Integrated Dell Remote Access Controller 9 User's Guide

June 2021
Rev. A01

Notas, precauciones y advertencias

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.

Contents

1

Descripción general de iDRAC

La Integrated Dell Remote Access Controller (iDRAC) está diseñada para aumentar su productividad como administrador del sistema y mejorar la disponibilidad general de los servidores Dell EMC. iDRAC envía alertas sobre problemas del sistema, lo ayuda a realizar actividades de administración remota y reduce la necesidad de acceso físico al sistema.

La tecnología iDRAC es parte de una solución de centro de datos más grande que aumenta la disponibilidad de aplicaciones y cargas de trabajo críticas del negocio. La tecnología le permite implementar, controlar, administrar, configurar y actualizar los sistemas Dell EMC, además de solucionar problemas sobre ellos, desde cualquier ubicación, sin utilizar agentes ni sistemas operativos.

Varios productos funcionan con iDRAC para simplificar y agilizar las operaciones de TI. A continuación, se indican algunos de las herramientas:

- OpenManage Enterprise
- Complemento Power Center para OpenManage
- OpenManage Integration para VMware vCenter
- Dell Repository Manager

iDRAC está disponible en las variantes siguientes:

- iDRAC Basic: disponible de manera predeterminada para los servidores serie 100 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
- iDRAC Datacenter: disponible en todos los modelos de servidores

Temas:

Ventajas de utilizar iDRAC

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 integrada a través de Lifecycle Controller: Lifecycle Controller proporciona capacidades de implementación y facilidad de reparación simplificada a través de la GUI de Lifecycle Controller para la implementación local

y las interfaces de servicios remotos (WSMan) para la implementación remota incorporada en Dell OpenManage Essentials y consolas de partners.

Para obtener más información sobre la interfaz gráfica de usuario de Lifecycle Controller, consulte *Guía del usuario de Lifecycle Controller* y para obtener información sobre los servicios remotos, consulte *Guía de inicio rápido de servicios remotos de Lifecycle Controller.* disponible en https://www.dell.com/idracmanuals.

Funciones clave

Entre las funciones clave de iDRAC, se incluyen las siguientes:

NOTA: Algunas funciones solamente están disponibles con la licencia de iDRAC Enterprise o Datacenter. Para obtener información sobre las funciones disponibles para una licencia, consulte Licencias de la iDRAC en la página 21.

Inventario y supervisión

- Streaming de datos de telemetría.
- 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.
- En el caso de los servidores blade: inicie la interfaz web del módulo de administración, vea la información modular de OpenManage Enterprise (OME) y las 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 *Guía del usuario de la controladora de administración del chasis* disponible en https://www.dell.com/cmcmanuals.
- Visualización de las interfaces de red disponibles en los sistemas operativos host
- iDRAC9 proporciona supervisión y funcionalidad de administración mejoradas con Quick Sync 2. Debe tener 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 utilizando recursos compartidos de archivos remotos y medios virtuales.
- Activación del descubrimiento automático
- Configuración del servidor con la función de exportación o importación del perfil JSON o XML mediante RACADM, WSMan y Redfish. Para obtener más información, consulte *Guía de inicio rápido de servicios remotos de Lifecycle Controller* disponible en https://www.dell.com/idracmanuals.
- 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
- 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 videos 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.
    - Automatice las opciones de recuperación del sistema.
    - Activar o desactivar el estado de ciclo de encendido completo de 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).
    - Realice una integración con una recopilación de SupportAssist. Esto se aplica únicamente si se ha instalado el módulo de servicio de iDRAC versión 2.0 o posterior.
- 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.

Prácticas recomendadas de Dell referidas al iDRAC

- Las iDRAC de Dell están diseñadas para estar en una red de administración independiente, no están diseñadas ni destinadas a que se agreguen ni conecten directamente a Internet. Si lo hace, es posible que se exponga el sistema conectado a problemas de seguridad y otros riesgos de los cuales Dell no es responsable.
- Dell EMC recomienda utilizar el puerto Gigabit Ethernet dedicado disponible en servidores tipo bastidor y torre. 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. La opción Dedicado permite asignar una dirección IP a la iDRAC a partir de la misma subred o de una distinta en comparación con las direcciones IP asignadas a las LOM o las NIC del host para administrar el tráfico de red.

- 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
- Autenticación de dos factores mediante la función de inicio de sesión de tarjeta inteligente. La autenticación de dos factores se basa en la tarjeta inteligente física y el PIN de la tarjeta inteligente.
- 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 utilizar 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.
- Configuración del tiempo de espera de la sesión (en segundos)
- Puertos IP configurables (para HTTP, HTTPS, SSH, consola virtual y medios virtuales).
- 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).

Nuevas funciones agregadas

En esta sección, se proporciona la lista de nuevas funciones agregadas en las siguientes versiones:

Firmware version 5.00.00.00

This release includes all the features from the previous releases. Following are the new features that are added in this release:

NOTE: For information about supported systems, refer to the respective version of Release Notes available at https://www.dell.com/support/article/sln308699 .

In 5.00.00.00 release, following features are added in Storage page on iDRAC GUI:

General

- Support for PCIe VDM (Enabled by default)
- Option to clear the system critical status to healthy state when unconfigured internal drive is removed
- Support NVMe Boot over Fibre Channel (NVMeOF)
- Support firmware update of TPM 1.2 and 2.0 for 15G servers
- Rsyslog server and Redfish event listener supports streaming of all message IDs
- Support for DNS configuration using IPv6 Router Advertisement (RA) messages, per RFC 8106.

GUI Enhancement

- Prevent iDRAC user logging out during browser refresh
- Show PCIe slot inventory in a simplified view
- New filters in Storage page
- Show the last used domain name by default in the login page (AD users)

Redfish Updates— Added support for the following Redfish features:

- Redfish lifecycle eventing (RLCE) streams server lifecycle changes across all message IDs
- HTTP/2 network protocol
- Added support for following:
  - ComputerSystem.GraceFulRestart
  - OperationApplyTime option for updates operations including SimpleUpdate, TransferProtocaol and MultipartUpload
  - ConvergedInfra.1#AppRawData attribute
  - DelliDRACCardService.GetKVMSessionOEM action
  - ConvergedInfra.1#AppRawData attribute

Support/Diagnostics
- CPU & Memory Utilization logging in Support Assist Collection
- Add PCIe tree of the system in the Support Assist Collection
- SupportAssist Logs to include historical thermal inlet and outlet temperature

Reports
- All Metric Report Definitions (MRD) have three new properties ServiceTag, MetricReportDefinitionDigest, and iDRACFirmwareVersion. Digest property helps consumer identify out-of-band changes in Custom MRD outside the influence of the component that created it. It helps as a reference to customers to track any changes made to the MRDs

Cómo utilizar esta guía

El contenido de esta guía del usuario permite realizar las tareas con:
- Interfaz web de la iDRAC: aquí se proporciona solo la información relacionada con la tarea. Para obtener información sobre los campos y las opciones, consulte la *Ayuda en línea de la 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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.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 *iDRAC Redfish API Guide* disponible en www.api-marketplace.com.

Navegadores web compatibles

iDRAC es compatible con los siguientes exploradores:
- Internet Explorer/Edge
- Mozilla Firefox
- Google Chrome
- Safari

NOTA: Es posible que algunas funciones de la interfaz del usuario de iDRAC y de la asistencia en línea no estén disponibles en el navegador Internet Explorer.

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

Hipervisores y SO admitidos

La iDRAC es compatible con los siguientes hipervisores y SO:
- Microsoft Windows Server y Windows PE
- VMware ESXi
- RedHat Enterprise Linux
- SuSe Linux Enterprise Server

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

Licencias de la iDRAC

Las funciones de la iDRAC están disponibles según el tipo de licencia. Según el modelo del sistema, la licencia de iDRAC Basic o iDRAC Express se instala de manera predeterminada. La licencia Enterprise de iDRAC, la licencia Datacenter de iDRAC y la licencia de Administración de clave empresarial segura (SEKM) de iDRAC están disponibles como una actualización y se pueden adquirir en cualquier momento. Solo las funciones con licencia están disponibles en las interfaces que permiten configurar o usar la iDRAC. Para obtener más información, consulte Funciones con licencia en iDRAC9.

Types of licenses

iDRAC Basic or iDRAC Express are the standard licenses available by default on your system. iDRAC Enterprise and Datacenter licenses includes all the licensed features and can be purchased at any time. The types of upsell offered are:

- 30-day evaluation—Evaluation licenses are duration-based and the timer runs when power is applied to the system. This license cannot be extended.
- Perpetual—The license is bound to the Service Tag and is permanent.

Following table lists the default license available on the following systems:

iDRAC Basic License	iDRAC Express License	iDRAC Enterprise License	iDRAC Datacenter License
PowerEdge Rack/Tower severs series 100-500	• PowerEdge C41XX • PowerEdge FC6XX • PowerEdge R6XX • PowerEdge R64XX • PowerEdge R7XX • PowerEdge R74XXd • PowerEdge R74XX • PowerEdge R8XX • PowerEdge R9XX • PowerEdge R9XX • PowerEdge T6XX • Dell Precision Rack R7920	All platforms, with upgrade option	All platforms, with upgrade option

Table 1. Default License

iDRAC Express License	iDRAC Enterprise License	iDRAC Datacenter License
• PowerEdge C41XX • PowerEdge FC6XX • PowerEdge R6XX • PowerEdge R64XX • PowerEdge R7XX • PowerEdge R74XXd • PowerEdge R74XX • PowerEdge R8XX • PowerEdge R9XX • PowerEdge R9XX • PowerEdge T6XX • Dell Precision Rack R7920	All platforms, with upgrade option	All platforms, with upgrade option

NOTE: The default license available with PowerEdge C64XX and C65xx systems is BMC. The BMC license was custom made for C64XX systems.

NOTE: Express for Blades license is the default license for PowerEdge M6XX and MXXXX systems.

Métodos para la adquisición de licencias

Utilice cualquiera de los métodos siguientes para adquirir licencias:

- Dell Digital Locker: Dell Digital Locker le permite ver y administrar sus productos, software e información de licencia en una sola ubicación. Un enlace a Dell Digital Locker está disponible en la interfaz web de DRAC: vaya a **Configuración** > **Licencias**.

NOTA: Para obtener más información sobre Dell Digital Locker, consulte las Preguntas frecuentes en el sitio web.

- Correo electrónico: la licencia se adjunta a un correo electrónico que se envía después de solicitarla desde el centro de asistencia técnica.
- Punto de venta: la licencia se adquiere al realizar un pedido de un sistema.

NOTA: Para administrar licencias o comprar licencias nuevas, vaya a Dell Digital Locker.

Adquisición de la clave de licencia de Dell Digital Locker

Para obtener la clave de licencia desde su cuenta, primero debe registrar su producto. Para ello, use el código de registro que se envía en el correo electrónico de confirmación del pedido. Debe ingresar este código en la pestaña **Registro del producto** después de iniciar sesión en Dell Digital Locker.

En el panel a la izquierda, haga clic en la pestaña **Productos** o **Historial de pedidos** para ver la lista de sus productos. Los productos basados en suscripción aparecen en la pestaña **Cuentas de facturación**.

Realice los siguientes pasos para descargar la clave de licencia de su cuenta de Dell Digital Locker:

1. Inicie sesión en su cuenta de Dell Digital Locker.
2. En el panel izquierdo, haga clic en **Productos**.
3. Haga clic en el producto que desea ver.
4. Haga clic en el nombre del producto.
5. En la página **Administración de productos**, haga clic en **Obtener clave**.
6. Siga las instrucciones que aparecen en la pantalla para obtener la clave de licencia.

NOTA: Si no tiene una cuenta de Dell Digital Locker, cree una con la dirección de correo electrónico proporcionado durante su compra.

NOTA: Para generar varias claves de licencia para nuevas compras, siga las instrucciones en **Herramientas** > **Activación de licencia** > **Licencias sin activar**

Operaciones de licencia

Para poder realizar las tareas de administración de licencias, asegúrese de adquirir las licencias necesarias. Para obtener más información, consulte los Métodos de adquisición de licencias.

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

Puede realizar las siguientes operaciones de licencia mediante iDRAC, RACADM, WSMan, Redfish y los servicios remotos de Lifecycle Controller para una administración de licencias de uno a uno, y Dell License Manager para la administración de licencias de uno a varios:

- Ver: ver la información de la licencia actual.
- 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 pasa las comprobaciones de validación.

  NOTA: Aunque puede exportar la licencia instalada de fábrica, no puede importarla. Para importar la licencia, descargue la licencia equivalente desde Digital Locker o recupérela desde el correo electrónico que recibió cuando la compró.

  NOTA: Después de importar la licencia, deberá volver a iniciar sesión en la iDRAC. Esto se aplica solo a la interfaz web de iDRAC.
- Exportar: permite exportar la licencia instalada. Para obtener más información, consulte la *Ayuda en línea de iDRAC*.
- Delete (Eliminar): elimina la licencia. Para obtener más información, consulte la *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.

  NOTA: Para que la opción Learn More (Más información) muestre la página correcta, asegúrese de que ***.dell.com** se agregue a la lista Sitios de confianza en Configuración de seguridad. Para obtener más información, consulte la documentación de ayuda de Internet Explorer.

Para realizar una implementación de licencias de uno a varios, puede utilizar Dell License Manager. Para obtener más información, consulte *Guía del usuario de Dell License Manager* disponible en https://www.dell.com/esmmanuals.

A continuación, se presentan los requisitos de privilegio de usuario para las diferentes operaciones de licencia:

- Ver y exportar la licencia: privilegio de inicio de sesión.
- Importación y eliminación de la licencia: iniciar sesión + configurar iDRAC + privilegio de control del servidor.

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 **Licensing (Licencias)**, se muestran las licencias relacionadas con los dispositivos o las licencias que están instaladas, pero que no tienen los dispositivos correspondientes 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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

Funciones sujetas a licencia en iDRAC9

En la siguiente tabla se proporcionan las funciones de la iDRAC9 activadas según la licencia adquirida:

Tabla 2. Funciones sujetas a licencia en iDRAC9

Función	iDRAC 9 Basic	iDRAC9 Express	iDRAC9 Express para servidores Blade	iDRAC9 Enterprise	iDRAC9 Datacenter
Interfaces/estándares					
Redfish y API RESTful de iDRAC	Sí	Sí	Sí	Sí	Sí
IPMI 2.0	Sí	Sí	Sí	Sí	Sí
DCMI 1.5	Sí	Sí	Sí	Sí	Sí
Interfaz gráfica web del usuario	Sí	Sí	Sí	Sí	Sí
Línea de comandos de RACADM (local/remota)	Sí	Sí	Sí	Sí	Sí
SSH	Sí	Sí	Sí	Sí	Sí
Redirección serial	Sí	Sí	Sí	Sí	Sí
WSMan	Sí	Sí	Sí	Sí	Sí
Protocolo de tiempo de la red	No	Sí	Sí	Sí	Sí
Conectividad					
NIC compartida (LOM)	Sí	Sí	N/A	Sí	Sí
NIC dedicado	Sí	Sí	Sí	Sí	Sí

Tabla 2. Funciones sujetas a licencia en iDRAC9 (continuación)

Función	iDRAC 9 Basic	iDRAC9 Express	iDRAC9 Express para servidores Blade	iDRAC9 Enterprise	iDRAC9 Datacenter
Etiquetado VLAN	Sí	Sí	Sí	Sí	Sí
IPv4	Sí	Sí	Sí	Sí	Sí
IPv6	Sí	Sí	Sí	Sí	Sí
DHCP	Sí	Sí	Sí	Sí	Sí
DHCP sin intervención manual	No	No	No	Sí	Sí
DNS dinámico	Sí	Sí	Sí	Sí	Sí
Paso a través del sistema operativo	Sí	Sí	Sí	Sí	Sí
iDRAC directa: USB del panel frontal	Sí	Sí	Sí	Sí	Sí
Vista Conexión	Sí	Sí	No	Sí	Sí
Seguridad					
Autoridad basada en roles	Sí	Sí	Sí	Sí	Sí
Usuarios locales	Sí	Sí	Sí	Sí	Sí
Cifrado SSL	Sí	Sí	Sí	Sí	Sí
Administrador de clave empresarial segura	No	No	No	Sí (con licencia SEKM)	Sí (con licencia SEKM)
Bloqueo de IP	No	Sí	Sí	Sí	Sí
Servicios de directorio (AD, LDAP)	No	No	No	Sí	Sí
Autentificación de dos factores (tarjeta inteligente)	No	No	No	Sí	Sí
Inicio de sesión único	No	No	No	Sí	Sí
Autentificación de PK (para SSH)	No	Sí	Sí	Sí	Sí
Integración de OAuth con servicios de autenticación basados en la Web	No	No	No	No	Sí
OpenID Connect para consolas Dell EMC	No	No	No	No	Sí
FIPS 140-2	Sí	Sí	Sí	Sí	Sí
Inicio de UEFI seguro: administración de certificados	Sí	Sí	Sí	Sí	Sí
Modo de bloqueo	No	No	No	Sí	Sí
Contraseña predeterminada única de iDRAC	Sí	Sí	Sí	Sí	Sí
Banner de política de seguridad personalizable: página de inicio de sesión	Sí	Sí	Sí	Sí	Sí

Tabla 2. Funciones sujetas a licencia en iDRAC9 (continuación)

Función	iDRAC 9 Basic	iDRAC9 Express	iDRAC9 Express para servidores Blade	iDRAC9 Enterprise	iDRAC9 Datacenter
Autenticación multifactor Easy	No	No	No	No	Sí
Inscripción automática de certificados (certificados SSL)	No	No	No	No	Sí
Quick Sync 2 de iDRAC: aut. opcional para operaciones de lectura	Sí	Sí	Sí	Sí	Sí
Quick Sync 2 de iDRAC: adición de número de dispositivo móvil en LCL	Sí	Sí	Sí	Sí	Sí
Borrado del sistema de dispositivos de almacenamiento interno	Sí	Sí	Sí	Sí	Sí
Presencia remota					
Control de alimentación	Sí	Sí	Sí	Sí	Sí
Control de arranque	Sí	Sí	Sí	Sí	Sí
Comunicación en serie en la LAN	Sí	Sí	Sí	Sí	Sí
Medios virtuales	No	No	Sí	Sí	Sí
Carpetas virtuales	No	No	No	Sí	Sí
Recurso compartido de archivos remotos	No	No	No	Sí	Sí
Acceso de HTML5 a consola virtual	No	No	Sí	Sí	Sí
Consola virtual	No	No	Sí	Sí	Sí
Conexión VNC al sistema operativo	No	No	No	Sí	Sí
Control de calidad/ancho de banda	No	No	No	Sí	Sí
Colaboración de consola virtual (hasta seis usuarios en simultáneo)	No	No	No (solo un usuario)	Sí	Sí
Chat de consola virtual	No	No	No	Sí	Sí
Particiones de flash virtual	No	No	No	Sí	Sí
NOTA: vFlash no está disponible en iDRAC9 para las plataformas PowerEdge Rx5xx/Cx5xx.					
Administrador de grupo	No	No	No	Sí	Sí
Compatibilidad con HTTP/HTTPS junto con NFS/CIFS	Sí	Sí	Sí	Sí	Sí
Alimentación y elementos térmicos					

