conectar un dispositivo USB?

Los dispositivos de medios virtuales y los dispositivos vFlash se conectan como un dispositivo USB compuesto al BUS de USB del host y comparten un puerto USB común. Cuando se conectan o desconectan dispositivos de medios virtuales o USB vFlash del bus de USB del host, se desconectan temporalmente todos los dispositivos de medios virtuales y vFlash del bus de USB del host y luego se vuelven a conectar. Si el sistema operativo del host utiliza un dispositivo de medios virtuales, no conecte ni desconecte uno o más dispositivos de medios virtuales o vFlash. Se recomienda conectar primero todos los dispositivos USB necesarios antes de utilizarlos.

¿Qué hace la opción Restablecer USB?

Restablece los dispositivos USB remotos y locales conectados al servidor.

¿Cómo se maximiza el rendimiento de los medios virtuales?

Para maximizar el rendimiento de los medios virtuales, inicie estos últimos con la consola virtual desactivada o realice una de las acciones siguientes:

- Cambie el control deslizante de rendimiento a la velocidad máxima.
- Desactive el cifrado tanto para los medios virtuales como para la consola virtual.

  NOTA: En este caso, la transferencia de datos entre el servidor administrado y el iDRAC para los medios virtuales y la consola virtual no estará protegida.
- Si utiliza cualquiera de los sistemas operativos de Windows Server, detenga 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 **Recopilador de sucesos de Windows** y, a continuación, 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.

Autentificación de SNMP

¿Por qué se muestra el mensaje 'Acceso remoto: error de autentificación SNMP'?

Como parte del descubrimiento, IT Assistant intenta verificar los nombres de la comunidad Obtener y Establecer del dispositivo. En IT Assistant, usted tiene el nombre de la comunidad Obtener = público y el nombre de la comunidad Establecer = privado. De manera predeterminada, el nombre de comunidad del agente SNMP para el agente de iDRAC es público. Cuando IT Assistant envía una solicitud de Establecer, el agente de iDRAC genera un error de autentificación SNMP porque acepta solicitudes solamente de la comunidad = público.

Para evitar la generación de errores de autentificación SNMP, debe introducir nombres de comunidad aceptados por el agente. Dado que iDRAC solo permite un nombre de comunidad, deberá utilizar el mismo nombre de comunidad Establecer y Obtener para la configuración de descubrimiento de IT Assistant.

Dispositivos de almacenamiento

La información para todos los dispositivos de almacenamiento conectados al sistema no se muestra y OpenManage Storage Management muestra un mayor número de dispositivos de almacenamiento que iDRAC. ¿Por qué?

iDRAC muestra información solamente para los dispositivos capacidad CEM (administración incorporada completa).

Módulo de servicios de iDRAC

Antes de instalar o ejecutar el módulo de servicio de iDRAC, ¿es necesario desinstalar Open Manage Server Administrator?

No, no es necesario desinstalar Server Administrator. Antes de instalar o ejecutar el Módulo de servicios de iDRAC, asegúrese de que haya detenido las funciones de Server Administrator que proporciona el Módulo de servicios de iDRAC.

¿Cómo se verifica si el módulo de servicio de iDRAC está instalado en el sistema?

Para saber si el módulo de servicio de iDRAC está instalado en el sistema:

- En los sistemas que ejecutan Windows
  Abra el **Panel de control**, verifique si el módulo de servicio de iDRAC figura en la lista de programas instalados que aparece en pantalla.
- En sistemas que ejecutan Linux
  Ejecute el comando `rpm –qi dcism` Si el Módulo de servicios de iDRAC está instalado, el estado que se muestra será **instalado**.

NOTA: Para verificar si el Módulo de servicios de iDRAC está instalado en Red Hat Enterprise Linux 7, use el comando `systemctl status dcismeng.service` en lugar del comando `init.d`.

¿Cómo se verifica el número de versión del módulo de servicio de iDRAC que se encuentra instalado en el sistema?

Para comprobar la versión del módulo de servicio de iDRAC en el sistema, realice cualquiera de las acciones siguientes:

- Haga clic en **Inicio** > **Panel de control** > **Programas y funciones**. La versión del Módulo de servicios de iDRAC instalado aparece en la pestaña **Versión**.
- Vaya a **Mi PC** > **Desinstalar o cambiar un programa**.

¿Cuál es el nivel de permisos mínimo necesario para instalar el módulo de servicio del iDRAC?