Tabla 2. Funciones sujetas a licencia en iDRAC9 (continuación)

Función	iDRAC 9 Basic	iDRAC9 Express	iDRAC9 Express para servidores Blade	iDRAC9 Enterprise	iDRAC9 Datacenter
Medidor de alimentación en tiempo real	Sí	Sí	Sí	Sí	Sí
Umbrales y alertas de alimentación	No	Sí	Sí	Sí	Sí
Gráficos de alimentación en tiempo real	No	Sí	Sí	Sí	Sí
Contadores de datos históricos de alimentación	No	Sí	Sí	Sí	Sí
Límites de alimentación	No	No	No	Sí	Sí
Integración de Power Center	No	No	No	Sí	Sí
Supervisión de la temperatura	Sí	Sí	Sí	Sí	Sí
Gráficos de temperatura	No	Sí	Sí	Sí	Sí
Personalización de flujo de aire PCIe (LFM)	No	No	No	No	Sí
Control de escape personalizado	No	No	No	No	Sí
Control Delta-T personalizado	No	No	No	No	Sí
Consumo de flujo de aire del sistema	No	No	No	No	Sí
Temperatura de entrada PCIe personalizada	No	No	No	No	Sí
Supervisión de la condición					
Supervisión completa sin agentes	Sí	Sí	Sí	Sí	Sí
Supervisión predictiva de fallas	Sí	Sí	Sí	Sí	Sí
SNMPv1 y v2 y v3 (capturas y obtenciones)	Sí	Sí	Sí	Sí	Sí
Alertas de correo electrónico	No	Sí	Sí	Sí	Sí
Umbrales configurables	Sí	Sí	Sí	Sí	Sí
Supervisión de ventiladores	Sí	Sí	Sí	Sí	Sí
Supervisión de suministros de energía	Sí	Sí	Sí	Sí	Sí

Tabla 2. Funciones sujetas a licencia en iDRAC9 (continuación)

Función	iDRAC 9 Basic	iDRAC9 Express	iDRAC9 Express para servidores Blade	iDRAC9 Enterprise	iDRAC9 Datacenter
Supervisión de memoria	Sí	Sí	Sí	Sí	Sí
GPU	No	No	No	Sí	Sí
Supervisión de CPU	Sí	Sí	Sí	Sí	Sí
Supervisión de RAID	Sí	Sí	Sí	Sí	Sí
Supervisión de NIC	Sí	Sí	Sí	Sí	Sí
Inventario óptico	Sí	Sí	Sí	Sí	Sí
Estadísticas ópticas	No	No	No	No	Sí
Supervisión de discos duros (gabinete)	Sí	Sí	Sí	Sí	Sí
Supervisión de rendimiento fuera de banda	No	No	No	Sí	Sí
Alertas de desgaste excesivo de SSD	Sí	Sí	Sí	Sí	Sí
Configuración personalizable para temperatura de salida	Sí	Sí	Sí	Sí	Sí
Registros de consola en serie	No	No	No	No	Sí
Registros SMART para unidades de almacenamiento	No	No	No	No	Sí
Detección de servidores Idle	No	No	No	No	Sí
Transmisión de telemetría	No	No	No	No	Sí
NOTA: La licencia de OpenManage Enterprise Advanced y el plug-in de PowerManage admiten datos de telemetría extraídos del iDRAC.					
Actualizar					
Actualización remota sin agentes	Sí	Sí	Sí	Sí	Sí
Herramientas de actualización incorporadas	Sí	Sí	Sí	Sí	Sí
Actualización desde el repositorio (actualización automática)	No	No	No	Sí	Sí
Programar actualización desde el repositorio	No	No	No	Sí	Sí

Tabla 2. Funciones sujetas a licencia en iDRAC9 (continuación)

Función	iDRAC 9 Basic	iDRAC9 Express	iDRAC9 Express para servidores Blade	iDRAC9 Enterprise	iDRAC9 Datacenter
Actualizaciones mejoradas de firmware de PSU	Sí	Sí	Sí	Sí	Sí
Implementación y configuración					
Configuración local a través de F10	Sí	Sí	Sí	Sí	Sí
Herramientas incorporadas de implementación del sistema operativo	Sí	Sí	Sí	Sí	Sí
Herramientas de configuración incorporadas	Sí	Sí	Sí	Sí	Sí
Descubrimiento automático	No	Sí	Sí	Sí	Sí
Implementación remota del sistema operativo	No	Sí	Sí	Sí	Sí
Paquete incorporado de controladores	Sí	Sí	Sí	Sí	Sí
Configuración completa del inventario	Sí	Sí	Sí	Sí	Sí
Exportación de inventario	Sí	Sí	Sí	Sí	Sí
Configuración remota	Sí	Sí	Sí	Sí	Sí
Configuración sin intervención	No	No	No	Sí	Sí
Retiro/reasignación del sistema	Sí	Sí	Sí	Sí	Sí
Perfil de configuración del servidor en la GUI	Sí	Sí	Sí	Sí	Sí
Adición de configuración del BIOS en la GUI de iDRAC	Sí	Sí	Sí	Sí	Sí
Propiedades de GPU	No	No	No	Sí	Sí
Diagnóstico, servicio y registro					
Herramientas de diagnóstico incorporadas	Sí	Sí	Sí	Sí	Sí
Reemplazo de piezas	No	Sí	Sí	Sí	Sí

NOTA: Después de realizar un reemplazo de piezas en hardware RAID y se haya completado el proceso para el reemplazo del firmware y de la configuración, los registros de Lifecycle informan entradas duplicadas de reemplazo de piezas, lo cual es un comportamiento esperado.

Tabla 2. Funciones sujetas a licencia en iDRAC9 (continuación)

Función	iDRAC 9 Basic	iDRAC9 Express	iDRAC9 Express para servidores Blade	iDRAC9 Enterprise	iDRAC9 Datacenter
Easy Restore (configuración del sistema)	Sí	Sí	Sí	Sí	Sí
Tiempo de espera automático para restauración fácil	Sí	Sí	Sí	Sí	Sí
NOTA: Las funciones de copia de seguridad y restauración del servidor no están disponibles en iDRAC9 para PowerEdge Rx5xx/Cx5xx.					
Indicadores LED de estado de la condición	Sí	Sí	N/A	Sí	Sí
Pantalla LCD (iDRAC9 requiere opcional)	Sí	Sí	N/A	Sí	Sí
iDRAC Quick Sync 2 (hardware BLE/Wi-Fi)	Sí	Sí	Sí	Sí	Sí
iDRAC directo (puerto de administración de USB frontal)	Sí	Sí	Sí	Sí	Sí
Módulo de servicio de iDRAC (iSM) integrado	Sí	Sí	Sí	Sí	Sí
Reenvío de alertas de iSM a alertas en banda para las consolas	Sí	Sí	Sí	Sí	Sí
Recopilación de SupportAssist (incorporada)	Sí	Sí	Sí	Sí	Sí
Captura de pantalla de bloqueo	No	Sí	Sí	Sí	Sí
Captura de video de bloqueo[1]	No	No	No	Sí	Sí
Captura de video de bloqueo sin agente (solo Windows)	No	No	No	No	Sí
Captura de inicio	No	No	No	Sí	Sí
Restablecimiento manual de iDRAC (botón de Id. de LCD)	Sí	Sí	Sí	Sí	Sí
Restablecimiento remoto de iDRAC (requiere iSM)	Sí	Sí	Sí	Sí	Sí
NMI virtual	Sí	Sí	Sí	Sí	Sí
Vigilancia del sistema operativo	Sí	Sí	Sí	Sí	Sí

Tabla 2. Funciones sujetas a licencia en iDRAC9 (continuación)

Función	iDRAC 9 Basic	iDRAC9 Express	iDRAC9 Express para servidores Blade	iDRAC9 Enterprise	iDRAC9 Datacenter
Registro de sucesos del sistema	Sí	Sí	Sí	Sí	Sí
Registro de Lifecycle	Sí	Sí	Sí	Sí	Sí
Registro mejorado en el registro de Lifecycle Controller	Sí	Sí	Sí	Sí	Sí
Notas de trabajo	Sí	Sí	Sí	Sí	Sí
Syslog remoto	No	No	No	Sí	Sí
Administración de licencias	Sí	Sí	Sí	Sí	Sí
Mejor experiencia del cliente					
iDRAC: procesador más rápido, más memoria	N/A	Sí	N/A	Sí	Sí
GUI presentada en HTML5	N/A	Sí	N/A	Sí	Sí
Adición de configuración del BIOS en la GUI de iDRAC	N/A	Sí	N/A	Sí	Sí

[1] Requiere iSM o 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 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 Configuración de iDRAC, presione <F2> durante el inicio y juego haga clic en **Configuración de iDRAC** en la página **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 **Configuración del sistema** > **Configuración avanzada de hardware** > **Configuración de iDRAC**. Para obtener más información, consulte la *Guía del usuario de Lifecycle Controller* disponible en **dell.com/idracmanuals**.
Interfaz web del 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. Los puertos HTTP y HTTPS predeterminados se pueden modificar. El acceso del usuario se basa en los privilegios de usuario.

Tabla 3. Interfaces y protocolos para acceder a iDRAC (continuación)

Interfaz o protocolo	Descripción
Interfaz web de OpenManage Enterprise (OME) Modular	**NOTA:** Esta interfaz solo está disponible para las plataformas MX. Además de supervisar y administrar el chasis, utilice la interfaz web de OME-Modular para realizar las siguientes acciones: ● 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 Para obtener más información, consulte *Guía del usuario de OME - Modular para el chasis PowerEdge MX7000* disponible en https://www.dell.com/openmanagemanuals.
Interfaz web de la CMC	**NOTA:** Esta interfaz no está disponible para las plataformas MX. Además de supervisar y administrar el chasis, utilice la interfaz web de la CMC para realizar las siguientes acciones: ● 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 Identificación del sistema durante 16 segundos. **NOTA:** El panel LCD solo está disponible con sistemas en rack o en torre que admiten bisel frontal. Para servidores Blade, la pantalla LCD se encuentra en el panel anterior del chasis y se comparte entre todos los servidores Blade.
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. ● 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 cuando se inicia sesión en iDRAC mediante SSH. 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 y API RESTful de iDRAC	La API de administración de plataformas escalable Redfish es un estándar definido por Distributed Management Task Force (DMTF). Redfish es un estándar de interfaz de administración de sistemas

Tabla 3. Interfaces y protocolos para acceder a iDRAC (continuación)

Interfaz o protocolo	Descripción
	de última generación, que permite una administración abierta, segura y escalable de servidores. Se trata de una nueva interfaz que utiliza semántica de interfaz RESTful para acceder a los datos que se define en el formato de modelo para realizar la administración de sistemas fuera de banda. Es adecuada para una amplia gama de servidores que van de servidores independientes a entornos blade y montados en rack y entornos de servicios en la 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 para la que se pueden crear secuencias de comandos fácilmente ● Adhesión a estándares ampliamente usados Para obtener la Guía de API de iDRAC Redfish, vaya a www.api-marketplace.com
WSMan	Los servicios remotos de LC se basan en el protocolo WSMan para realizar tareas de administración de uno a varios sistemas. Debe utilizar el cliente WSMan como el cliente WinRM (Windows) o el cliente OpenWSMan (Linux) para utilizar la funcionalidad de servicios remotos de LC. También puede utilizar PowerShell y Python para crear secuencias de comandos para la interfaz WSMan. Los servicios web para la administración (WSMan) son 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 de información común (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 son proporcionados por la interfaz de instrumentación de iDRAC asignada a los perfiles DMTF y los perfiles de extensión. Para obtener más información, consulte lo siguiente: ● *Guía de inicio rápido de servicios remotos de Lifecycle Controller* disponible en https://www.dell.com/idracmanuals . ● MOF y perfiles: http://downloads.dell.com/wsman. ● Sitio web de DMTF: dmtf.org/standards/profiles
SSH	Use SSH para ejecutar comandos RACADM. 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 la iDRAC por primera vez, se genera una clave de host única RSA de 1024 bits.
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 la *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.
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 que funciona en una red de Windows.
SMB	iDRAC9 admite el protocolo de bloques de mensajes de servidor (SMB). Este es un protocolo de uso compartido de archivos de red y la versión mínima predeterminada de SMB admitida es la versión 2.0; SMBv1 ya no es compatible.
NFS	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

En la siguiente tabla se muestran los puertos necesarios para acceder a la iDRAC de manera remota por medio de servidores de seguridad. Estos son los puertos predeterminados que iDRAC utiliza en espera para las conexiones. De manera opcional, puede modificar la mayoría de los puertos. Para modificar los puertos, consulte Configuración de servicios en la página 102.

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

Número de puerto	Tipo	Función	Puerto configurable	Nivel de cifrado máximo
22	TCP	SSH	Sí	SSL de 256 bits
80	TCP	HTTP	Sí	Ninguno
161	UDP	Agente SNMP	Sí	Ninguno
443	TCP	• Acceso GUI web con HTTPS • Consola virtual y medios virtuales con la opción eHTML5 • Consola virtual y medios virtuales con la opción HTML5 cuando está activada la redirección del servidor web	Sí	SSL de 256 bits
623	UDP	RMCP/RMCP+	No	SSL de 128 bits
5000	TCP	De iDRAC a iSM	No	SSL de 256 bits
NOTA: El nivel de cifrado máximo es SSL de 256 bits si están instalados ambos iSM 3.4 (o superior) y el firmware de la iDRAC 3.30.30.30 (o superior).				
5900	TCP	Consola virtual y medios virtuales con opción HTML5, Java y ActiveX	Sí	SSL de 128 bits
5901	TCP	VNC	Sí	SSL de 128 bits
NOTA: El puerto 5901 se abre cuando la función VNC está activada.				

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

Tabla 5. Puertos que iDRAC utiliza como cliente

Número de puerto	Tipo	Función	Puerto configurable	Nivel de cifrado máximo
25	TCP	SMTP	Sí	Ninguno
53	UDP	DNS	No	Ninguno
68	UDP	Dirección IP asignada por DHCP	No	Ninguno
69	TFTP	TFTP	No	Ninguno
123	UDP	Protocolo de hora de red (NTP)	No	Ninguno
162	UDP	Captura SNMP	Sí	Ninguno
445	TCP	Common Internet File System (Sistema de archivos de Internet común - CIFS)	No	Ninguno
636	TCP	LDAP sobre SSL (LDAPS)	No	SSL de 256 bits
2049	TCP	Network File System (Sistema de archivos de red - NFS)	No	Ninguno
3269	TCP	LDAPS para catálogo global (GC)	No	SSL de 256 bits
5353	UDP	mDNS	No	Ninguno

Tabla 5. Puertos que iDRAC utiliza como cliente (continuación)

Número de puerto	Tipo	Función	Puerto configurable	Nivel de cifrado máximo
NOTA: Cuando el descubrimiento iniciado de nodos o Administrador de grupo están habilitados, iDRAC usa mDNS para comunicarse a través del puerto 5353. Sin embargo, cuando ambos están deshabilitados, el firewall interno de iDRAC bloquea el puerto 5353 y aparece como puerto abierto|filtrado en los análisis de puertos.				
514	UDP	Syslog remoto	Sí	Ninguno

Otros documentos que podrían ser de utilidad

Algunas de las interfaces de la iDRAC tienen integrado el documento *Ayuda en línea* al que se puede acceder haciendo clic en el icono (?) de ayuda. En *Ayuda en línea* se proporciona información acerca de los campos disponibles en la interfaz web de la iDRAC y sus descripciones. Además, los siguientes documentos que están disponibles en el sitio web del servicio de asistencia Dell Support en **dell.com/support** proporcionan información adicional acerca de la configuración y la operación de la iDRAC en su sistema.

- En la guía de la API de Redfish de iDRAC disponible en https://developer.dell.com, se proporciona información sobre la API de Redfish.
- En el documento *Guía de la CLI de RACADM para iDRAC* se proporciona información sobre los subcomandos de RACADM, las interfaces admitidas y los grupos de base de datos de propiedad de la iDRAC además de definiciones de objeto.
- En el documento *Guía de descripción general de administración de sistemas* se proporciona información acerca de los distintos programas de software disponibles para realizar tareas de administración de sistemas.
- En la *Guía del usuario de la herramienta de configuración de Dell Remote Access* se proporciona información sobre cómo utilizar la herramienta para detectar las direcciones IP de la iDRAC en la red, realizar una a varias actualizaciones de firmware y activar la configuración del directorio para las direcciones IP detectadas.
- 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.
- En la *Guía del usuario del módulo de servicio del iDRAC* se 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 *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.

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 el documento *Guía de introducción* se proporciona una descripción general de las características del sistema, de la configuración de su sistema y de las especificaciones técnicas.
- En el documento *Manual de instalación y servicio* se proporciona información sobre las características del sistema y se describe cómo solucionar problemas del sistema e instalar o sustituir componentes del sistema.

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 comunicarse con Dell para tratar asuntos relacionados con ventas, asistencia técnica o servicio de atención al cliente, visite https://www.dell.com/contactdell.

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 consultar todos los documentos de OpenManage Connections y Enterprise Systems Management, visitehttps://www.dell.com/esmmanuals
  - Para consultar los documentos de OpenManage, visite https://www.dell.com/openmanagemanuals
  - Para consultar los documentos de iDRAC y Lifecycle Controller, visite https://www.dell.com/idracmanuals
  - Para consultar documentos sobre herramientas de mantenimiento, visite https://www.dell.com/serviceabilitytools
  - Para consultar los documentos de Client Command Suite Systems Management, visite https://www.dell.com/omconnectionsclient

Acceso a los documentos mediante la búsqueda de productos

1. Consulte https://www.dell.com/support.
2. En la casilla de búsqueda **Ingrese una etiqueta de servicio, un número de serie...**, ingrese el nombre de producto. Por ejemplo, **`PowerEdge`** o **`iDRAC`**.

   Se muestra una lista de archivos que coinciden.
3. Seleccione su producto y haga clic en el icono de búsqueda o presione Intro.
4. Haga clic en **DOCUMENTACIÓN**.
5. Haga clic en **MANUALES Y DOCUMENTOS**.

Acceso a los documentos mediante el selector de productos

También puede seleccionar el producto para acceder a los documentos.

1. Consulte https://www.dell.com/support.
2. Haga clic en **Browse all products** (Buscar todos los productos).
3. Haga clic en la categoría de producto deseada, como servidores, software, almacenamiento, etc.
4. Haga clic en el producto deseado y, a continuación, haga clic en la versión deseada, si corresponde.

   NOTA: Para algunos productos, es posible que tenga que desplazarse por las subcategorías.
5. Haga clic en **DOCUMENTACIÓN**.
6. Haga clic en **MANUALES Y DOCUMENTOS**.

Acceso a la guía de API de Redfish

La guía de API de Redfish ya está disponible en Dell API Marketplace. Para acceder a la guía de API de Redfish:

1. Consulte www.api-marketplace.com.
2. Haga clic en **Explorar API** y, a continuación, en **API**.
3. En API de Redfish de iDRAC9, haga clic en **Ver más**.

2

Inicio de sesión en iDRAC

Puede iniciar sesión en iDRAC como usuario de iDRAC, de Microsoft Active Directory o de protocolo ligero de acceso a directorios (LDAP). También puede iniciar sesión con OpenID Connect y Single Sign On o tarjeta inteligente.

Para mejorar la seguridad, cada sistema se envía 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 efectuar el pedido del 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 de iDRAC se asigna dinámicamente.

NOTA:

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

NOTA: Para obtener información sobre los caracteres recomendados para los nombres de usuario y las contraseñas, consulte Caracteres recomendados para nombres de usuario y contraseñas en la página 154.

Para cambiar la contraseña predeterminada, consulte Cambio de la contraseña de inicio de sesión predeterminada en la página 46.

Banner de seguridad personalizable

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

OpenID Connect

NOTA: Esta función solo está disponible para las plataformas MX.

Puede iniciar sesión en iDRAC con las credenciales de otras consolas web, como Dell EMC OpenManage Enterprise (OME) - Modular. Cuando esta función está activada, se comienzan a administrar los permisos de usuario de iDRAC en la consola. iDRAC proporciona la sesión de usuario con todos los permisos que se especifican en la consola.

NOTA: Cuando el modo de bloqueo está activado, las opciones de inicio de sesión de OpenID Connect no se muestran en la página de inicio de sesión de iDRAC.

Ahora puede obtener acceso a ayuda detallada sin iniciar sesión en la iDRAC. Utilice los enlaces de la página de inicio de sesión de iDRAC para acceder a la ayuda e información de la versión, los controladores y las descargas, los manuales, y TechCenter.

Temas:

- Visualización de la condición del sistema
- Inicio de sesión en iDRAC mediante la autentificación de clave pública
- Varias sesiones de iDRAC
- Contraseña segura predeterminada
- Cambio de la contraseña de inicio de sesión predeterminada
- Activación o desactivación del mensaje de advertencia de contraseña predeterminada
- Política de seguridad de contraseñas
- Bloqueo de IP
- Activación o desactivación del paso del sistema operativo a iDRAC mediante la interfaz web
- Activación o desactivación de alertas mediante RACADM

Forzar cambio de contraseña (FCP)

Con la función “Forzar cambio de contraseña”, se le solicita que cambie la contraseña predeterminada de fábrica del dispositivo. La función se puede habilitar como parte de la configuración de fábrica.

La pantalla de FCP aparece después de que el usuario se haya autenticado correctamente y no se puede omitir. Solo después de que el usuario ingresa una contraseña, se permitirán el acceso y la operación normales. El estado de este atributo no se verá afectado por una operación de restablecimiento de la configuración a los valores predeterminados.

NOTA: Para configurar o restablecer el atributo FCP, debe contar con privilegios de inicio de sesión y de configuración de usuario.

NOTA: Cuando FCP está habilitado, la configuración "Aviso de contraseña predeterminada" se desactiva después de cambiar la contraseña predeterminada del usuario.

NOTA: Cuando el usuario raíz inicia sesión mediante la autenticación de clave pública (PKA), se omite la FCP.

Cuando FCP está habilitada, no se permiten las siguientes acciones:

- Iniciar sesión en iDRAC mediante cualquier interfaz de usuario, excepto por la interfaz IPMI en la LAN, que utiliza la CLI con las credenciales de usuario.
- Iniciar sesión en iDRAC mediante la aplicación OMM a través de Quick Sync-2
- Agregar un miembro iDRAC en Group Manager.

Inicio de sesión en iDRAC mediante OpenID Connect

NOTA: Esta función solo está disponible en las plataformas MX.

Para iniciar sesión en iDRAC mediante OpenID Connect:

1. En un navegador web compatible, escriba `https://[iDRAC-IP-address]` y presione Intro.
   Se mostrará la página Inicio de sesión.
2. Seleccione **OME Modular** en el menú **Iniciar sesión con:**.
   Aparece la página de inicio de sesión de la consola.
3. Ingrese el **Nombre de usuario** y la **Contraseña** de la consola.
4. Haga clic en **Iniciar sesión**.
   Ha iniciado sesión en iDRAC con los privilegios de usuario de la consola.
   NOTA: Cuando el modo de bloqueo está activado, la opción de inicio de sesión de OpenID Connect no se muestra en la página de inicio de sesión de iDRAC.

Logging in to iDRAC as local user, Active Directory user, or LDAP user

Before you log in to iDRAC using the web interface, ensure that you have configured a supported web browser and the user account is created with the required privileges.

NOTE: The user name is not case-sensitive for an Active Directory user. The password is case-sensitive for all users.

NOTE: In addition to Active Directory, openLDAP, openDS, Novell eDir, and Fedora-based directory services are supported.

NOTE: LDAP authentication with OpenDS is supported. The DH key must be larger than 768 bits.

NOTE: RSA feature can be configured and enabled for LDAP user, but the RSA does not support if the LDAP is configured on Microsoft active directory. Hence LDAP user login fails. RSA is supported only for OpenLDAP.

To log in to iDRAC as local user, Active Directory user, or LDAP user:

1. Open a supported web browser.
2. In the **Address** field, type `https://[iDRAC-IP-address]` and press Enter.

   NOTE: If the default HTTPS port number (port 443) changes, enter: `https://[iDRAC-IP-address]:[port-number]` where `[iDRAC-IP-address]` is the iDRAC IPv4 or IPv6 address and `[port-number]` is the HTTPS port number.

   The **Login** page is displayed.
3. For a local user:
   - In the **Username** and **Password** fields, enter your iDRAC user name and password.
   - From the **Domain** drop-down menu, select **This iDRAC**.
4. For an Active Directory user, in the **User name** and **Password** fields, enter the Active Directory user name and password. If you have specified the domain name as a part of the username, select **This iDRAC** from the drop-down menu. The format of the user name can be: <domain>\<username>, <domain>/<username>, or <user>@<domain>.

   For example, dell.com\john_doe, or JOHN_DOE@DELL.COM.

   Active Directory domain from the **Domain** drop-down menu displays the last used domain.
5. For an LDAP user, in the **Username** and **Password** fields, enter your LDAP user name and password. Domain name is not required for LDAP login. By default, **This iDRAC** is selected in the drop-down menu.
6. Click **Submit**. You are logged in to iDRAC with the required user privileges.

   If you log in with Configure Users privileges and the default account credentials, and if the default password warning feature is enabled, the **Default Password Warning** page is displayed allowing you to easily change the password.

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 confianza de la autoridad de certificación (CA) 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 enlace `https://[IP address]`.

   Aparece la página **Inicio de sesión de iDRAC** en la que se le solicita insertar la tarjeta inteligente.

   NOTA: Si se cambió el número de puerto HTTPS predeterminado (puerto 443), escriba: `https://[IP address]:[port number]` , donde `[IP address]` es la dirección IP para la iDRAC 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 un símbolo del sistema para el PIN de la tarjeta inteligente. No se necesita una contraseña.

3. Ingrese el PIN de tarjeta inteligente para los usuarios locales de tarjeta inteligente.

   Ahora está conectado a iDRAC.

   NOTA: Si usted es un usuario local para el cual está activada la opción **Habilitar comprobación de CRL para inicio de sesión con tarjeta inteligente**, iDRAC intenta descargar la lista de revocación de certificados (CRL) y comprueba el certificado del usuario en la CRL. El inicio de sesión falla si el certificado aparece como revocado en la CRL o si la CRL no se puede descargar por algún motivo.

   NOTA: Si inicia sesión en iDRAC mediante tarjeta inteligente cuando RSA está activada, el token RSA se omitirá y podrá iniciar sesión directamente.

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.
- Active el inicio de sesión mediante tarjeta inteligente.

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

1. Inicie sesión en iDRAC mediante el enlace `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 iDRAC y `[port number]` es el número de puerto HTTPS.

2. Inserte la tarjeta inteligente y haga clic en **Iniciar sesión**.
   Se muestra una petición del **PIN** de la tarjeta inteligente.
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.

NOTA: Cuando el usuario de AD configura SSO mientras RSA está activado, se omite el token RSA y el usuario inicia sesión directamente.

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

NOTA: Esta función no está disponible en las plataformas MX.

Mediante la función SSO, puede iniciar la interfaz web de iDRAC desde la interfaz web del CMC. Un usuario de CMC tiene los privilegios de usuario de CMC cuando inicia iDRAC desde CMC. Si la cuenta de usuario está presente en CMC y no en iDRAC, el usuario 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 *Guía del usuario de la controladora de administración del chasis* disponible en https://www.dell.com/cmcmanuals.

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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.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 paquete de certificados de CA predeterminado en la estación de administración. Por ejemplo, para RHEL5 de 64 bits, es **/etc/pki/tls/cert.pem**.
3. Agregue el certificado CA con formato PEM al certificado CA de la estación de administración.

   Por ejemplo, utilice el `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 más información sobre cómo acceder a iDRAC mediante RACADM local, consulte *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

Acceso a iDRAC mediante RACADM de firmware

Puede utilizar la interfaz SSH para acceder a iDRAC y ejecutar los comandos del firmware RACADM. Para obtener más información, consulte *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

Autenticación simple de dos factores (2FA simple)

iDRAC ofrece una opción de autenticación simple de dos factores para mejorar la seguridad de los usuarios locales durante el inicio de sesión. Cuando inicia sesión desde una dirección IP de origen diferente del último inicio de sesión, se le solicitará que ingrese los detalles de autenticación del segundo factor.

La autenticación simple de dos factores tiene dos pasos de autenticación:

- Nombre de usuario y contraseña de iDRAC
- Código simple de seis dígitos que se envía al usuario por correo electrónico. El usuario debe ingresar este código de seis dígitos cuando se le solicite durante el inicio de sesión.

NOTA:

- Para obtener un código de seis dígitos, es obligatorio configurar la opción “Dirección personalizada del remitente personalizado” y tener una configuración de SMTP válida.
- El código 2FA vence después de 10 minutos o deja de ser válido si ya se utilizó antes del vencimiento.
- Si un usuario intenta iniciar sesión desde otra ubicación con una dirección IP diferente mientras todavía está pendiente una comprobación de 2FA de la dirección IP original, se enviará el mismo token para el intento de inicio de sesión desde la nueva dirección IP.
- Esta función es compatible con la licencia de iDRAC Enterprise o Datacenter.

Si 2FA está habilitado, no se permite realizar las siguientes acciones:

- Iniciar sesión en la iDRAC mediante cualquier interfaz de usuario que utilice la CLI con las credenciales de usuario predeterminadas.
- Iniciar sesión en iDRAC mediante la aplicación OMM a través de Quick Sync-2
- Agregar un miembro iDRAC en Administrador de grupo.

NOTA: RACADM, Redfish, WSMAN, IPMI LAN, serie, la CLI de una dirección IP de origen funciona solo después de iniciar sesión correctamente desde interfaces compatibles, como la GUI de iDRAC y SSH.

2FA de RSA SecurID

iDRAC se puede configurar para autenticarse con solo un servidor RSA AM a la vez. Los ajustes globales en el servidor RSA AM se aplican a todos los usuarios locales de iDRAC, AD y LDAP.

NOTA: La textura de 2FA de RSA SecurID solo está disponible en la licencia de Datacenter.

A continuación, se indican los requisitos previos antes de configurar iDRAC para habilitar RSA SecurID:

- Configure el servidor de Microsoft Active Directory.
- Si intenta habilitar RSA SecurID en todos los usuarios de AD, agregue el servidor de AD al servidor RSA AM como un origen de identidad.
- Asegúrese de disponer de un servidor de LDAP genérico.
- Para todos los usuarios de LDAP, el origen de la identidad del servidor LDAP se debe agregar en el servidor RSA AM.

Para habilitar RSA SecurID en iDRAC, se requieren los siguientes atributos del servidor RSA AM:

1. **URL de la API de autenticación de RSA**: la sintaxis de la URL es: `https://<rsa-am-server-hostname>:<port>/mfa/v1_1` y, de manera predeterminada, el puerto es 5555.

2. **ID del cliente de RSA**: de manera predeterminada, el ID del cliente de RSA es igual que el nombre de host del servidor RSA AM. Encuentre el ID de cliente RSA en la página de configuración del agente de autenticación del servidor RSA AM.
3. **Clave de acceso de RSA**: la clave de acceso se puede recuperar en RSA AM; para ello, navegue a la sección **Configuración** > **Configuración del sistema** > **RSA SecurID** > **Autenticación de la API**, que generalmente se muestra como `198cv5x195fdi86u43jw0q069byt0x37umlfwxc2gnp4s0xk11ve2lffum4s8302`. Para configurar los ajustes a través de la GUI iDRAC:
   - Vaya a **Configuración de iDRAC** > **Usuarios**.
   - En la sección **Usuarios locales**, seleccione un usuario local existente y haga clic en **Editar**.
   - Desplácese hacia abajo al pie de la página Configuración.
   - En la sección **RSA SecurID**, haga clic en el enlace **Configuración de RSA SecurID** para ver o editar estos ajustes.

   También puede configurar los ajustes como se indica a continuación:
   - Vaya a **Configuración de iDRAC** > **Usuarios**.
   - En la sección **Servicios de directorio**, seleccione **Microsoft Active Service** o **Servicio de directorio de LDAP genérico** y haga clic en **Editar**.
   - En la sección **RSA SecurID**, haga clic en el enlace **Configuración de RSA SecurID** para ver o editar estos ajustes.
4. **Certificado de servidor RSA AM (cadena)**

Puede iniciar sesión en iDRAC mediante el token de RSA SecurID a través de SSH y GUI de iDRAC.

Aplicación de token de RSA SecurID

Debe instalar la aplicación de token de RSA SecurID en el sistema o en el teléfono inteligente. Cuando intenta iniciar sesión en iDRAC, se le solicita ingresar el código de acceso que se muestra en la aplicación.

Si se ingresa un código de acceso incorrecto, el servidor de RSA AM solicita al usuario que proporcione el "Siguiente token". Esto puede suceder, aunque el usuario haya ingresado el código de acceso correcto. Esta entrada demuestra que el usuario posee el token correcto que genera el código de acceso correcto.

Para obtener el **Siguiente token** de la aplicación de token de RSA SecurID, haga clic en **Opciones**. Revise el **Siguiente token** y el siguiente código de acceso estará disponible. El tiempo es crítico en este paso. De lo contrario, es posible que iDRAC falle la verificación del siguiente token. Si expira el tiempo de espera del inicio de sesión del usuario de iDRAC, se requerirá otro intento de inicio de sesión

Si se ingresa un código de acceso incorrecto, el servidor de RSA AM le solicitará al usuario que proporcione el "Siguiente token". Esta comprobación se solicitará, aunque el usuario haya ingresado el código de acceso correcto. Esta entrada demuestra que el usuario posee el token correcto que genera el los códigos de acceso correctos.

Para obtener el token siguiente de la aplicación de token de RSA SecurID, haga clic en **Opciones** y marque **Siguiente token**. Se genera un nuevo token. El tiempo es crítico en este paso. De lo contrario, es posible que iDRAC falle la verificación del siguiente token. Si expira el tiempo de espera del inicio de sesión del usuario de iDRAC, se requerirá otro intento de inicio de sesión.

Visualización de la condición del sistema

Antes de llevar a cabo una tarea o desencadenar un evento, puede utilizar RACADM para verificar si el sistema se encuentra en un estado adecuado. Para ver el estado del servicio remoto desde RACADM, use el comando `getremoteservicesstatus`.

Tabla 6. Valores posibles para el estado del sistema

Sistema host	Lifecycle Controller (LC)	Estado en tiempo real	Estado general
• Apagado • En POST (Power-On Self-Test [autoprueba de encendido]) • Fuera de POST • Recopilación de inventario del sistema • Ejecución de tarea automatizada	• Listo • No se ha inicializado • Recargando datos • Desactivado • En recuperación • En uso	• Listo • No está listo	• Listo • No está listo

Tabla 6. Valores posibles para el estado del sistema (continuación)

Sistema host	Lifecycle Controller (LC)	Estado en tiempo real	Estado general
• Lifecycle Controller Unified Server Configurator • El servidor se ha detenido durante la petición de error de F1/F2 debido a un error de POST • El servidor se ha detenido en la petición de F1/F2/F11 debido a que no hay dispositivos de inicio disponibles • El servidor ha ingresado en el menú de configuración de F2 • El servidor ha ingresado en el menú del administrador de inicio de F11			

1. Lectura/escritura: solo lectura
2. Privilegio de usuario: usuario de inicio de sesión
3. Licencia requerida: iDRAC Express o iDRAC Enterprise
4. Dependencia: ninguna

Inicio de sesión en iDRAC mediante la autentificación de clave pública

Puede iniciar sesión en iDRAC a través de SSH sin introducir una contraseña. También puede enviar un solo comando de RACADM como argumento de línea de comandos a la aplicación SSH. Las opciones de línea de comandos se comportan como RACADM remoto, ya que la sesión finaliza al completarse 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 cantidad de sesiones iDRAC posibles mediante las distintas interfaces.

Tabla 7. Varias sesiones de iDRAC

Interfaz	Número de sesiones
Interfaz web del iDRAC	8
RACADM remoto	4
Firmware RACADM	SSH: 4 Serie - 1

iDRAC permite varias sesiones para el mismo usuario. Una vez que un usuario crea la cantidad máxima de sesiones permitidas, otros usuarios no pueden iniciar sesión en iDRAC. Esto puede provocar una *Denegación de servicio* para un usuario administrador legítimo.

En caso de agotamiento de sesión, tome las siguientes medidas:

- Si se agotan las sesiones basadas en un servidor web, puede iniciar sesión mediante SSH o RACADM local.
- Entonces, un administrador puede finalizar las sesiones existentes mediante los comandos de racadm (`racadm getssninfo`; `racadm closessn -i <index>`).

Contraseña segura predeterminada

Todos los sistemas compatibles se envían con una contraseña única predeterminada para la iDRAC, a menos que elija establecer *calvin* como contraseña mientras se realiza el pedido del sistema. Esta contraseña única ayuda a mejorar la seguridad de la iDRAC y del servidor. Para mejorar aún más la seguridad, se recomienda cambiar la contraseña predeterminada.

La contraseña única para el sistema está disponible en la etiqueta de información del sistema. Para localizar la etiqueta, consulte la documentación de su servidor en https://www.dell.com/support.

NOTA: Para PowerEdge C6420, M640 y FC640, la contraseña predeterminada es *calvin*.