Para instalar el módulo de servicio de iDRAC, es necesario tener privilegios de nivel de administrador.

En el Módulo de servicios de iDRAC Versión 2.0 y anteriores, al instalar el Módulo de servicios de iDRAC, se mostrará un mensaje de error que indica que no se admite este servidor. Ya consulté la Guía del usuario para obtener información adicional sobre los servidores admitidos. ¿Cómo se resuelve el error?

Antes de instalar el Módulo de servicios de iDRAC, asegúrese de que el servidor sea un servidor PowerEdge de 12a generación o posterior. Asimismo, asegúrese de que dispone de un sistema de 64 bits.

Se muestra el siguiente mensaje en el registro del sistema operativo, incluso cuando el paso directo de sistema operativo a iDRAC mediante USBNIC se ha configurado correctamente. ¿Por qué?

The iDRAC Service Module is unable to communicate with iDRAC using the OS to iDRAC Pass-through channel

El Módulo de servicios de iDRAC utiliza la función de paso directo de sistema operativo a iDRAC por medio de la NIC de USB para establecer la comunicación con iDRAC. A veces, la comunicación no se establece aunque la interfaz de la NIC de USB esté configurada con los puntos finales de IP correctos. Esto puede ocurrir cuando la tabla de enrutamiento del sistema operativo del host contiene varias entradas para la misma máscara de destino y el destino de la NIC de USB de destino no aparece como el primero en el orden de enrutamiento.

Destination	Puerta de enlace	Máscara de red de destino	Indicadores	Métrica	Ref.	Usar Iface
Predeterminado	10.94.148.1	0.0.0.0	UG	1 024	0	0 em1
10.94.148.0	0.0.0.0	255.255.255.0	U	0	0	0 em1
vínculo local	0.0.0.0	255.255.255.0	U	0	0	0 em1
vínculo local	0.0.0.0	255.255.255.0	U	0	0	0 enp0s20u12u3

En el ejemplo, **enp0s20u12u3** es la interfaz de la NIC de USB. La máscara de destino del vínculo local se repite y la NIC de USB no es la primera en el orden. Esto genera el problema de conectividad entre el Módulo de servicios de iDRAC e iDRAC mediante el paso directo de sistema operativo a iDRAC. Para solucionar el problema de conectividad, asegúrese de que la dirección IPv4 de la NIC de USB de iDRAC (el valor predeterminado es 169.254.0.1) sea accesible desde el sistema operativo del host.

Caso contrario:

- Cambie la dirección de la NIC de USB de iDRAC en una máscara de destino única.
- Elimine las entradas que no son necesarias de la tabla de enrutamiento a fin de asegurarse de que la NIC de USB quede seleccionada por ruta cuando el host desea alcanzar la dirección IPv4 de la NIC de USB de iDRAC.

En el Módulo de servicios de iDRAC Versión 2.0 y anteriores, cuando desinstale el Módulo de servicios de iDRAC desde un servidor VMware ESXi, el conmutador virtual se denomina vSwitchiDRACvusb y el grupo de puertos se denomina Red de iDRAC en el cliente vSphere. ¿Cómo se deben borrar?

Mientras se instala el VIB del Módulo de servicios de iDRAC en un servidor VMware ESXi, el Módulo de servicios de iDRAC crea vSwtich y Portgroup para comunicarse con iDRAC a través del paso directo de sistema operativo a iDRAC en el modo NIC de USB. Después de la desinstalación, el conmutador virtual **vSwitchiDRACvusb** y el grupo de puertos **Red de iDRAC** no se eliminan. Para borrarlo manualmente, realice uno de los siguientes pasos:

- Vaya al asistente de configuración de vSphere Client y elimine las entradas.
- Vaya a Esxcli y escriba los comandos siguientes:
  - Para eliminar el grupo de puertos: `esxcfg-vmknic -d -p "iDRAC Network"`
  - Para eliminar el vSwitch: `esxcfg-vswitch -d vSwitchiDRACvusb`

NOTA: Es posible volver a instalar el módulo de servicio de iDRAC en el servidor Vmware ESXi, ya que esto no es un problema funcional para el servidor.

¿En qué parte del sistema operativo se encuentra disponible el registro de LifeCycle replicado?