NOTA: El restablecimiento de la iDRAC a los valores predeterminados de fábrica revierte la contraseña predeterminada a la que tenía el servidor cuando se envió.

Si olvidó la contraseña y no tiene acceso a la etiqueta de información del sistema, hay algunos métodos para restablecer la contraseña a nivel local o remoto.

Restablecimiento de la contraseña de iDRAC predeterminada localmente

Si dispone de acceso físico al sistema, puede restablecer la contraseña utilizando lo siguiente:

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

Restablecer contraseña predeterminada mediante la utilidad de configuración de la iDRAC

Puede acceder a la utilidad de configuración de la iDRAC mediante la configuración del sistema de su servidor. Mediante la función restablecer a los valores predeterminados de la iDRAC, es posible restablecer al valor predeterminado las credenciales de inicio de sesión de la iDRAC.

AVISO: El restablecimiento de la iDRAC a los valores predeterminados, restablece la iDRAC a todos los valores predeterminados de fábrica.

Configuración de la iDRAC mediante la utilidad de configuración de la iDRAC:

1. Reinicie el servidor y presione <F2>.
2. En la página **Configuración del sistema**, haga clic en **Configuración de iDRAC**.
3. Haga clic en **Restablecer la configuración de iDRAC a los valores predeterminados**.
4. Haga clic en **Sí** para confirmar y, a continuación, haga clic en **Atrás**.
5. Haga clic en **Finalizar**.

El servidor se reinicia después de que todos los valores de la iDRAC se establecen a los valores predeterminados.

Restablecimiento de la contraseña predeterminada mediante la RACADM local

1. Inicie sesión en el sistema operativo de host instalado en el sistema.
2. Acceda a la interfaz de RACADM local.
3. Siga las instrucciones en Cambio de la contraseña de inicio de sesión predeterminada mediante RACADM en la página 47.

Uso de OpenManage Mobile para restablecer la contraseña predeterminada

Puede utilizar OpenManage Mobile (OMM) para iniciar sesión y cambiar la contraseña predeterminada. Para iniciar sesión en iDRAC mediante OMM, escanee el código QR en la etiqueta de información del sistema. Para obtener más información sobre el uso de OMM, consulte la documentación de OMM en *Guía del usuario de OME - Modular para el chasis PowerEdge MX7000* disponible en https://www.dell.com/openmanagemanuals.

NOTA: El escaneo del código QR inicia la sesión en la iDRAC solo si las credenciales predeterminadas se encuentran en los valores predeterminados. Introduzca las credenciales actualizadas, si las cambió de los valores predeterminados.

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 de servidor

Cree un archivo de perfil de configuración de servidor (SCP) con una contraseña nueva 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 en la página 320.

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 en la página 320.

Cambio de la contraseña predeterminada mediante NIC de USB

Si tiene acceso a un teclado, un mouse y un dispositivo de pantalla, conéctelos al servidor con NIC de USB 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 en Cambio de la contraseña de inicio de sesión predeterminada mediante la interfaz web en la página 46.

Restablecimiento de la contraseña de iDRAC predeterminada remotamente

Si no dispone de 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, use cualquiera de las interfaces locales como RACADM o la interfaz web para cambiar la contraseña.

Sistema remoto sin aprovisionamiento

Si no hay ningún sistema operativo instalado en el servidor y si tiene una configuración de PXE disponible, utilice PXE y, a continuación, utilice 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.
- La función Advertencia de contraseña predeterminada está activada.
- Se proporcionan el nombre de usuario y la contraseña predeterminados de iDRAC en la etiqueta de información del sistema.

También se muestra un mensaje de advertencia cuando inicie sesión en iDRAC utilizando SSH, RACADM remoto o la interfaz web. En el caso de la interfaz Web y SSH, se muestra un único mensaje de advertencia en cada sesión. Respecto a RACADM remoto, aparece el mensaje de advertencia en cada comando.

NOTA: Para obtener información sobre los caracteres recomendados para los nombres de usuario y las contraseñas, consulte Caracteres recomendados para nombres de usuario y contraseñas en la página 154.

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 en la página 154.

3. En el campo **Confirmar contraseña**, introduzca nuevamente la contraseña.
4. Haga clic en **Continue (Continuar)**.

   Se configura la contraseña nueva y usted 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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

NOTA: Para obtener información sobre los caracteres recomendados para los nombres de usuario y las contraseñas, consulte Caracteres recomendados para nombres de usuario y contraseñas en la página 154.

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, realice lo siguiente:

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. 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 en la página 154.
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 visualización del mensaje de advertencia de contraseña predeterminada. Para ello, debe tener el privilegio Configure User (Configurar usuario).

Política de seguridad de contraseñas

Con la interfaz de iDRAC, puede revisar la política de seguridad de contraseñas y comprobar errores si no se cumple con la política. La política de contraseña no se puede aplicar a las contraseñas guardadas anteriormente, los perfiles de configuración del servidor (SCP) copiados de otros servidores y las contraseñas incorporadas en el perfil.

Para acceder a la configuración de las contraseñas, vaya a **Configuración de iDRAC** > **Usuarios** > **Configuración de contraseña**.

En esta sección, se encuentran disponibles los siguientes campos:

- **Puntuación mínima:** especifica la puntuación mínima de la política de seguridad de la contraseña. Los valores para este campo son:
  - 0: Sin protección
  - 1: Protección débil
  - 2: Nivel medio de protección
  - 3: Protección sólida
- **Política simple:** especifica los caracteres requeridos en una contraseña segura. Tiene las siguientes opciones:

- Letras mayúsculas
- Números
- Símbolos
- Longitud mínima

- **Expresión regular:** la expresión regular junto con la puntuación mínima se utiliza para el cumplimiento de la contraseña. Los valores válidos están entre 1 y 4.

Bloqueo de IP

Puede usar el bloqueo de IP para determinar dinámicamente cuándo se producen errores excesivos de inicio de sesión desde una dirección IP, bloquear o impedir que la dirección IP inicie sesión en la iDRAC9 durante un lapso preseleccionado. En el bloqueo de IP, se incluye lo siguiente:

- El número permitido de errores de inicio de sesión.
- El período en segundos en que se deben producir estos errores.
- La cantidad de tiempo, en segundos, en que se impide que la dirección IP establezca una sesión después de que se supere la cantidad total permitida de errores.

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

NOTA: Cuando se rechazan los intentos consecutivos de inicio de sesión provenientes de la dirección IP del cliente, es posible que algunos clientes de SSH muestren el siguiente mensaje:

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

.

NOTA: La función de bloqueo de IP admite hasta 5 rangos de IP. Puede ver o configurar estos solo mediante RACADM.

Tabla 8. Propiedades de restricción de reintentos de inicio de sesión

Propiedad	Definición
`iDRAC.IPBlocking.BlockEnable`	Habilita la función de bloqueo de IP. Cuando hay errores consecutivos `iDRAC.IPBlocking.FailCount` provenientes de una sola dirección IP dentro de una cantidad específica de tiempo `iDRAC.IPBlocking.FailWindow` se rechazan todos los demás intentos de establecer una sesión provenientes de esa dirección durante un lapso determinado `iDRAC.IPBlocking.PenaltyTime`
`iDRAC.IPBlocking.FailCount`	Establece la cantidad de errores de inicio de sesión provenientes de una dirección IP antes de que dichos intentos sean rechazados.
`iDRAC.IPBlocking.FailWindow`	El tiempo, en segundos, durante el cual se cuentan los intentos fallidos. Si ocurren errores más allá de este período, el contador se restablece.
`iDRAC.IPBlocking.PenaltyTime`	Este es el lapso establecido, en segundos, en el cual se deben rechazar todos los intentos de inicio de sesión provenientes de una dirección IP con una cantidad excesiva de errores.

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 **Configuración de iDRAC** > **Conectividad** > **Red** > **Paso del sistema operativo a iDRAC**.
   Se mostrará la página **Paso del sistema operativo a iDRAC**.
2. Cambie el estado a **Activado**.
3. Seleccione una de las siguientes opciones para el modo de paso:
   - **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.

   NOTA: Si establece el modo de paso en LOM, asegúrese de lo siguiente:
   - iDRAC y el sistema operativo se encuentran en la misma subred
   - La selección de NIC en la configuración de la red está establecida en una LOM
4. Si el servidor está conectado en el modo LOM compartido, el campo **Dirección IP del sistema operativo** estará desactivado.

   NOTA: Si la red VLAN está habilitada en iDRAC, LOM-Passthrough funcionará solamente en el modo LOM compartido con etiquetas de VLAN configuradas en el host.

   NOTA:
   - Cuando el modo de paso está establecido en LOM, no es posible iniciar iDRAC desde el SO del host después de un arranque en frío.
   - Se eliminó intencionalmente la función de paso de LOM mediante la función Modo dedicado.
5. Si selecciona **NIC de USB** como configuración de paso, introduzca la dirección IP de la NIC del USB.

   El valor predeterminado es 169.254.1.1. 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 de host o la red local, deberá cambiarla.

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

   NOTA: Si prefiere IPv6, la dirección predeterminada es fde1:53ba:e9a0:de11::1. Si es necesario, esta dirección se puede modificar en la configuración idrac.OS-BMC.UsbNicULA. Si no desea IPv6 en el NIC de USB, se puede desactivar cambiando la dirección a "::"
6. Haga clic en **Aplicar**.
7. 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 sobre el Server Administrator, consulte *Guía del usuario de OpenManage Server Administrator* disponible en https://www.dell.com/openmanagemanuals.

Temas:

Configuración de la dirección IP de iDRAC

Debe ajustar la configuración de red inicial según su infraestructura de red para habilitar la comunicación bidireccional con iDRAC. Puede configurar la dirección IP mediante una de las siguientes interfaces:

- Utilidad iDRAC Settings (Configuración de iDRAC)
- Lifecycle Controller (Consulte *Guía del usuario de Lifecycle Controller*)
- Panel LCD del chasis o servidor (Consulte *Manual de instalación y servicio* del sistema)

  NOTA: En los servidores blade, puede configurar las opciones de red mediante el panel LCD del chasis solo durante la configuración inicial de CMC. No es posible volver a configurar la iDRAC mediante el panel LCD del chasis una vez que este se implemente.
- Interfaz web de la CMC (no es válido para las plataformas MX) (consulte *Guía del usuario de la controladora de administración del chasis*)

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.
- Acceda al iDRAC mediante cualquiera de las interfaces siguientes:
  - Interfaz web de iDRAC mediante un explorador compatible (Internet Explorer, Firefox, Chrome o Safari)
  - Secure Shell (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.
  - 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 https://www.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.

Establecimiento de la configuración de red

Para establecer la configuración de red, realice lo siguiente:

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

1. En **Activar NIC**, seleccione **Activado**.
2. En el menú desplegable **Selección de NIC**, seleccione uno de los puertos siguientes en función de los requisitos de red:

   NOTA: Esta opción no está disponible en las plataformas MX.

   - **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. La opción Dedicado permite asignar una dirección IP a iDRAC a partir de la misma subred o de una distinta en comparación con las direcciones IP asignadas a los LOM o la NIC del host para administrar el tráfico de red.

     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 el caso de los servidores blade con dos puertos NDC, hay dos opciones LOM (LOM1 y LOM2) disponibles y, en los servidores con cuatro puertos NDC, las cuatro opciones LOM están disponibles.

   NOTA: Las LOM compartidas no son compatibles con *bNDC Intel X520–k 2P de 10 G* si se usan en un servidor de altura completa con dos NDC, ya que no son compatibles con el arbitraje de hardware.

3. En el menú desplegable **Selección de NIC**, elija el puerto desde el que desea acceder al sistema de manera remota; a continuación, se muestran las opciones:

   NOTA: Esta función no está disponible en las plataformas MX.

NOTA: Puede seleccionar la tarjeta de interfaz de red dedicada o una opción de una lista de LOM disponibles en las tarjetas intermedias de puerto doble o cuádruple.

- **Chasis (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. La opción Dedicado permite asignar una dirección IP a iDRAC a partir de la misma subred o de una distinta en comparación con las direcciones IP asignadas a los LOM o la NIC del host para administrar el tráfico de red.

- **Para tarjetas de puerto cuádruple: LOM1-LOM16**
- **Para tarjetas de puerto doble: LOM1, LOM2, LOM5, LOM6, LOM9, LOM10, LOM13, LOM14.**

4. En el menú desplegable **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: Esta opción está desactivada si la **Selección de NIC** está configurada en el modo **Dedicado**.

   NOTA: Cuando utiliza la configuración de la **red de conmutación por error**, se recomienda que todos los puertos LOM estén conectados a la misma red.

   Para obtener más información, consulte la sección Modificación de la configuración de red mediante la interfaz web en la página 98

5. 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.

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

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

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

   NOTA: Esta opción está desactivada si la **Negociación automática** está configurada en el modo **Activado**.

   NOTA: Si la formación de equipo de red está configurada para el sistema operativo host con el mismo adaptador de red que la selección de NIC; entonces, también se debe configurar la red de conmutación por error. En la selección de NIC y la red de conmutación por error, se deben utilizar los puertos que están configurados como parte del equipo de red. Si se utilizan más de dos puertos como parte del equipo de red, la selección de red de conmutación por error debe ser "Todos".

8. Bajo **MTU de NIC**, ingrese el tamaño de la unidad de transmisión máxima en la NIC.

   NOTA: El límite predeterminado y máximo para MTU en NIC es 1500 y el valor mínimo es 576. Si IPv6 está habilitado, se requiere un valor de MTU de 1280 o superior.

Configuración común

Si la infraestructura de red tiene servidor DNS, registre iDRAC en el DNS. Estos son los requisitos de los ajustes iniciales para funciones avanzadas, tales como servicios de directorio: Active Directory o LDAP, Single Sign On y tarjeta inteligente.

Para registrar iDRAC:

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

Para el campo **Nombre DNS de iDRAC**, el formato de nombre predeterminado es *idrac-Service_Tag*, donde Service_Tag es el número de la etiqueta de servicio del servidor. La longitud máxima es de 63 caracteres y se admiten los siguientes caracteres:

- A-Z
- a-z
- 0-9
- Guión (-)

Configuración de los valores de IPv4

Para configurar los valores de IPv4:

1. Seleccione la opción **Enabled (Activado)** en **Enable IPv4 (Activar IPv4)**.

   NOTA: En los servidores PowerEdge de 14.ª generación, DHCP está habilitado 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 **Use DHCP to obtain DNS server address (Usar DHCP para obtener dirección de servidor DNS)**, de modo que el servidor DHCP pueda asignar los valores de **Static Preferred DNS Server (Servidor DNS estático preferido)** y **Static Alternate DNS Server (Servidor DNS estático alternativo)**. De lo contrario, introduzca las direcciones IP para **Static Preferred DNS Server (Servidor DNS estático preferido)** y **Static Alternate DNS Server (Servidor DNS estático alternativo)**.

Configuring the IPv6 settings

Based on the infrastructure setup, you can use IPv6 address protocol.

To configure the IPv6 settings:

NOTE: If IPv6 is set to static, ensure that you configure the IPv6 gateway manually, which is not needed in case of dynamic IPV6. Failing to configure manually in case of static IPv6 results in loss of communication.

1. Select **Enabled** option under **Enable IPv6**.
2. For the DHCPv6 server to automatically assign the IP address and prefix length to iDRAC, select the **Enabled** option under **Enable Auto-configuration**.

   NOTE: You can configure both static IP and DHCP IP at the same time.

3. In the **Static IP Address 1** box, enter the static IPv6 address.
4. In the **Static Prefix Length** box, enter a value between 1 and 128.
5. In the **Static Gateway** box, enter the gateway address.

   NOTE: If you configure static IP, the current IP address 1 displays static IP and the IP address 2 displays dynamic IP. If you clear the static IP settings, the current IP address 1 displays dynamic IP.

6. If you are using DHCP, enable **DHCPv6 to obtain DNS Server addresses** to obtain Primary and Secondary DNS server addresses from DHCPv6 server. You can configure the following if required:
   - In the **Static Preferred DNS Server** box, enter the static DNS server IPv6 address.
   - In the **Static Alternate DNS Server** box, enter the static alternate DNS server.
7. When DNS information is not obtainable by either DHCPv6 or static configuration, you can use RFC 8106 "IPv6 Router Advertisement Options for DNS Configuration. It is identified by IPv6 Router. Using RA DNS configuration does not impact existing DNS configurations (either DHCPv6 or static).
   - The iDRAC can obtain DNS name server and DNS search domain information from IPv6 Router Advertisement messages. Please refer to RFC 8106 and your IPv6 router's user guide for details on how to configure the router to advertise this information.

- If DNS information is available from both the DHCPv6 server and the IPv6 Router Advertisement, the iDRAC uses both. In case of conflict, the DHCPv6 server's DNS information takes precedence in the iDRAC's /etc/resolv.conf settings.

NOTE: For iDRAC to use RA DNS information, IPv6.Enable and IPv6.Autoconfig must be enabled. If Auto-configuration is disabled, the iDRAC does not process IPv6 RA messages, and uses only static DNS settings as configured.

Configuración de los valores de IMPI

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 **Chasis (dedicado)**, los valores de VLAN son de solo lectura y solo se pueden cambiar mediante la CMC. Si el servidor está configurado en modo compartido, puede configurar los valores de VLAN en modo compartido en 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 Chassis Management Controller (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 CMC está disponible solamente para los servidores blade.

1. Inicie sesión en la interfaz web del CMC.
2. Vaya a **Configuración de iDRAC Configuración CMC**.
   Aparecerá la página **Implementar iDRAC**.
3. En **Configuración de red de iDRAC**, seleccione **Activar LAN** y otros parámetros de red según los requisitos. Para obtener más información, consulte *Ayuda en línea para la CMC*.
4. Para conocer valores de red adicionales específicos a cada servidor Blade, vaya a **Información general de servidor<nombre del servidor>**.
   Se muestra la página **Estado del servidor**.
5. Haga clic en **Iniciar iDRAC** y vaya a **Configuración de iDRAC Conectividad** > **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 la 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 *Guía del usuario de la controladora de administración del chasis* disponible en https://www.dell.com/cmcmanuals.

Descubrimiento automático

La función de detección automática permite que los servidores recién instalados detecten automáticamente la consola de administración remota que aloja el servidor de aprovisionamiento. El servidor de aprovisionamiento proporciona credenciales personalizadas de usuario administrativo para iDRAC, de modo que el servidor no aprovisionado pueda detectarse y administrarse desde la consola de administración. Para obtener más información acerca del servidor de aprovisionamiento, consulte *Guía de inicio rápido de servicios remotos de Lifecycle Controller* disponible en https://www.dell.com/idracmanuals.

El servidor de aprovisionamiento funciona con una dirección IP estática. La función de detección automática en iDRAC se utiliza para buscar el servidor de aprovisionamiento con DHCP/DNS de unidifusión/mDNS.