Para ver los registros de Lifecycle replicados:

Sistema operativo	Ubicación
Microsoft Windows	**Visor de sucesos** > **Registros de Windows** > **Sistema**. Todos los registros de Lifecycle del Módulo de servicios de iDRAC se replican bajo el nombre de origen **Módulo de servicios de iDRAC**. **NOTA: En iSM Versión 2.1 y versiones posteriores, los registros de Lifecycle se replican bajo el nombre de origen del registro de Lifecycle Controller. En iSM Versión 2.0 y versiones anteriores, los registros se replican bajo el nombre de origen del Módulo de servicios de iDRAC.** **NOTA: La ubicación del registro de Lifecycle se puede configurar mediante el instalador del Módulo de servicios de iDRAC. Puede configurar la ubicación al instalar el Módulo de servicios de iDRAC o al modificar el instalador.**
Red Hat Enterprise Linux , SUSE Linux, CentOS y Citrix XenServer	/var/log/messages

Sistema operativo	Ubicación
VMware ESXi	/var/log/syslog.log

¿Cuáles son los paquetes o ejecutables dependientes de Linux disponibles para la instalación mientras se completa la instalación en Linux?

Para ver la lista de paquetes dependientes de Linux, consulte la sección *Dependencias de Linux* en *iDRAC Service Module Installation Guide* (Guía de instalación del módulo de servicio de iDRAC).

RACADM

Después de realizar un restablecimiento de iDRAC (mediante el comando racreset de RACADM), si se emite algún comando, aparece el mensaje siguiente. ¿Qué significa esto?

```
ERROR: Unable to connect to RAC at specified IP address
```

El mensaje indica que antes de emitir otro comando, debe esperar hasta que iDRAC complete el restablecimiento.

Al utilizar comandos y subcomandos de RACADM, algunos errores no quedan claros.

Es posible que reciba uno o más de los siguientes errores cuando use los comandos de RACADM:

- Mensajes de error de RACADM local: problemas de sintaxis, errores tipográficos, nombres incorrectos, etc.
- Mensajes de error de RACADM remota: problemas como, por ejemplo, una dirección IP, un nombre de usuario o una contraseña incorrectos.

Durante una prueba de ping a iDRAC, si el modo de red cambia del modo Dedicado al modo Compartido, no hay respuesta de ping.

Borre la tabla ARP en el sistema.

RACADM remoto no se puede conectar a iDRAC desde SUSE Linux Enterprise Server (SLES) 11 SP1.

Asegúrese de que están instaladas las versiones oficiales de openssl y libopenssl. Ejecute el siguiente comando para instalar los paquetes RPM:

```
rpm -ivh --force < filename >
```

donde `filename` es el archivo de los paquetes openssl o libopenssl.

Por ejemplo:

```
rpm -ivh --force openssl-0.9.8h-30.22.21.1.x86_64.rpm
rpm -ivh --force libopenssl0_9_8-0.9.8h-30.22.21.1.x86_64.rpm
```

¿Por qué no están disponibles RACADM remoto y los servicios web después de un cambio de propiedad?

Es posible que los servicios de RACADM remota y la interfaz web tarden un poco en estar disponibles después de restablecer el servidor web de iDRAC.

El servidor web iDRAC se restablece en los casos siguientes:

- Cuando la configuración de la red o las propiedades de seguridad de la red se cambian mediante la interfaz web de usuario de iDRAC.
- Se cambia la propiedad iDRAC.Webserver.HttpsPort, inclusive cuando un `racadm set -f <config file>` la cambia.
- Se utiliza el comando racresetcfg.
- iDRAC se restablece.
- Se carga un nuevo certificado del servidor SSL.

¿Por qué se muestra un mensaje de error si se intenta eliminar una partición después de crearla mediante RACADM local?

Esto sucede porque la operación de creación de partición está en curso. Sin embargo, la partición se elimina después de cierto tiempo y aparece 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.

Configuración permanente de la contraseña predeterminada como calvin

Si su sistema se entregó con una contraseña única de iDRAC predeterminada pero desea establecer *calvin* como la contraseña predeterminada, debe utilizar los puentes disponibles en la placa del sistema.

PRECAUCIÓN: Al cambiar la configuración de los puentes en forma permanente, se cambia la contraseña predeterminada a *calvin.* No se podrá volver a la contraseña única incluso si se restablece el iDRAC a la configuración predeterminada de fábrica.

Para obtener más información sobre la ubicación del puente y el procedimiento, consulte la documentación para su servidor en **dell.com/support/manuals**.

Varios

Cuando se instala un sistema operativo, el nombre del host puede aparecer/cambiarse automáticamente como no.