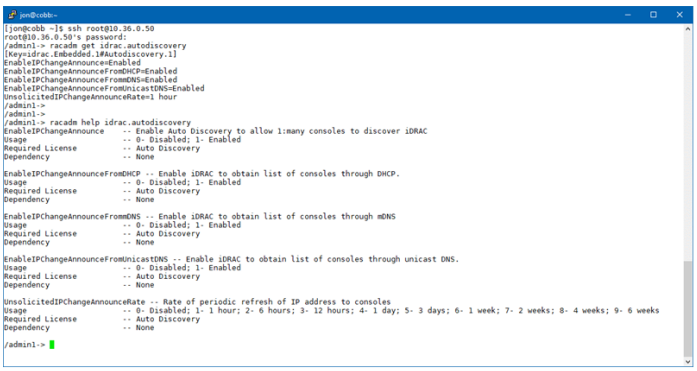
- Cuando iDRAC tiene la dirección de la consola, envía su propia etiqueta de servicio, la dirección IP, el número de puerto de Redfish, el certificado Web, etc.
- Esta información se publica periódicamente en las consolas.

DHCP, el servidor DNS o el nombre de host DNS predeterminado detecta el servidor de aprovisionamiento. Si se especifica un DNS, la dirección IP del servidor de aprovisionamiento se recupera desde el DNS y no se necesita la configuración de DHCP. Si se especifica el servidor de aprovisionamiento, se omite la detección, por lo que no se necesita DHCP ni DNS.

La detección automática se puede activar de las siguientes maneras:

1. Utilizando la GUI de iDRAC: **Configuración de iDRAC** > **Conectividad** > **Detección automática de iDRAC**

2. Utilizando RACADM:



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 **Configuración de iDRAC** > **Activación remota**.
   Se muestra la página **Activación remota de la configuración de iDRAC**.
3. Active el descubrimiento automático, introduzca la dirección IP del servidor de aprovisionamiento y haga clic en **Atrás**.

   NOTA: La especificación de la dirección IP del servidor de aprovisionamiento es opcional. Si no se establece, se detecta 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 aprovisiona todos los componentes en un servidor en una única operación. Estos componentes incluyen el BIOS, la iDRAC y PERC. Con la configuración automática, se importa automáticamente un archivo XML o JSON de perfil de configuración del servidor (SCP) que contiene todos los parámetros configurables. El servidor DHCP que asigna la dirección IP también proporciona los detalles para acceder al archivo SCP.

Los archivos SCP se crean mediante la configuración de un servidor de configuración gold. Luego, esta configuración se exporta a una ubicación de red compartida de NFS, CIFS, HTTP o HTTPS a la que puede acceder el servidor DHCP y la iDRAC del servidor que se está configurando. El nombre de archivo SCP se puede basar en la etiqueta de servicio o el número de modelo del servidor de destino, o bien se puede otorgar como nombre genérico. El servidor DHCP usa una opción de servidor DHCP para especificar el nombre de archivo SCP (de manera opcional), la ubicación de archivo SCP y las credenciales de usuario para acceder a la ubicación del archivo.

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

Las opciones de uso compartido de archivos HTTP y HTTPS son compatibles con el firmware de iDRAC 3.00.00.00 o posterior. Se deben proporcionar detalles de la dirección HTTP o HTTPS. En caso de que el proxy esté habilitado en el servidor, el usuario debe proporcionar ajustes de proxy adicionales para permitir que HTTP o HTTPS transfieran información. La marca de opción `-s` se actualiza como:

Tabla 9. Diferentes tipos de recursos compartidos y valores asignados

-s (ShareType)	asignación
NFS	`0` o `nfs`
CIFS	`2` o `cifs`
HTTP	`5` o `http`
HTTPS	`6` o `https`

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

En la siguiente lista, se describen los parámetros necesarios y opcionales asignados para el valor de la cadena:

`-f (Filename)`: nombre del archivo del perfil de configuración del servidor exportado. Esto se requiere en las versiones de firmware de iDRAC anteriores a 2.20.20.20.

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

`-s (ShareType)`: asignación de 0 para NFS, 2 para CIFS, 5 para HTTP y 6 para HTTPS. Este campo es obligatorio en las versiones de firmware de iDRAC 3.00.00.00.

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

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

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

`-d (ShutdownType)`: 0 para apagado ordenado o 1 para apagado forzado (configuración predeterminada: 0) Este campo es opcional.

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

`-e (EndHostPowerState)`: 0 para APAGADO o 1 para ENCENDIDO (valor predeterminado: 1). Este campo es opcional.

Las marcas de opciones adicionales son compatibles con el firmware de iDRAC 3.00.00.00 o posterior para habilitar la configuración de los parámetros del proxy HTTP y establecer el tiempo de espera de reintento a fin de acceder al archivo de perfil:

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

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

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

`—pu (ProxyUserName)`: nombre de usuario con acceso al servidor proxy. Este campo es necesario para la compatibilidad con proxy.

`—pp (ProxyPassword)`: contraseña de usuario con acceso al servidor proxy. Este campo es necesario para la compatibilidad con proxy.

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

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

Para las versiones de firmware de iDRAC 3.00.00.00 o posteriores, los archivos de perfil en formato JSON son compatibles. Los siguientes nombres de archivo se utilizarán si el parámetro de nombre de archivo no está presente:

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

NOTA: Para obtener más información sobre HTTP, consulte el informe técnico *14G Support for HTTP and HTTPS across IDRAC9 with Lifecycle Controller Interfaces* (Soporte 14G para HTTP y HTTPS a través de la IDRAC9 con interfaces de Lifecycle Controller) en https://www.dell.com/support.

NOTA:

- La configuración automática solo se puede activar cuando las opciones **DHCPv4** y **Activar IPV4** están activadas.
- Las funciones de configuración automática y detección automática son mutuamente excluyentes. Deshabilite la detección automática para que funcione la configuración automática.
- La configuración automática se deshabilita una vez que un servidor lleva a cabo una operación de configuración automática.

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

El usuario puede configurar servidores individuales que requieren distintos archivos de configuración asignados mediante modelos de servidores o etiquetas de servicio de servidores individuales. En un entorno que tiene diferentes servidores con requisitos específicos, se pueden usar distintos nombres de archivo SCP para distinguir cada servidor o tipo de servidor. Por ejemplo, si hay dos modelos de servidores para configurar, un PowerEdge R740s y un PowerEdge R540s, debe utilizar dos archivos SCP: `R740-config.xml` y `R540-config.xml`.

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

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, la iDRAC anuncia el 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. La iDRAC procesa el archivo SCP y configura todos los atributos que se enumeran en el archivo

Opciones de DHCP

DHCPv4 permite transferir varios 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 **Inicio** > **Herramientas de administración** > **DHCP** para abrir la herramienta de administración de 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 **Entrada 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 **Inicio** > **Herramientas de administración** > **DHCP** para abrir la herramienta de administración del servidor DHCP.
2. Encuentre el servidor y expanda los elementos que se ubican en él.
3. Haga clic con el botón derecho en **IPv4** y elija **Definir clases de proveedores**.
4. Haga clic en **Agregar**.
   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**. Aparecerá `060 iDRAC` en la columna **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 ayudará a importar el archivo de configuración 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 del perfil de configuración del servidor (SCP) exportado.
    - `Sharename (-n)`: Indica el nombre del recurso compartido de red.
    - `ShareType (-s)`:

      Además de ser compatible con el uso compartido de archivos basado en NFS y CIFS, el firmware de la iDRAC 3.00.00.00 (o versiones posteriores) también es compatible con el acceso a archivos de perfil mediante HTTP y HTTPS. El indicador `-s option` se actualiza de la siguiente manera:

      `-s (ShareType)`: Escriba nfs o 0 para NFS, cifs o 2 para CIFS, http o 5 para HTTP, o bien, https o 6 para HTTPS (obligatorio).
    - `IPAddress (-i)`: Indica la dirección IP del recurso compartido de archivos.

      NOTA: `Sharename (-n)`, `ShareType (-s)` e `IPAddress (-i)` son atributos obligatorios que deben incluirse. Para HTTP o HTTPs, el atributo -n no es obligatorio.
    - `Username (-u)`: Indica el nombre de usuario necesario para acceder al recurso compartido de red. Esta información es necesaria solo para CIFS.

- `Password (-p)`: Indica la contraseña necesaria para acceder al recurso compartido de red. Esta información es necesaria solo para CIFS.
- `ShutdownType (-d)`: Indica el modo de apagado. 0 Indica apagado ordenado y 1 indica 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.

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 <*NOMBRE DE USUARIO*> -p <*CONTRASEÑA*> -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:

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

  NOTA: Para obtener más información sobre las reglas de asignación de nombres de los archivos, consulte Configuración de servidores y componentes del servidor mediante la configuración automática en la página 57.
- Sharename (-n): indica el nombre del recurso compartido de red.
- ShareType (-s): indica el tipo de recurso compartido. 0 indica NFS, 2 indica CIFS, 5 indica HTTP y 6 indica HTTPS.

  NOTA: Ejemplo para el recurso compartido CIFS, HTTP, HTTPS y NFS de Linux:
  - **NFS**: `-f system_config.xml -i 192.168.0.130 -n /nfs -s 0 -d 0 -t 500`

    Asegúrese de utilizar NFS2 o NFS3 para el recurso compartido de red NFS.
  - **CIFS**: `-f system_config.xml -i 192.168.0.130 -n sambashare/config_files -s 2 -u user -p password -d 1 -t 400`
  - **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`
- 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. -n no se necesita para HTTP ni HTTPS.

- Username (-u): indica el nombre de usuario requerido para acceder al recurso compartido de red. Esta información se requiere solo para CIFS.
- Password (-p): indica la contraseña requerida para acceder al recurso compartido de red. Esta información se requiere solo para CIFS.
- ShutdownType (-d): indica el modo de apagado. 0 indica apagado ordenado y 1 indica apagado forzado.

  NOTA: El valor predeterminado es 0.
- Timetowait (-t): indica el tiempo que espera el sistema de 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 {
host my_host {
hardware ethernet b8:2a:72:fb:e6:56;
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 compatible (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 de que el servidor de seguridad y los permisos de usuario estén 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 de SCP 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**:
   - **Enable Once (Habilitar una vez)**: configura el componente solo una vez mediante el archivo de SCP al que hace referencia el servidor DHCP. Después de esto, se desactiva la configuración automática.
   - **Enable once after reset (Habilitar una vez después de restablecer)**: después de restablecer iDRAC, se configuran los componentes solo una vez mediante el archivo de SCP al que hace referencia 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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

Para obtener más información sobre la función de configuración automática, consulte el informe técnico *Zero-Touch, bare-metal server provisioning using the Dell EMC iDRAC with Lifecycle Controller Auto Config feature* (Aprovisionamiento de servidores físicos sin configurar mediante la función de configuración automática de Lifecycle Controller) disponible en https://www.dell.com/support.

Cómo usar contraseñas de algoritmos hash para obtener una mayor seguridad

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

Con la nueva función de contraseña de algoritmos hash:

- Puede generar sus propios algoritmos hash SHA256 para configurar contraseñas del BIOS y contraseñas de usuario de iDRAC. Esto le permite tener valores de SHA256 en el perfil de configuración de 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 de contraseñas de algoritmo hash o el reemplazo para la iDRAC. Puede utilizar SCP para la configuración de contraseñas de algoritmo hash o el reemplazo en la RACADM remota, WSMan o Redfish.
- Puede configurar un servidor plantilla 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 de servidor con los valores de algoritmo hash de las contraseñas. En la exportación se incluyen los valores hash que se necesitan para la autenticación de IPMI y SNMPv3. Después de importar este perfil, debe utilizar la versión más reciente de la herramienta Dell IPMI; si utiliza una versión más antigua, no se podrá realizar la autenticación de IPMI para los usuarios que tengan establecidos valores de contraseña con hash.
- 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 hash de contraseña SHA256 y no con otros (SHA1v3Key, MD5v3Key o IPMIKey), la autenticación mediante SNMP v3 e IPMI 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

NOTA: Los campos `SHA256Password` y `SHA256PasswordSalt` están reservados para la importación XML y no se configuran con herramientas de líneas de comandos. Es posible que al ajustar uno de los campos se bloquee el inicio de sesión en iDRAC del usuario actual. Cuando se importa una contraseña mediante `SHA256Password`, la iDRAC no aplicará la comprobación de la longitud de la contraseña.

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 / HTTP / HTTPS 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 atributos de algoritmo hash de contraseña nueva. Si se quita el comentario de ambas opciones, se genera un error y no se establece la contraseña. Un atributo con comentario no se aplica durante una importación.

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

La contraseña de hash puede generarse sin autenticación de SNMPv3 e IPMI con o sin Salt. Ambos requieren SHA256.

Para generar contraseñas de hash con Salt:

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 agrega una cadena binaria de 16 bytes. Se requiere que el atributo Salt tenga 16 bytes, si se proporciona. Una vez añadida, se convierte en una cadena de 32 caracteres. El formato es “contraseña” + “salt”, por ejemplo:

   Contraseña = SOMEPASSWORD

   Salt = ALITTLEBITOFSALT (se agregan 16 caracteres)

2. Abra un símbolo del sistema de Linux y ejecute el siguiente comando:

   ```
   Generate Hash-> echo-n SOMEPASSWORDALITTLEBITOFSALT|sha256sum  -><HASH>
   ```

   ```
   Generate Hex Representation of Salt -> echo -n ALITTLEBITOFSALT | xxd -p   -> <HEX-SALT>
   ```

   ```
   set iDRAC.Users.4.SHA256Password <HASH>
   ```

   ```
   set iDRAC.Users.4.SHA256PasswordSalt <HEX-SALT>
   ```

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

   NOTA: Si desea borrar una contraseña a la que se aplicó previamente el comando Salt, asegúrese de que la contraseña con el comando Salt esté configurado de forma explícita en una cadena vacía, es decir:

   ```
   set iDRAC.Users.4.SHA256Password
   ca74e5fe75654735d3b8d04a7bdf5dcdd06f1c6c2a215171a24e5a9dcb28e7a2
   ```

   ```
   set iDRAC.Users.4.SHA256PasswordSalt
   ```

4. Después de configurar la contraseña, la autenticación de contraseña de texto sin formato normal funcionará, excepto que no funcione la autentificación de SNMP v3 e IPMI para las cuentas de usuario de iDRAC que tengan contraseñas actualizadas con hash.

Modificación de la configuración de la cuenta de administrador local

Después de configurar la dirección IP de la iDRAC, puede modificar la configuración de la cuenta de administrador local (es decir, el usuario 2) mediante la utilidad de configuración de la 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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.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 enfriar un servidor puede aumentar en forma significativa la alimentación de todo el sistema. El control térmico es la administración activa del enfriamiento del sistema mediante la administración de la alimentación del sistema y la velocidad de los ventiladores, a fin de garantizar un sistema confiable y reducir la salida acústica del sistema, el flujo de aire y el consumo de energía del sistema. Puede ajustar la configuración del control térmico y optimizar el rendimiento del sistema y los requisitos de rendimiento por vatio.

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

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

A continuación, se muestra la lista de funciones de administración térmica:

- **Consumo de flujo de aire del sistema**: muestra el consumo de flujo de aire del sistema en tiempo real (en CFM), lo que permite el equilibrio del flujo de aire en el nivel del centro de datos y el rack.
- **Delta-T personalizado**: limita el aumento de la temperatura del aire desde la entrada hasta la salida para que se dimensione correctamente el enfriamiento en el nivel de la infraestructura.
- **Control de temperatura de salida**: especifica el límite de temperatura del aire que sale del servidor para que coincida con las necesidades del centro de datos.
- **Temperatura de entrada PCIe personalizada**: seleccione la temperatura correcta de entrada para que coincida con los requisitos del dispositivo de otros fabricantes.
- **Configuración del flujo de aire PCIe**: proporciona una vista completa del enfriamiento del dispositivo PCIe del servidor y permite la personalización del enfriamiento de las tarjetas de terceros.

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 **Configuración** > **Configuración del sistema** > **Configuración de hardware** > **Configuración de enfriamiento**.
2. Especifique lo siguiente:
   - **Optimización del perfil térmico**: seleccione el perfil térmico:
     - **Configuración del perfil térmico predeterminado (potencia mínima)**: implica que el algoritmo térmico utiliza la misma configuración de perfil del sistema que se definió en la página **BIOS del sistema** > **Configuración BIOS del sistema** > **Configuración del perfil del sistema**.

     De manera 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)**:
       - Dismunción 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.
     - **Límite de sonido**: esta opción reduce la salida acústica desde un servidor a costa de una pequeña reducción de rendimiento. La activación del límite de sonido puede incluir la implementación o la evaluación temporal de un servidor en un espacio ocupado, pero no debe usarse durante pruebas comparativas o aplicaciones que requieran mucho rendimiento.

     NOTA: Si selecciona **Rendimiento máximo** o **Alimentación mínima**, anula la configuración térmica asociada a la configuración del perfil del sistema en la página **BIOS del sistema** > **Configuración BIOS del sistema.Configuración del perfil del sistema**.
   - **Límite de temperatura de salida máximo**: en el menú desplegable, seleccione la temperatura de aire de salida máxima. Los valores se muestran según el sistema.

     El valor predeterminado es **Valor predeterminado, 70 °C (158 °F)**.

     Esta opción permite cambiar las velocidades de los ventiladores del sistema para que la temperatura de salida no supere el límite de temperatura de salida seleccionado. Esto no se puede garantizar siempre bajo todas las condiciones de funcionamiento del sistema debido a la dependencia en la carga del sistema y la capacidad de enfriamiento del sistema.
   - **Intervalos de velocidad del ventilador**: seleccionar esta opción permite el 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.
- **Apagado**: el intervalo de la velocidad del ventilador se establece 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. A su vez, 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 energía 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 puede utilizarse a fin de aumentar el enfriamiento del sistema para otros fines.

NOTA: El valor de configuración del VENTILADOR está disponible en iDRAC incluso cuando el sistema no tiene ningún VENTILADOR. Esto se debe a que, iDRAC envía la configuración especificada al administrador del chasis para procesar los datos de iDRAC y enviar el enfriamiento necesario al sistema según la configuración.

- **Umbrales**
  - **Límite de temperatura máximo de entrada de PCIe**: el valor predeterminado es 55 °C. Seleccione la temperatura mínima de 45 °C para tarjetas PCIe de terceros que requieren una menor temperatura de entrada.
  - **Límites de temperatura de salida**: mediante la modificación los valores de lo siguiente, puede establecer los límites de temperatura de salida:
    - **Establecer límite de temperatura de salida máximo**
    - **Establecer límite de aumento de la temperatura del aire**
  - **Velocidad mínima del ventilador en PWM (% del máximo)**: seleccione esta opción para realizar un ajuste preciso de la velocidad del ventilador. Si utiliza esta opción, puede configurar una velocidad más alta del ventilador del sistema de base o aumentar la velocidad del ventilador del sistema en caso de que otras opciones personalizadas de velocidad de ventiladores no generan las velocidades más altas requeridas.
    - **Predeterminado**: configura la velocidad mínima del ventilador con el valor predeterminado según lo establecido por el algoritmo de refrigeración del sistema.
    - **Personalizado**: ingrese el porcentaje que desee cambiar respecto de la velocidad del ventilador. El rango está entre 9 y 100.

    El intervalo permitido para velocidad mínima del ventilador en PWM se basa dinámicamente en la configuración del sistema. El primer valor es la velocidad en inactividad y el segundo valor es la configuración máxima (según la configuración del sistema, la velocidad máxima que puede ser hasta de un 100 %).

    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 velocidad mínima del ventilador a un 35 % limita la velocidad del ventilador para que nunca sea inferior al 35 % de PWM.

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

Los valores de configuración son persistentes, es decir que, una vez configurados y aplicados, no cambiarán automáticamente a la configuración predeterminada durante el reinicio del sistema, ciclos de encendido y apagado, actualizaciones del BIOS o de iDRAC. Es posible que las opciones personalizadas de refrigeración no sean compatibles con todos los servidores. Si no se admiten las opciones, no aparecerán o no se podrá proporcionar un valor personalizado.

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

   Aparece el mensaje siguiente:

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

4. 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 10. 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`
			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.`

Tabla 10. Configuración térmica (continuación)

Objeto	Descripción	Uso	Ejemplo
			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 muestra 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`

`FanSpeedMaxOffsetVal`	• Al obtener esta variable, se lee el valor de desplazamiento de velocidad del ventilador en % de PWM en	Valores de 0 a 100	`racadm get system.thermalsettings`

Tabla 10. Configuración térmica (continuación)

Objeto	Descripción	Uso	Ejemplo

	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.
			`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, esta compensación produce una velocidad 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 compensación se aplicará y los objetos `FanSpeedLowOffsetVal`, `FanSpeedMaxOffsetVal`,
		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 compensación de velocidad alta del ventilador (como se define en `FanSpeedHighOffsetVal`):
			`racadm set system.thermalsettings.FanSpeedOffset 1`

Tabla 10. Configuración térmica (continuación)

Objeto	Descripción	Uso	Ejemplo
	`FanSpeedHighOffsetVal` y `FanSpeedMediumOffsetVal` (definidos anteriormente) son los valores en los cuales se aplicará la compensación.		
`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.	Valores: • 1: Activado	Para desactivar cualquier conjunto de respuestas de

Tabla 10. Configuración térmica (continuación)

Objeto	Descripción	Uso	Ejemplo
	• 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.	• 0: Desactivado **NOTA:** El valor predeterminado es 1.	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.

Modificación de la configuración de flujo de aire de PCIe mediante la interfaz web de iDRAC

Utilice la configuración de flujo de aire de PCIe cuando se desea aumentar el margen térmico para las tarjetas PCIe de alta potencia personalizadas.

NOTA: La configuración de flujo de aire de PCIe no está disponible en las plataformas MX.

Realice lo siguiente para modificar la configuración de flujo de aire de PCIe:

1. En la interfaz web de iDRAC, vaya a **Configuración** > **Configuración del sistema** > **Configuración de hardware** > **Configuración de enfriamiento**.
   La página **Configuración de flujo de aire de PCIe** se muestra debajo de la sección de configuración del ventilador.
2. Especifique lo siguiente:
   - **Modo LFM**: seleccione el modo **Personalizado** para activar la opción de LFM personalizado.
   - **LFM personalizado**: ingrese el valor de LFM.
3. Haga clic en **Aplicar** para aplicar la configuración.

   Aparece el mensaje siguiente:

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

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

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

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: Se requiere Java 8 o posterior para usar esta función y para iniciar la consola virtual de iDRAC a través de una red IPv6.

4. Desde el DVD de *herramientas y documentación de Dell Systems Management*, instale VMCLI 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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.
5. Instale los elementos siguientes según los requisitos:
   - 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 estar en la misma red que CMC y OME Modular. Para obtener más información acerca de cómo aislar la red CMC de la red del sistema administrado, consulte *Guía del usuario de la controladora de administración del chasis* disponible en https://www.dell.com/cmcmanuals.
- 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 navegadores compatibles, consulte las *Notas de la versión* disponibles en https://www.dell.com/idracmanuals.

Se puede acceder a la mayoría de las funciones de la interfaz web de la iDRAC mediante el uso de estos navegadores con valores predeterminados. Para que se ejecuten ciertas funciones, debe cambiar algunas opciones de configuración. Estos valores incluyen deshabilitar bloqueadores de elementos emergentes, habilitar Java, ActiveX o la compatibilidad del plug-in de HTML5 y así sucesivamente.

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 la iDRAC, es posible que deba configurar ciertas opciones que se describen en esta sección. Puede utilizar otros navegadores compatibles con su configuración predeterminada.

NOTA: La configuración de proxy en blanco se trata de la misma forma que sin proxy.

Configuración de Internet Explorer

En esta sección, se proporcionan detalles acerca de la configuración de Internet Explorer (IE) para garantizar que usted pueda acceder a todas las funciones de la interfaz web de iDRAC y pueda utilizarlas. Esta configuración incluye:

- 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
- Desactivar 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 **Custom Level (Nivel personalizado)**, seleccione **Medium-Low (Medio-bajo)** y haga clic en **Reset (Restablecer)**. Haga clic en **OK** (Aceptar) para confirmar.

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

Cuando acceda a la interfaz web de la iDRAC, es posible que se le solicite que agregue la dirección IP de la iDRAC a la lista de los dominios de confianza si la dirección no está incluida en la lista. Cuando haya terminado, haga clic en **Actualizar** o vuelva a iniciar el navegador web para establecer una conexión a la interfaz web de la iDRAC. Si no se le solicita que agregue la dirección IP, se recomienda que la agregue 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 poder descargar los archivos de registro y otros elementos locales por medio de la interfaz web, se recomienda desactivar la opción Configuración de seguridad mejorada de Internet Explorer en 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 pueda acceder a todas las funciones de la interfaz web de la iDRAC y utilizarlas. Esta configuración incluye las siguientes funciones:

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

NOTA: Es posible que el navegador Mozilla Firefox no tenga una barra de desplazamiento en la página de ayuda en línea de la iDRAC.

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 instale un visor de consola virtual para cada iDRAC que 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 la preferencia)**, **Status (Estado)**, **Type (Tipo)** y **Value (Valor)** cambian a texto en negrita. El valor de **Status (Estado)** cambia a los valores establecidos por el usuario y el valor de **Value (Valor)** cambia a falso.
4. En la columna **Nombre de la preferencia**, busque **xpinstall.enabled**.
   Asegúrese de que el valor de **Value (Valor)** sea **true (verdadero)**. De no ser así, haga doble clic en **xpinstall.enabled** para establecer el valor de **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 de Firefox, introduzca `about:config`.
2. En la sección **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 https://www.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 es compatible solamente con Internet Explorer. HTML5 o un visor de Java se admiten en cualquier explorador.

   NOTA: Se requiere Java 8 o posterior para usar esta función y para iniciar la consola virtual de iDRAC a través de una 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` se puede incluir en el paquete de .NET Framework o en el paquete del 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 medios virtuales y consola virtual de HTML5 se crean con la tecnología HTML5. A continuación, se enumeran los beneficios 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 medios virtuales y consola virtual 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 Microsoft Edge para utilizar el complemento basado en HTML5

Debe configurar los ajustes de Edge antes de iniciar y ejecutar aplicaciones de consola virtual y de medios virtuales basadas en HTML5. Para configurar los valores del explorador:

1. Haga clic en **Configuración** > **Ver configuración avanzada** y desactive la opción **Bloquear ventanas emergentes**.
2. Modifique la dirección IPv6 de la siguiente forma:

   ```
   https://2607:f2b1:f083:147::1eb.ipv6:literal.net/restgui to https://2607-f2b1-f083-147--1eb.ipv6-literal.net/restgui
   ```

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.

En los sistemas operativos de 64 bits, puede instalar ambas versiones (de 32 bits o 64 bits) de Internet Explorer. Puede utilizar la versión de 32 bits o 64 bits; no obstante, debe instalar el complemento correspondiente. Por ejemplo, si instala el complemento en el navegador de 64 bits y luego abre el visor en un navegador de 32 bits, deberá instalar el complemento nuevamente.

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 de ActiveX:

1. Borre la memoria caché del explorador.
2. Agregue el nombre de host o la dirección IP de iDRAC a la lista **Sitios locales de Internet**.
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 IP de iDRAC. Para ello, haga clic en **Herramientas** > **Configuración de Vista de compatibilidad**.

   NOTA:
   - Las diferentes versiones de Internet Explorer comparten los valores 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 último cuando Internet Explorer muestre una advertencia de seguridad.
   - Si aparece el error **Editor desconocido** mientras se inicia la consola virtual, es posible que se deba al cambio de la ruta de acceso del certificado de firma de código. Para solucionar este error, debe descargar una clave adicional. Utilice 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 **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

Cuando inicia la consola virtual o los medios virtuales, se muestran los indicadores para verificar los certificados. Si tiene certificados de servidor web personalizados, puede evitar estos indicadores mediante la importación de certificados de CA al almacenamiento de certificados de confianza de Java o ActiveX.

Para obtener más información acerca de la inscripción automática de certificados (ACE), consulte la sección Inscripción automática de certificados en la página 116

Importación de certificados de CA al almacén de certificados de confianza de Java

Para importar el certificado de CA al almacén de certificados de confianza de Java:

1. Inicie el **Panel de control de Java**.
2. Seleccione la ficha **Seguridad** y haga clic en **Certificados**.
   Se muestra el cuadro de diálogo **Certificados**.
3. En el menú desplegable Tipo de certificado, seleccione **Certificados de confianza**.
4. Haga clic en **Importar**, seleccione el certificado de CA (en formato de codificación Base64) y haga clic en **Abrir**.
   El certificado seleccionado se importa al almacén de certificados de confianza de inicio web.
5. Haga clic en **Cerrar** y, a continuación, en **Aceptar**. Se cierra la ventana **Java Control Panel (Panel de control de Java)**.

Importación de certificados de CA al almacén de certificados de confianza de ActiveX

Debe utilizar la herramienta de línea de comandos OpenSSL para crear el algoritmo hash del certificado mediante el algoritmo hash seguro (SHA). Se recomienda utilizar la herramienta OpenSSL 1.0.x o una versión posterior, ya que esta utiliza SHA de

manera predeterminada. El certificado de CA debe estar codificado en formato PEM Base64. Este es un proceso único que se debe realizar para importar cada certificado 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 en la estación de administración mediante el comando: `openssl x509 -in (name of CA cert) -noout -hash`.

   Se generará un archivo de salida. Por ejemplo, si el nombre de archivo del certificado de CA es **cacert.pem**, 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 idioma admitidas. Para algunos idiomas admitidos, se deberá cambiar el tamaño de la ventana del navegador 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 idioma admitidas. Algunas funciones de la interfaz web de iDRAC, como la consola virtual, podrían requerir pasos adicionales para acceder a funciones o letras específicas. Otros teclados no son compatibles y podrían provocar problemas inesperados.

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

Updating device firmware

Using iDRAC, you can update the iDRAC, BIOS, and all device firmware that is supported by using Lifecycle Controller update such as:

- Fibre Channel (FC) cards
- Diagnostics
- Operating System Driver Pack
- Network Interface Card (NIC)
- RAID Controller
- Power Supply Unit (PSU)
- NVMe PCIe devices
- SAS/SATA hard drives
- Backplane update for internal and external enclosures
- OS Collector

CAUTION: The PSU firmware update may take several minutes depending on the system configuration and PSU model. To avoid damaging the PSU, do not interrupt the update process or power on the system during PSU firmware update.

NOTE: When updating the PSU firmware for PowerEdge C series servers, ensure that all servers in the same chassis are powered OFF first. If any of the other servers in the chassis are powered ON, the update process fails.

You must upload the required firmware to iDRAC. After the upload is complete, the current version of the firmware installed on the device and the version being applied is displayed. If the firmware being uploaded is not valid, an error message is displayed. Updates that do not require a reboot are applied immediately. Updates that require a system reboot are staged and committed to run on the next system reboot. Only one system reboot is required to perform all updates.

NOTE:

- When SEKM mode is enabled on a controller, iDRAC Firmware downgrade/upgrade shall fail when tried from a SEKM to a non-SEKM iDRAC version. iDRAC Firmware upgrade/downgrade shall pass when done within the SEKM versions.
- PERC firmware downgrade shall fail when SEKM is enabled.

After the firmware is updated, the **System Inventory** page displays the updated firmware version and logs are recorded.

The supported firmware image file types are:

- `.exe` — Windows-based Dell Update Package (DUP). You must have Control and Configure Privilege to use this image file type.
- `.d9` — Contains both iDRAC and Lifecycle Controller firmware

For files with `.exe` extension, you must have the System Control privilege. The Remote Firmware Update licensed feature and Lifecycle Controller must be enabled.

For files with `.d9` extension, you must have the Configure privilege.

NOTE: Ensure that all nodes in the system are powered off before updating the PSU firmware.

NOTE: After upgrading the iDRAC firmware, you may notice a difference in the time stamp displayed in the Lifecycle Controller log. Time displayed in LC Log is different from NTP/Bios-Time for few logs during idrac reset.

You can perform firmware updates by using the following methods:

- Uploading a supported image type, one at a time, from a local system or network share.
- Connecting to an FTP, TFTP, HTTP or HTTPS site or a network repository that contains Windows DUPs and a corresponding catalog file.

  You can create custom repositories by using the Dell Repository Manager. For more information, see *Dell Repository Manager Data Center User's Guide*. iDRAC can provide a difference report between the BIOS and firmware installed on the system and the updates available in the repository. All applicable updates contained in the repository are applied to the system. This feature is available with iDRAC Enterprise or Datacenter license.

  NOTE: HTTP/HTTPS only supports with either digest authentication or no authentication.
- Scheduling recurring automated firmware updates by using the catalog file and custom repository.

There are multiple tools and interfaces that can be used to update the iDRAC firmware. The following table is applicable only to iDRAC firmware. The table lists the supported interfaces, image-file types, and whether Lifecycle Controller must be in enabled state for the firmware to be updated.

Table 11. Image file types and dependencies

	.D9 Image		iDRAC DUP	
Interface	**Supported**	**Requires LC enabled**	**Supported**	**Requires LC enabled**
BMCFW64.exe utility	Yes	No	No	N/A
Racadm FWUpdate (old)	Yes	No	No	N/A
Racadm Update (new)	Yes	Yes	Yes	Yes
iDRAC UI	Yes	Yes	Yes	Yes
WSMan	Yes	Yes	Yes	Yes
In-band OS DUP	No	N/A	Yes	No
Redfish	Yes	N/A	Yes	N/A

The following table provides information on whether a system restart is required when firmware is updated for a particular component:

NOTE: When multiple firmware updates are applied through out-of-band methods, the updates are ordered in the most efficient possible manner to reduce unnecessary system restart.

Table 12. Firmware update — supported components

Component Name	Firmware Rollback Supported? (Yes or No)	Out-of-band — System Restart Required?	In-band — System Restart Required?	Lifecycle Controller GUI — Restart Required?
Diagnostics	No	No	No	No
OS Driver Pack	No	No	No	No
iDRAC	Yes	No	No*	Yes
BIOS	Yes	Yes	Yes	Yes
RAID Controller	Yes	Yes	Yes	Yes
BOSS	Yes	Yes	Yes	Yes
NVDIMM	No	Yes	Yes	Yes
Backplanes	Yes	Yes	Yes	Yes
NOTE: • For Expander (Active) backplanes, system restart is required. • For SEP (Passive) backplanes, rebootless update is supported only from 4.00.00.00 release onwards.				
Enclosures	Yes	Yes	No	Yes
NIC	Yes	Yes	Yes	Yes
Power Supply Unit	Yes	Yes	Yes	Yes
CPLD	No	Yes	Yes	Yes
NOTE: After CPLD firmware upgrade is complete, iDRAC restarts automatically.				
FC Cards	Yes	Yes	Yes	Yes
NVMe PCIe SSD drives	Yes	Yes	Yes	Yes
SAS/SATA hard drives	No	Yes	Yes	No
OS Collector	No	No	No	No
CMC (on PowerEdge FX2 servers)	No	Yes	Yes	Yes
TPM	No	Yes	Yes	Yes
Non-SDL Software and Peripherals Application	No	No	No	No

NOTE:

- TPM firmware update is supported from 5.00.00.00 release onwards and this action is staged. Downgrading (rollback) or reinstalling the same firmware version is not supported.
- TPM does not support rollback.
- When stacking TPM firmware update with BIOS update (unsupported TPM version), TPM update fails.
- Once iDRAC is flashed or TPM is inserted, first time host reboot with POST completion is required to fetch the TPM details from BIOS and detect TPM in software inventory.
- Latest BIOS version is needed for TPM firmware updates to be supported using iDRAC interfaces. Recommended to update BIOS first before updating iDRAC.
- TPM must be enabled in BIOS first before you can perform firmware update using iDRAC interfaces.

NOTE: For details of supported components for MX platform, see Table 13.

Table 13. Firmware update — supported components for MX platforms

Component Name	Firmware Rollback Supported? (Yes or No)	Out-of-band — System Restart Required?	In-band — System Restart Required?	Lifecycle Controller GUI — Restart Required?
Diagnostics	No	No	No	No
OS Driver Pack	No	No	No	No
iDRAC	Yes	No	No*	Yes
BIOS	Yes	Yes	Yes	Yes
RAID Controller	Yes	Yes	Yes	Yes
BOSS	Yes	Yes	Yes	Yes
NVDIMM	No	Yes	Yes	Yes
Backplanes	Yes	Yes	Yes	Yes
Enclosures	Yes	Yes	No	Yes
NIC	Yes	Yes	Yes	Yes
Power Supply Unit	No	No	No	No
CPLD	No	Yes	Yes	Yes
FC Cards	Yes	Yes	Yes	Yes
NVMe PCIe SSD drives	Yes	Yes	No	No
SAS/SATA hard drives	No	Yes	Yes	No
OS Collector	No	No	No	No

* Indicates that though a system restart is not required, iDRAC must be restarted to apply the updates. iDRAC communication and monitoring may temporarily be interrupted.

When you check for updates, the version marked as **Available** does not always indicate that it is the latest version available. Before you install the update, ensure that the version you choose to install is newer than the version currently installed. If you want to control the version that iDRAC detects, create a custom repository using Dell Repository Manager (DRM) and configure iDRAC to use that repository to check for updates.

Actualización del firmware mediante la interfaz web de iDRAC

Puede actualizar el firmware del dispositivo utilizando imágenes de firmware disponibles en el sistema local, desde un repositorio en un recurso compartido de red (CIFS, NFS, HTTP o HTTPS) o desde 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 **Mantenimiento** > **Actualización del sistema**.