Hay dos escenarios posibles:

- Escenario 1: el iDRAC no muestra el último nombre del host una vez que instala un sistema operativo. Necesita instalar OMSA o iSM junto con el iDRAC para reflejar el nombre del host.
- Escenario 2: el iDRAC tenía un nombre de host para un sistema operativo específico y se ha instalado un sistema operativo diferente. Aun así, el nombre del host aparece como el nombre del host anterior sin sobrescribir el nombre del host. El motivo es que el nombre del host es una información que proviene del sistema operativo, el iDRAC sólo guarda la información. Si se ha instalado un nuevo sistema operativo, el iDRAC no restablece el valor del nombre del host. Sin embargo, las versiones más recientes de los sistemas operativos son capaces de actualizar el nombre del host en iDRAC durante el primer inicio del sistema operativo.

¿Cómo se busca una dirección IP de iDRAC para un servidor Blade?

NOTA: La opción Chassis Management Controller (CMC) está disponible solamente para los servidores blade.

- **Mediante el uso de la interfaz web del CMC**:
  Vaya a **Chasis** > **Servidores** > **Configuración** > **Implementar**. En la tabla que se muestra, observe la dirección IP del servidor.
- **Uso de la consola virtual**: reinicie el servidor para ver la dirección IP de iDRAC durante la POST. Seleccione la consola "Dell CMC" en OSCAR para iniciar sesión en el CMC por medio de una conexión de serie local. Los comandos RACADM de CMC se pueden enviar desde esta conexión.
  Para obtener más información sobre los comandos de CMC RACADM, consulte *CMC RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos de CMC RACADM), disponible en **dell.com/esmmanuals**.

  Para obtener más información sobre los comandos de iDRAC RACADM, consulte *iDRAC RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC), disponible en **dell.com/idracmanuals**.
- **Mediante el uso del 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 el uso de 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?