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

2. En la pestaña **Actualizar**, seleccione **Local** como el **Tipo de ubicación**.

   NOTA: Si selecciona Local, asegúrese de descargar la imagen del firmware en una ubicación del sistema local. Seleccione un archivo que se apilará en el iDRAC para su actualización. Puede seleccionar otros archivos, uno a la vez, y cargarlos en la iDRAC. Los archivos se cargan en un espacio temporal de la iDRAC y tienen un límite aproximado de 300 MB.

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 **Contenidos** se muestra un ícono con el signo más (+) junto al nombre del archivo de imagen de firmware. Expanda el nombre para ver la información de la versión de firmware **Nombre de dispositivo**, **Actual** y **Versión de firmware disponible**.

5. Seleccione el archivo de firmware necesario y realice una de las acciones siguientes:
   - En el caso de las imágenes del firmware que no requieren un reinicio del sistema host, haga clic en **Instalar** (única opción disponible). 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**.

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

6. Para mostrar la página **Cola de trabajos**, haga clic en **Cola de trabajos**. Utilice esta página para ver y administrar las actualizaciones de firmware por etapas o haga clic en **Aceptar** para actualizar la página actual y ver el estado de la actualización de firmware.

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

NOTA: No podrá continuar, si la sesión se ha vencido después de cargar el archivo de firmware. Este problema solo se puede resolver mediante el `reset` de RACADM.

NOTA: Una vez que se completa la actualización de firmware, aparece el mensaje de error: `RAC0508: An unexpected error occurred. Wait for few minutes and retry the operation. If the problem persists, contact service provider.` Esto es normal. Puede esperar unos instantes y actualizar el navegador. Luego, será redirigido a la página de inicio de sesión.

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, la iDRAC se conecta al destino especificado, busca nuevas actualizaciones y aplica o divide en etapas todas las actualizaciones aplicables. El archivo de registro se crea en el servidor remoto, el cual 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 la iDRAC para que utilice este repositorio para buscar y realizar actualizaciones de firmware. El uso de un repositorio interno permite controlar el firmware y las versiones disponibles para iDRAC y ayuda a evitar cualquier cambio involuntario de firmware.

NOTA: Para obtener más información sobre DRM, consulte www.dell.com/openmanagemanuals > Administrador del repositorio.

Se necesita una licencia de iDRAC Enterprise o Datacenter 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 de archivos de catálogo y la transferencia de archivos a través de 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
```

Actualización del firmware de dispositivos mediante RACADM

Para actualizar el firmware del dispositivo mediante RACADM, utilice el subcomando `update`. Para obtener más información, consulte *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

Ejemplos:

- 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
```