- **Desde la interfaz web de iDRAC**:
  Vaya a **Configuración de iDRAC** > **CMC**. La página **Resumen de CMC** muestra la dirección IP de CMC.
- **Desde la consola virtual**:
  Seleccione la consola "Dell CMC" en OSCAR para iniciar sesión en el CMC por medio de una conexión de serie local. Los comandos RACADM de CMC se pueden enviar desde esta conexión.

```
$ 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.

Para obtener más información sobre los comandos de CMC RACADM, consulte *CMC RACADM Command Line Interface Reference Guide* (Guía de referencia de la interfaz de línea de comandos de CMC RACADM), disponible en **dell.com/esmmanuals**.

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

¿Cómo se busca una dirección IP de iDRAC para un servidor tipo bastidor o torre?

- **Desde la interfaz web de iDRAC**:
  Vaya a **Sistema** > **Detalles** > **Detalles de iDRAC**. La página **Detalles de iDRAC** muestra la dirección IP de iDRAC.
- **Desde el RACADM local**:
  Utilice el comando racadm getsysinfo.
- **Desde el LCD**:
  En el servidor físico, utilice los botones de navegación en el panel LCD para ver la dirección IP de iDRAC. Vaya a **Vista de configuración** > **Vista** > **IP de iDRAC** > **IPv4** o **IPv6** > **IP**.
- **Desde OpenManage Server Administrator**:
  En la interfaz web de Server Administrator, vaya a **Gabinete modular** > **Módulo de sistema/servidor** > **Chasis del sistema principal/sistema principal** > **Acceso remoto**.

La conexión de red de iDRAC no funciona.

Servidores Blade:

- Asegúrese de que el cable de LAN esté conectado al CMC.
- Asegúrese de que esté activada en el sistema la configuración de NIC, la de IPv4 o IPv6, y que además esté activada la modalidad estática o DHCP.

Servidores tipo bastidor y torre:

- En el modo compartido, asegúrese de que el cable de LAN esté conectado al puerto NIC donde aparezca el símbolo de llave inglesa.
- En el modo dedicado, asegúrese de que el cable de LAN esté conectado al puerto LAN de iDRAC.
- Asegúrese de que esté activada en el sistema la configuración de NIC, la de IPv4 e IPv6, y que además esté activada la modalidad estática o DHCP.

El servidor Blade se ha insertado en el chasis y se ha presionado el interruptor de corriente, pero el servidor no se encendió.

- iDRAC requiere hasta dos minutos para inicializar antes de que el servidor pueda encenderse.
- Compruebe el presupuesto de alimentación de CMC. Es posible que se haya sobrepasado el presupuesto de alimentación del chasis.

¿Cómo se recupera el nombre de usuario y la contraseña de usuario administrativo de iDRAC?

Debe restaurar el iDRAC a sus valores predeterminados. Para obtener más información, consulte Restablecimiento de iDRAC a los valores predeterminados de fábrica.

¿Cómo se cambia el nombre de la ranura para el sistema en un chasis?

1 Inicie sesión en la interfaz web de la CMC y vaya a **Chasis** > **Servidores** > **Configuración**.
2 Introduzca el nuevo nombre para la ranura en la fila del servidor y haga clic en **Aplicar**.

iDRAC en el servidor blade no responde durante el inicio.

Extraiga y vuelva a insertar el servidor.

Compruebe la interfaz web de la CMC para ver si iDRAC se muestra como componente que se puede actualizar. De ser así, siga las instrucciones en Actualización del firmware mediante la interfaz web de la CMC.

Consulte la documentación del producto para seleccionar un método de contacto conveniente.

Cuando se intenta iniciar el servidor administrado, el indicador de alimentación es de color verde, pero no hay POST ni video.

Esto sucede debido a cualquiera de las condiciones siguientes:

- La memoria no está instalada o no se puede acceder a ella.
- La CPU no está instalada o no se puede acceder a ella.
- Falta la tarjeta vertical de video o esta no está conectada correctamente.

Asimismo, consulte los mensajes de error del registro de iDRAC mediante la interfaz web de iDRAC o desde el panel LCD del servidor.

29

Situaciones 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.

Temas:

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 solucionar problemas y poner el servidor en servicio mediante iDRAC.

Antes de realizar la solución de problemas de un servidor inaccesible, asegúrese de que se cumplan los siguientes prerrequisitos:

- Activación de la última pantalla de último bloqueo
- Activación de las alertas en iDRAC

Para identificar la causa, compruebe lo siguiente en la interfaz web de iDRAC y restablezca la conexión al sistema:

NOTA: Si no puede acceder a la interfaz web de iDRAC, vaya al servidor, acceda al panel LCD, escriba la dirección IP o el nombre de host y luego realice las siguientes operaciones mediante la interfaz web del iDRAC desde su estación de administración:

- Estado del LED del servidor: parpadea en color ámbar o permanece sólido en ámbar.
- Estado del LCD del panel anterior o mensaje de error: color ámbar del LCD o mensaje de error.
- La imagen del sistema operativo se muestra en la consola virtual. Si puede ver la imagen, restablezca el sistema (inicio en caliente) y vuelva a iniciar sesión. Si puede iniciar sesión, el problema está solucionado.
- Pantalla de último bloqueo.
- Video de captura de inicio.
- Video de captura de error.
- Estado de condición del sistema: iconos *x* rojos para los componentes del sistema con error.

- Estado de la matriz de almacenamiento: matriz posiblemente fuera de línea o con error.
- Registro de Lifecycle para sucesos críticos relacionados con el hardware y el firmware del sistema y las entradas del registro grabadas en el momento del error del sistema.
- Genere un informe de asistencia técnica y vea los datos recopilados.
- Utilizar funciones de supervisión proporcionadas por el módulo de servicio de iDRAC

Obtención de la información del sistema y evaluación de la condición del sistema

Para obtener la información del sistema y evaluación de la condición del sistema:

- En la interfaz web de iDRAC, vaya a **Descripción general** > **Resumen** para ver la información del sistema y acceder a los distintos enlaces de esta página para evaluar la condición del sistema. Por ejemplo, puede comprobar la condición del ventilador del chasis.
- También puede configurar el LED de localización del chasis y, en función del color, evaluar la condición del sistema.
- Si el módulo de servicio del iDRAC está instalado, se muestra la información del host del sistema operativo.

Establecimiento de alertas y configuración de alertas por correo electrónico

Para establecer alertas y configurar alertas por correo electrónico:

1 Active las alertas.
2 Configure la alerta por correo electrónico y compruebe los puertos.
3 Realice un reinicio, un apagado o un ciclo de encendido del sistema administrado.
4 Envíe una alerta de prueba.

Visualización y exportación del Registro de sucesos del sistema y el Registro de Lifecycle

Para ver y exportar el registro de lifecycle y el registro de sucesos del sistema (SEL):

1 En la interfaz web de iDRAC, vaya a **Mantenimiento** > **Registro de sucesos del sistema** para ver SEL y **Registros de Lifecycle** para ver el registro de Lifecycle.

> **NOTA: El SEL también se graba en el registro de Lifecycle. Mediante las opciones de filtrado para ver el SEL.**

2 Exporte el SEL o el registro de Lifecycle en el formato XML a una ubicación externa (estación de administración, USB, recurso compartido de red, etc.). Como alternativa, puede activar el registro de sistema remoto de modo que todos los registros que se graban en el registro de Lifecycle también se escriban simultáneamente en los servidores remotos configurados.
3 Si está utilizando el módulo de servicio del iDRAC, exporte el registro de Lifecycle al registro del sistema operativo.

Interfaces para actualizar el firmware de iDRAC

Utilice las interfaces siguientes para actualizar el firmware de iDRAC:

- Interfaz web del iDRAC
- API de Redfish
- CLI de RACADM (iDRAC y CMC)
- Dell Update Package (DUP)
- Interfaz web del CMC

- Lifecycle Controller–Remote Services
- Lifecycle Controller
- Dell Remote Access Configuration Tool (DRACT)

Realización de un apagado ordenado del sistema

Para realizar un apagado ordenado, vaya a una de las ubicaciones siguientes en la interfaz web de iDRAC:

- En **Panel**, seleccione **Apagado ordenado** y, a continuación, haga clic en **Aplicar**.

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

Creación de una nueva cuenta de usuario de administrador

Puede modificar la cuenta de usuario de administrador local predeterminada o crear una nueva cuenta de usuario de administrador. Para modificar la cuenta de usuario de administrador local, consulte Modificación de la configuración de la cuenta de administrador local.

Para crear una cuenta de usuario de administrador nueva, consulte las secciones siguientes:

- Configuración de usuarios locales
- Configuración de usuarios de Active Directory
- Configuración de los usuarios LDAP genéricos

Inicio de la consola remota de servidores y montaje de una unidad USB

Para iniciar la consola remota de servidores y montaje de una unidad USB:

1 Conecte una unidad flash USB (con la imagen necesaria) a una estación de administración.
2 Utilice uno de los métodos siguientes para iniciar la consola virtual a través de la interfaz web de iDRAC:
   - Vaya a **Panel** > **Consola virtual** y haga clic en **Iniciar consola virtual**.

   Se muestra el **Vista previa de consola virtual**.
3 En el menú **Archivo**, haga clic en **Medios virtuales** > **Iniciar medios virtuales**.
4 Haga clic en **Agregar imagen** y seleccione la imagen situada en la unidad flash USB.
   La imagen se agrega a la lista de unidades disponibles.
5 Seleccione la unidad para asignarla. La imagen de la unidad flash USB se asigna al sistema administrado.

Instalación del sistema operativo básico conectado a los medios virtuales y los recursos compartidos de archivos remotos

Para ello, consulte Implementación del sistema operativo mediante recurso compartido de archivos remotos.

Administración de la densidad de bastidor

Supongamos que se han instalado dos servidores en un bastidor. Para agregar dos servidores adicionales, se debe determinar cuánta capacidad queda en el bastidor.

Para evaluar la capacidad de un bastidor con el fin de agregar servidores adicionales:

1 Consulte los datos de consumo de alimentación actuales y los históricos de los servidores.
2 Según los datos, la infraestructura de alimentación y las limitaciones del sistema de refrigeración, active la política de límites de alimentación y establezca los valores de los límites.

> **NOTA: Es recomendable establecer una limitación cercana al pico y luego utilizar ese nivel de limitación para determinar cuánta capacidad queda en el bastidor para la adición de servidores adicionales.**

Instalación de una nueva licencia electrónica

Para obtener más información, consulte Operaciones de licencia.

Aplicación de valores de configuración de la identidad de E/S para varias tarjetas de red en un reinicio del sistema host individual

Si tiene varias tarjetas de red en un servidor que es parte de un entorno de red de área de almacenamiento (SAN) y desea aplicar distintas direcciones virtuales y valores de configuración de iniciador y destino para dichas tarjetas, utilice la función Optimización de la identidad de E/S para reducir el tiempo de configuración de los valores. Para hacerlo:

1 Asegúrese de que el BIOS, el iDRAC y las tarjetas de red están actualizadas a la versión de firmware más reciente.
2 Active la Optimización de la identidad de E/S.
3 Exporte el archivo de configuración XML desde el iDRAC.
4 Edite los valores de configuración de la optimización de la identidad de E/S en el archivo XML.
5 Importe el archivo de configuración XML al iDRAC.