- 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
```

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

Algunas versiones de los DUP se crean de modo que entran en conflicto entre sí. Esto sucede con el tiempo a medida que se crean nuevas versiones del software. Puede que una versión más reciente del software sea compatible con dispositivos heredados. Se puede agregar compatibilidad para los dispositivos nuevos. Considere, por ejemplo, los dos DUP Network_Firmware_NDT09_WN64_21.60.5.EXE y Network_Firmware_8J1P7_WN64_21.60.27.50.EXE. Los dispositivos admitidos por estos DUP caben en tres grupos.

- El grupo A son los dispositivos heredados que solo son compatibles con NDT09.

- El grupo B son los dispositivos compatibles con NDT09 y 8J1P7.
- El grupo C son los dispositivos nuevos admitidos solo por 8J1P7.

Considere un servidor que tenga uno o más dispositivos de cada uno de los grupos A, B y C. Si los DUP se utilizan de a uno a la vez, deberían funcionar correctamente. Utilizar NDT09 por sí mismo actualiza los dispositivos del grupo A y del grupo B. Utilizar 8J1P7 por sí mismo actualiza los dispositivos del grupo B y del grupo C. Sin embargo, si intenta utilizar ambos DUP al mismo tiempo, pueden intentar crear dos actualizaciones para los dispositivos del grupo B al mismo tiempo. Esto puede fallar con un error válido: "El trabajo para este dispositivo ya está presente". El software de actualización no puede resolver el conflicto de dos DUP válidos intentando dos actualizaciones válidas en los mismos dispositivos al mismo tiempo. Al mismo tiempo, ambos DUP son necesarios para admitir dispositivos del grupo A y del grupo C. El conflicto también se extiende a la realización de reversiones en los dispositivos. Como práctica recomendada, se sugiere usar cada DUP individualmente.

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 el reinicio del sistema después de completar la actualización del 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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

Actualización del firmware mediante Lifecycle Controller Remote Services

Para obtener información sobre cómo actualizar el firmware mediante Lifecycle Controller Remote Services, consulte *Guía de inicio rápido de servicios remotos de Lifecycle Controller* disponible en https://www.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 **Chassis Management at Server Mode (Modo de 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 (Modo de administración de chasis en el 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 que están en espera 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 sobre los campos mostrados, consulte *iDRAC Online Help (Ayuda en línea de iDRAC)*.

Para eliminar uno o varios trabajos, seleccione los trabajos correspondientes 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. Puede eliminar todos los trabajos puestos en cola para su ejecución durante el próximo reinicio. No puede eliminar los trabajos activos; es decir, los trabajos 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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

Reversión del firmware del dispositivo

Puede revertir el firmware para iDRAC o cualquier dispositivo compatible con Lifecycle Controller, incluso si la actualización se realizó anteriormente con otra interfaz. Por ejemplo, si el firmware se actualizó con la interfaz gráfica del usuario de Lifecycle Controller, puede revertirlo con la interfaz web de iDRAC. Puede realizar la reversión del firmware para varios 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, con la reversión del firmware de la iDRAC también se revierte el firmware de Lifecycle Controller.

Se recomienda mantener el firmware actualizado para asegurarse de que tiene las funciones y actualizaciones de seguridad más recientes. Es posible que deba revertir una actualización o instalar una versión anterior si encuentra algún problema después de una actualización. Para instalar una versión anterior, utilice Lifecycle Controller para ver si hay actualizaciones y seleccione la versión que desea instalar.

Para conocer detalles acerca de los componentes compatibles y no compatibles con la reversión de firmware, consulte la tabla Firmware update — supported components en la página 81

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 de CMC (no compatible con las plataformas MX)
- Interfaz web de OME-Modular (compatible con las plataformas MX)
- Interfaz de la línea de comandos de CMC RACADM (no compatible con las plataformas MX)
- iDRAC RACADM CLI
- 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 en la página 88.

Reversión del firmware mediante RACADM

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

   ```
   racadm swinventory
   ```

   Para el dispositivo para el que desea revertir el firmware, la `Rollback Version` debe estar `Available`. Además, anote los FQDD.

2. Revierta el firmware del dispositivo mediante:

   ```
   racadm rollback <FQDD>
   ```

   Para obtener más información, consulte *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

Reversión del firmware mediante Lifecycle Controller

Para obtener información, consulte *Guía del usuario de Lifecycle Controller* disponible en https://www.dell.com/idracmanuals.

Reversión del firmware mediante Lifecycle Controller Remote Services

Para obtener información, consulte *Guía de inicio rápido de servicios remotos de Lifecycle Controller* disponible en https://www.dell.com/idracmanuals.

Recuperación de iDRAC

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 identificación y estado del sistema parpadea en intervalos de ~1/2 segundos. (El LED se encuentra en la parte posterior de los servidores en rack y en torre, y en la parte frontal de los un servidores 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 a ámbar sólido, lee el archivo firmimg.d9, vuelve a programar iDRAC y luego reinicia la iDRAC.

Easy Restore

En la restauración fácil, se utiliza la memoria flash de la restauración fácil para respaldar los datos. Cuando reemplaza la placa base y enciende el sistema, el BIOS consulta a la iDRAC y le solicita restaurar los datos de la copia de seguridad. En la primera pantalla del BIOS, se le solicita que restaure la etiqueta de servicio, las licencias y la aplicación de diagnóstico de UEFI. En la segunda pantalla del BIOS, se le solicita que restaure los valores de la configuración del sistema. Si elige no restaurar los datos en la primera pantalla del BIOS y si no configura la etiqueta de servicio mediante otro método, se volverá a mostrar la primera pantalla del BIOS. La segunda pantalla del BIOS se muestra solo una vez.

NOTA:

- Los valores de configuración del sistema se respaldan solo cuando la opción Recopilar inventario del sistema tras reiniciar (CSIOR) está activada. Asegúrese de que Lifecycle Controller y CSIOR estén activados.
- 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.

Después de reemplazar la tarjeta madre del servidor, la Restauración fácil permite restaurar automáticamente los siguientes datos:

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

NOTA: En los servidores con iDRAC versión 3.00.00.00 en adelante, la Restauración fácil se realiza automáticamente en 5 minutos si no se produce una interacción del usuario.

A continuación, se indican los detalles de duración de tiempo necesarios para realizar algunas acciones de restauración:

- La restauración de los contenidos del sistema, como los diagnósticos, el registro de eventos del sistema (SEL) y el módulo de ID de OEM generalmente tarda menos de un minuto.
- La restauración de los datos de configuración del sistema (iDRAC, BIOS, NIC) puede tardar varios minutos (en algunos casos aproximadamente 10 minutos) en completarse.

NOTA: Durante este tiempo, no aparece ninguna indicación ni barra de progreso, y es posible que el servidor se reinicie un par de veces para completar la restauración de la configuración.

Supervisión de iDRAC mediante otras herramientas de administración del sistema

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

Perfil de configuración de servidor admitido: importación y exportación

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

NOTA: Debe tener privilegios de administrador para realizar la tarea Exportar e importar SCP.

Puede importar y exportar desde la estación de administración local y desde un recurso compartido de red a través de CIFS, NFS, HTTP o HTTPS. Con SCP, puede seleccionar e importar o exportar configuraciones a nivel de componente para el BIOS, la NIC y RAID. Puede importar y exportar SCP a la estación de administración local o a un recurso compartido de red de CIFS, NFS, HTTP o HTTPS. Puede importar y exportar perfiles individuales de la iDRAC, del BIOS, de la NIC y de RAID, o bien todos juntos como un solo archivo.

Puede especificar una vista previa de la importación o exportación de SCP donde se está ejecutando el trabajo y se genera un resultado de la configuración, pero no se aplica ninguno de los valores de la configuración.

Se creará un trabajo una vez que la importación o exportación se haya iniciado a través de la GUI. El estado de los trabajos puede verse en la página Línea de espera de trabajos.

NOTA:

- Solo se acepta el nombre de host o la dirección IP para la dirección de destino.
- Puede buscar una ubicación específica para importar los archivos de configuración de servidor. Deberá seleccionar el archivo de configuración de servidor correcto que desee importar. Por ejemplo: import.xml.
- Según el formato del archivo exportado (que usted seleccionó), se agrega la extensión correspondiente de forma automática. Por ejemplo, import.xml.
- Durante la exportación, el nombre de archivo SCP puede cambiar. Por ejemplo, con.xml to _con.xml.
- SCP aplica la configuración completa en un solo trabajo con la cantidad mínima de reinicios. Sin embargo, en algunas configuraciones de sistema, algunos atributos cambian el modo de operación de un dispositivo, o bien es posible que creen dispositivos secundarios con atributos nuevos. Cuando esto sucede, es posible que SCP no pueda aplicar todas las configuraciones durante un trabajo único. Revise las entradas de ConfigResult del trabajo para solucionar cualquier ajuste de configuración pendiente.

SCP le permite realizar una implementación del sistema operativo (OSD) mediante un único archivo XML/JSON en varios sistemas. Además, puede realizar las operaciones existentes a la vez, como configuraciones y actualizaciones del repositorio.

SCP también permite exportar e importar claves públicas de SSH para todos los usuarios de iDRAC. Hay 4 claves públicas de SSH para todos los usuarios.

A continuación, se indican los pasos para la implementación del sistema operativo mediante SCP:

1. Exportar archivo SCP
2. El archivo SCP contiene todos los atributos suprimidos que se necesitan para realizar la OSD.
3. Edite o actualice los atributos de OSD y, a continuación, ejecute la operación de importación.
4. Luego, SCP Orchestrator valida estos atributos de OSD.
5. SCP Orchestrator ejecuta la configuración y las actualizaciones del repositorio especificadas en el archivo SCP.
6. Una vez finalizada la configuración y las actualizaciones, se apaga el sistema operativo host.

   NOTA: Solo se admiten los recursos compartidos de CIFS y NFS para alojar los medios del sistema operativo.
7. SCP Orchestrator inicia la OSD mediante la conexión de los controladores para el sistema operativo seleccionado y, a continuación, inicia un arranque único en los medios del SO presentes en NFS/recurso compartido.
8. LCL muestra el progreso del trabajo.
9. Una vez que el BIOS se inicia en los medios del sistema operativo, el trabajo de SCP aparece como completo.
10. Los medios conectados y los medios del sistema operativo se desconectarán automáticamente después de 65.535 segundos o después de la duración especificada por el atributo `OSD.1#ExposeDuration`.

Importación del perfil de configuración del servidor mediante la interfaz web de iDRAC

Para importar el perfil de configuración del servidor, realice lo siguiente:

1. Vaya a **Configuración** > **Perfil de configuración del servidor**
   Aparecerá la página **Perfil de configuración del servidor**.
2. Seleccione una de las siguientes opciones para especificar el tipo de ubicación:
   - **Local** para importar el archivo de configuración guardado en una unidad local.
   - **Recurso compartido de red** para importar el archivo de configuración desde el recurso compartido CIFS o NFS.
   - **HTTP o HTTPS** para importar el archivo de configuración desde un archivo local mediante la transferencia de archivos HTTP/HTTPS.

   NOTA: Según el tipo de ubicación, debe ingresar la configuración de red o la configuración de HTTP/HTTPS. Si el proxy está configurado para HTTP/HTTPS, también se requiere la configuración de proxy.
3. Seleccione los componentes que se indican en la opción **Importar componentes**.
4. Seleccione el tipo de **apagado**.
5. Seleccione el **Tiempo máximo de espera** para especificar el tiempo de espera antes de que el sistema se apague después de que finalice la importación.
6. Haga clic en **Importar**.

Exportación del perfil de configuración del servidor mediante la interfaz web del iDRAC

Para exportar el perfil de configuración del servidor, realice lo siguiente:

1. Vaya a **Configuración** > **Perfil de configuración del servidor**
   Aparecerá la página **Perfil de configuración del servidor**.
2. Haga clic en **Exportar**.
3. Seleccione una de las siguientes opciones para especificar el tipo de ubicación:
   - **Local** para guardar el archivo de configuración en una unidad local.
   - **Recurso compartido de red** para guardar el archivo de configuración en un recurso compartido CIFS o NFS.
   - **HTTP o HTTPS** para guardar el archivo de configuración en un archivo local mediante la transferencia de archivos HTTP/HTTPS.

   NOTA: Según el tipo de ubicación, debe ingresar la configuración de red o la configuración de HTTP/HTTPS. Si el proxy está configurado para HTTP/HTTPS, también se requiere la configuración de proxy.
4. Seleccione los componentes para los que desea respaldar la configuración.
5. Seleccione el **Tipo de exportación**; a continuación, se presentan las opciones:
   - **Básico**
   - **Exportación de reemplazo**
   - **Exportación de clonación**
6. Seleccione un **Formato de archivo de exportación**.
7. Seleccione **Elementos adicionales de exportación**.
8. Haga clic en **Exportar**.

Configuración de arranque seguro mediante la configuración del BIOS o F2

El arranque seguro de UEFI es una tecnología que permite eliminar un vacío de seguridad importante que puede ocurrir durante una transferencia entre el firmware de UEFI y el sistema operativo (SO) de UEFI. En el arranque seguro de UEFI, cada componente de la cadena se valida y autoriza según un certificado específico antes de que se pueda cargar o ejecutar. Con el arranque seguro, se elimina la amenaza y se verifica la identidad del software en cada paso del arranque: firmware de plataforma, tarjetas de opción y cargador de arranque del SO.

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

Cuando está activado, con el arranque seguro de UEFI, se evita que se carguen los controladores de dispositivo de UEFI sin firmar, se muestra un mensaje de error y no se permite que el dispositivo funcione. Debe desactivar el arranque seguro para cargar los controladores de dispositivo sin firmar.

En la 14.ª generación y versiones posteriores de los servidores Dell PowerEdge, puede habilitar o deshabilitar la función de arranque seguro mediante el uso de diferentes interfaces (RACADM, WSMAN, REDFISH y LC-UI).

Formatos aceptables de archivo

La política de arranque seguro contiene solo una clave en PK, pero varias claves pueden residir en KEK. Lo ideal es que el fabricante o el propietario de la plataforma mantenga la clave privada correspondiente a la PK pública. Otras personas (como los proveedores de sistema operativo y de dispositivos) mantienen las claves privadas correspondientes a las claves públicas en KEK. De esta forma, los propietarios de la plataforma o terceros pueden agregar o eliminar entradas en el archivo db o dbx de un sistema específico.

En la política de arranque seguro, se utiliza db y dbx para autorizar la ejecución del archivo de imagen previo al arranque. Para que se ejecute un archivo de imagen, se debe asociar con una clave o valor hash en db, y no asociarse con una clave o valor hash en dbx. Cualquier intento de actualizar el contenido de db o dbx debe firmarse con una PK o KEK privada. Cualquier intento de actualizar el contenido de PK o KEK debe firmarse con una PK privada.

Tabla 14. Formatos aceptables de archivo

Componente de la política	Formatos aceptables de archivo	Extensiones aceptables de archivo	Cantidad máxima permitida de registros
PK	Certificado X.509 (solo formato DER binario)	1. `.cer` 2. `.der` 3. .crt	Uno
KEK	Certificado X.509 (solo formato DER binario) Almacén de claves públicas	1. `.cer` 2. `.der` 3. `.crt` 4. `.pbk`	Más de una
DB y DBX	Certificado X.509 (solo formato DER binario) Imagen de EFI (el BIOS del sistema calculará e importará la recopilación de imágenes)	1. `.cer` 2. `.der` 3. `.crt` 4. `.efi`	Más de una

Para acceder a la función Configuración de arranque seguro, haga clic en Seguridad del sistema en Configuración del BIOS del sistema. Para ir a Configuración del BIOS del sistema, presione F2 cuando aparezca el logotipo de la empresa durante la POST.

- De manera predeterminada, el arranque seguro está deshabilitado y la política de arranque seguro se establece en Estándar. Para configurar la política de arranque seguro, debe habilitar el arranque seguro.
- Cuando el modo de arranque seguro se establece en Estándar, significa que el sistema tiene certificados predeterminados y recopilaciones de imágenes o hash cargados de fábrica. Esto sirve para la seguridad del firmware estándar, los controladores, las ROM de opción y los cargadores de arranque.
- Para admitir un nuevo controlador o firmware en un servidor, el certificado respectivo debe estar inscrito en la base de datos del almacén de certificados de arranque seguro. Por lo tanto, la política de arranque seguro debe estar configurada en Personalizada.

Cuando la política de arranque seguro está configurada como Personalizada, se heredan los certificados estándar y las recopilaciones de imágenes cargados en el sistema de forma predeterminada, opción que se puede modificar. La política de arranque seguro configurada como Personalizada le permite realizar operaciones tales como Ver, Exportar, Importar, Eliminar, Eliminar todo, Restablecer y Restablecer todo. Mediante estas operaciones, puede configurar las políticas de arranque seguro.

Si configura la política de arranque seguro como Personalizada, se habilitan 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. Para seleccionar la política (PK/KEK/DB/DBX) en la que desea hacer el cambio y realizar las acciones adecuadas, haga clic en el vínculo correspondiente. En cada sección, se incluirán vínculos para realizar las operaciones de Importar, Exportar, Eliminar y Restablecer. Los vínculos se habilitan en función de lo que corresponda, lo cual depende de la configuración del momento. Borrar todo y Restablecer todo son las operaciones que tienen impacto en todas las políticas. Con Eliminar todo, se borran todos los certificados y las recopilaciones de imágenes de la política personalizada; y, con Restablecer todo, se restauran todos los certificados y recopilaciones de imágenes del almacén de certificados Estándar o Predeterminado.

Recuperación del BIOS

La función de recuperación del BIOS permite recuperar manualmente el BIOS desde una imagen almacenada. El BIOS está seleccionado cuando se enciende el sistema y si se detecta un BIOS dañado o en riesgo, se muestra un mensaje de error. A continuación, puede iniciar el proceso de recuperación del BIOS por medio de RACADM. Para realizar una recuperación manual del BIOS, consulte la iDRAC RACADM Command Line Interface Reference Guide (Guía de referencia de la interfaz de línea de comandos iDRAC RACADM) disponible en https://www.dell.com/idracmanuals.

4

Plugin Management

A plugin is individually packaged in a DUP. Plugins do not get removed on iDRAC reboot, reset, or AC cycles, they can only be removed by iDRAC sanitize operation or LC wipe operation. You can enable or disable the plugins. When enabled, plugins are only installed but not started.

To manage plugins from iDRAC GUI, go to **iDARC Settings** > **Settings** > **Plugins**.

NOTE: You must have Login privilege and Control and Configure Privilege to install, update, and remove the plugins. You can only view the installed plugins with Login privilege.

Following are the information available in Plugin inventory:

- Name — Name of the plugin. Maximum number of characters-512
- Version — Version of Installed plugin
- State — Enabled / Disabled
- Status — Starting, Not Started, Running, Stopping, Updating, Stopped: Disabled, Stopped: Installed— No Hardware, Stopped: Installed— Version Dependency, Stopped: Plugin Failure, Stopped: Internal Error — Unknown Error, Stopped: Plugin Conflict.
- Manufacture — Name of the company, maximum 512characters
- ReleaseDate — Date of creation of DUP
- SoftwareId — Component ID

Installing/Upgrading plugin

1. Download Plugin from Dell.com
2. Go to iDRAC Update page
3. Select Plugin DUP file
4. Install Plugin

   NOTE: If a plugin is valid, a success message is shown after the plugin installed. If the hardware is not present, then an LC message is logged indicating that Plugin is not started. If the plugin is invalid, an error message is displayed.

Remove Plugin

1. Go to Plugins page - **iDARC Settings** > **Settings** > **Plugins**
2. Select Uninstall/Remove
3. Plugin is then stopped and removed from iDRAC.

When a non-SDL (Non Supported Device List) card is installed, iDRAC cannot detect a SDK plugin. You need to manually find and install the SDK plugin. iDRAC firmware downgrade can result in plugins being disabled or limited functionality.

NOTE: Installing, updating, or removing a plugin takes less than 5 minutes.

5

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 se hayan establecido la configuración de red iDRAC y un navegador compatible y de que se hayan actualizado las licencias necesarias. Para obtener más información sobre la función de licencias de iDRAC, consulte Licencias de la iDRAC en la página 21.

Puede configurar iDRAC con los siguientes elementos:

- Interfaz web del iDRAC
- RACADM
- Servicios remotos (consulte la *Guía del usuario de Dell Lifecycle Controller Remote Services*)
- IPMITool (consulte la *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
   - SSH
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:

- 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 de switch
- Id. de conexión de 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
- Uso de DHCP para obtener dirección de servidor DNS
- Servidor DNS preferido actual
- Servidor DNS alternativo actual

Configuración IPv6 actual

- Activación de IPv6
- 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 la iDRAC mediante RACADM, consulte la información sobre el subcomando `getsysinfo` o `get` que se proporciona en *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

Modificación de la configuración de red

Después de configurar los valores de red de iDRAC mediante la utilidad de configuración de iDRAC, también puede modificar la configuración a través de la interfaz web de iDRAC, RACADM, Lifecycle Controller y el administrador del servidor (después de arrancar el sistema operativo). Para obtener más información sobre la configuración de privilegios y las herramientas, 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 **Configuración de iDRAC** > **Conectividad** > **Red** > **Ajustes de red**. Aparecerá la página **Red**.
2. Especifique la configuración de red, los valores comunes, IPv4, IPv6, IPMI o la configuración de VLAN según sus requisitos y haga clic en **Aplicar**.

   Si selecciona **NIC dedicado automáticamente** en **Configuración de red**, cuando la iDRAC tenga una selección de NIC como LOM compartida (1, 2, 3 o 4) y se detecte un vínculo en la NIC dedicada de la 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*.

   NOTA: Si iDRAC utiliza DHCP y usted obtuvo un alquiler para su dirección IP, dicho alquiler se liberará al grupo de direcciones del servidor DHCP cuando NIC, Ipv4 o DHCP estén desactivados.

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. Se deniegan todas las demás solicitudes de inicio de sesión.
- Cuando se producen errores repetidos al iniciar sesión desde una dirección IP específica, se impide el inicio de sesión de esa dirección en iDRAC durante un lapso predefinido. Si inicia sesión de forma incorrecta dos veces, no podrá volver a iniciar sesión de nuevo hasta pasados 30 segundos. Si inicia sesión de forma incorrecta más de dos veces, no podrá volver a iniciar sesión de nuevo hasta pasados 60 segundos.

NOTA: Esta función soporta hasta 5 rangos de IP. Puede ver o establecer esta función mediante RACADM y Redfish.

A medida que se acumulen errores al iniciar sesión de una dirección IP específica, se registran mediante un contador interno. Cuando el usuario inicie sesión correctamente, se borrará el historial de fallas y se restablecerá el contador interno.

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

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 **Configuración de iDRAC** > **ConectividadRedConfiguración de red** > **Configuración avanzada de la red**.
   Aparecerá la página **Red**.
2. Haga clic en **Configuración avanzada de la red**.
   Se muestra la página **Seguridad de la red**.
3. Especifique la configuración de filtrado de IP mediante **Dirección del rango de IP** y **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): FIPS es un conjunto de estándares utilizados por las agencias gubernamentales y contratistas de Estados Unidos. El modo FIPS cumple los requisitos de FIPS 140-2, nivel 1. Para obtener más información sobre FIPS, consulte la FIPS User Guide for iDRAC and CMC for non MX platforms (Guía del usuario de FIPS para iDRAC y CMC en plataformas no MX).
   NOTA: Si habilita el **Modo FIPS**, se restablecerá la iDRAC con los valores predeterminados.

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 a la dirección IP entrante y 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.

NOTA: La configuración del filtrado de IP admite hasta 5 rangos de IP.

El inicio de sesión continúa 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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

Selección de conjunto de cifrado

Se puede utilizar la Selección de conjunto de cifrado para limitar el cifrado en iDRAC o las comunicaciones del cliente y determinar cuán segura será la conexión. Proporciona un nivel adicional de filtrado del conjunto de cifrado TLS actualmente en uso. Estos valores se pueden configurar mediante la interfaz web de iDRAC y las interfaces de línea de comandos de RACADM y WSMAN.

Configuración de la selección de conjunto de cifrado mediante la interfaz web de iDRAC

PRECAUCIÓN: Usar el comando de cifrado de OpenSSL para analizar cadenas con sintaxis no válida puede dar lugar a errores inesperados.

NOTA: Esta es una opción avanzada de seguridad. Antes de configurar esta opción, asegúrese de que tiene un amplio conocimiento de lo siguiente:

- La sintaxis de la cadena de cifrado de OpenSSL y su uso.
- Herramientas y procedimientos para validar la configuración del conjunto de cifrado resultante para garantizar que los resultados estén alineados con las expectativas y los requisitos.

NOTA: Antes de establecer la Configuración avanzada para los conjuntos de cifrado TLS, asegúrese de que utiliza un navegador web compatible.

Para agregar cadenas personalizadas de cifrado:

1. En la interfaz web de iDRAC, vaya a **Configuración de iDRAC** > **Servicios** > **Servidor web**.
2. Haga clic en **Establecer cadena de cifrado** en la opción **Cadena de cifrado del cliente**.
   Aparece la página **Establecer cadena personalizada de cifrado**.
3. En el campo **Cadena personalizada de cifrado**, escriba una cadena válida y haga clic en **Establecer cadena de cifrado**.

   NOTA: Para obtener más información acerca de las cadenas de cifrado, consulte www.openssl.org/docs/man1.0.2/man1/ciphers.html.

4. Haga clic en **Aplicar**.
   Establecer la cadena personalizada de cifrado finaliza la sesión actual de iDRAC. Espere unos minutos antes de abrir una nueva sesión de iDRAC.

Los cifrados compatibles con iDRAC en el puerto 5000 son los siguientes:

ssl-enum-ciphers:

Cifrados TSLv1.1:

- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (secp256r1)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1)
- TLS_ECDHE_RSA_WITH_RC4_128_SHA (secp256r1)
- TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048)
- TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048)
- TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048)
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (rsa 2048)
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (rsa 2048)
- TLS_RSA_WITH_IDEA_CBC_SHA (rsa 2048)
- TLS_RSA_WITH_RC4_128_MD5 (rsa 2048)
- TLS_RSA_WITH_RC4_128_SHA (rsa 2048)
- TLS_RSA_WITH_SEED_CBC_SHA (rsa 2048)

Cifrados TLSv1.2:

- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (secp256r1)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1)
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1)
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1)
- TLS_ECDHE_RSA_WITH_RC4_128_SHA (secp256r1)
- TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048)
- TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048)
- TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048)
- TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048)
- TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048)
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (rsa 2048)
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (rsa 2048)
- TLS_RSA_WITH_IDEA_CBC_SHA (rsa 2048)
- TLS_RSA_WITH_RC4_128_MD5 (rsa 2048)
- TLS_RSA_WITH_RC4_128_SHA (rsa 2048)
- TLS_RSA_WITH_SEED_CBC_SHA (rsa 2048)

Configuración de selección del conjunto de cifrado usando RACADM

Para configurar la selección del conjunto de cifrado usando RACADM, utilice cualquiera de los siguientes comandos:

- `racadm set idraC.webServer.customCipherString ALL:!DHE-RSA-AES256-GCM-SHA384:!DHE-RSA-AES256-GCM-SHA384`
- `racadm set idraC.webServer.customCipherString ALL:-DHE-RSA-CAMELLIA256-SHA`
- `racadm set idraC.webServer.customCipherString ALL:!DHE-RSA-AES256-GCM-SHA384:!DHE-RSA-AES256-SHA256:+AES256-GCM-SHA384:-DHE-RSA-CAMELLIA256-SHA`

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.

Modo FIPS (INTERFAZ)

El FIPS es un estándar de seguridad para computadoras que los contratistas y las agencias gubernamentales de Estados Unidos deben utilizar. A partir de la versión de iDRAC 2.40.40.40, iDRAC permite activar el modo FIPS.

La iDRAC estará oficialmente certificada 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 realización del Programa de validación del módulo criptográfico se denomina software validado por FIPS. Debido al tiempo que demora la realización de la validación de FIPS, no todas las versiones de iDRAC son validadas. Para obtener información sobre el estado más reciente de la validación de FIPS, 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 los valores predeterminados de fábrica. Si desea restaurar la configuración, cree una copia de seguridad del perfil de configuración de 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 FIPS) restablece iDRAC a la configuración predeterminada.

3. Aparece un mensaje que le solicitará que confirme el cambio. Haga clic en **OK** (Aceptar).
   Se reiniciará iDRAC en el modo FIPS. Espere al menos 60 segundos antes de volver a conectarse a 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	Habilite el acceso a la interfaz web de iDRAC. Si deshabilita la interfaz web, el RACADM remoto también se deshabilitará. Utilice el RACADM local para volver a habilitar el servidor web y el RACADM remoto.
Configuración del SEKM	Permite habilitar la funcionalidad de administración de claves empresariales seguras en iDRAC mediante una arquitectura de servidor de cliente.
SSH	Acceda a iDRAC mediante el firmware RACADM.
RACADM remoto	Acceda a iDRAC de forma remota.
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.
Redfish	Activa la compatibilidad de la API RESTful de Redfish.
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 **Configuración de iDRAC** > **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 **Evitar que esta página cree diálogos adicionales**. Si selecciona esta opción, no podrá configurar los servicios.

   Puede configurar **SEKM** en la página Configuración de iDRAC. Haga clic en **Configuración de iDRAC** > **Servicios** > **Configuración de la SEKM**.

   NOTA: Si desea obtener información detallada sobre el procedimiento detallado para configurar SEKM, consulte la *Ayuda en línea de iDRAC*.

   NOTA: Cuando el modo **Seguridad (Cifrado)** se cambia de **Ninguno** a **SEKM**, el trabajo en tiempo real no está disponible. Sin embargo, este se agregará a la lista de trabajos por etapas. Por otro lado, el trabajo en tiempo real se realiza correctamente cuando el modo se cambia de **SEKM** a **Ninguno**.

   Compruebe lo siguiente cuando se cambie el valor del campo **Nombre de usuario** en la sección Certificado de cliente en el servidor KeySecure (por ejemplo: si se cambia el valor de **Nombre común (NC)** a **ID de usuario (UID)**)

   a. Cuando se utilice una cuenta existente, haga lo siguiente:
      - Compruebe en el certificado de SSL de iDRAC que, en lugar del campo **Nombre común**, el campo **Nombre de usuario** coincida con el nombre de usuario actual en KMS. Si no coinciden, tendrá que establecer el campo del nombre de usuario y volver a generar el certificado SSL. Luego, debe firmarlo en KMS y volver a cargarlo a iDRAC.

   b. Cuando se utilice una cuenta de usuario nueva, haga lo siguiente:
      - Asegúrese de que la cadena del **Nombre de usuario** coincida con el campo del nombre de usuario en el certificado SSL del iDRAC.
      - Si no coinciden, tendrá que volver a configurar los atributos de KMS de iDRAC Nombre de usuario y Contraseña.
      - Una vez que se verifica que el certificado contiene el nombre de usuario, el único cambio que se debe aplicar es cambiar la propiedad de la clave del usuario anterior al usuario nuevo para hacer coincidir el nuevo nombre de usuario de KMS.

   Mientras utiliza Vormetric Data Security Manager como KMS, asegúrese de que el campo Nombre común (CN) en el certificado SSL de iDRAC coincida con el nombre de host agregado a Vormetric Data Security Manager. De lo contrario, es posible que el certificado no se importe correctamente.

   NOTA:
   - La opción **Restablecer clave** se desactivará cuando los informes `racadm sekm getstatus` se muestren como **Fallidos**.

- La SEKM solo es compatible con los campos **Nombre común**, **ID de usuario** o **Unidad de organización** para el campo **Nombre de usuario** en Certificado de cliente.
- Si utiliza un CA de terceros para firmar el CSR de iDRAC, asegúrese de que este CA de terceros admite el valor **UID** para el campo **Nombre de usuario** en Certificado de cliente. Si este no se admite, utilice **Nombre común** como el valor para el campo **Nombre de usuario**.
- Si está utilizando campos de nombre de usuario y contraseña, asegúrese de que el servidor KMS admita esos atributos.

NOTA: En el caso del servidor de administración de claves de KeySecure,

- cuando crea una solicitud de certificado SSL, debe incluir la dirección IP del servidor de administración de claves en el campo **Nombre alternativo de sujeto**
- La dirección IP debe estar en el siguiente formato: IP:xxx.xxx.xxx.xxx.

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.Racadm
- iDRAC.SNMP

Para obtener más información acerca de estos objetos, consulte *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

Funciones de SEKM

A continuación, se indican las funciones de SEKM disponibles en iDRAC:

1. **Política de depuración de claves de SEKM**: iDRAC proporciona un valor de política que permite configurar iDRAC para depurar las claves antiguas no utilizadas en el servidor de administración de claves (KMS) durante la operación de regeneración de claves. Puede configurar atributo de lectura/escritura de iDRAC KMSKeyPurgePolicy en uno de los siguientes valores:
   - Conservar todas las claves: esta es la configuración predeterminada y el comportamiento existente, en el cual iDRAC deja todas las claves de KMS intactas durante la operación de regeneración de claves.
   - Conservar las claves N y N-1: iDRAC elimina todas las claves de KMS, excepto la actual (N) y la clave anterior (N-1) durante la operación de regeneración de claves.
2. **Depuración de claves de KMS tras la deshabilitación de SEKM**: como parte de la solución Secure Enterprise Key Manager (SEKM), iDRAC permite deshabilitar SEKM en iDRAC. Una vez que SEKM esté deshabilitado, las claves generadas por iDRAC en KMS no se utilizan y permanecen en KMS. Esta función permite que iDRAC elimine esas claves cuando SEKM está deshabilitado. iDRAC proporciona una nueva opción "-purgeKMSKeys" para el comando heredado existente "racadm sekm disable", que permite depurar claves en KMS cuando SEKM está deshabilitado en iDRAC.

   NOTA: Si SEKM ya está deshabilitado y desea depurar las claves antiguas, debe volver a habilitar SEKM y, a continuación, deshabilitar la opción de paso -purgeKMSKeys.
3. **Política de creación de claves**: como parte de esta versión, iDRAC se ha configurado previamente con una política de creación de claves. El atributo KeyCreationPolicy es de solo lectura y se establece como el valor "Key per iDRAC".
   - El atributo iDRAC de solo lectura iDRAC iDRAC.SEKM.KeyIdentifierN informa el identificador de clave que creó KMS.

     ```
     racadm get iDRAC.SEKM.KeyIdentifierN
     ```
   - El atributo iDRAC de solo lectura iDRAC.SEKM.KeyIdentifierNMinusOne informa el identificador de clave anterior tras la operación de regeneración de claves.

     ```
     racadm get iDRAC.SEKM.KeyIdentifierNMinusOne
     ```

4. **Regeneración de claves SEKM**: iDRAC proporciona dos opciones para regenerar la clave de la solución SEKM, ya sea iDRAC o PERC. Se recomienda regenerar la clave de iDRAC, ya que así regenera todos los dispositivos con capacidad de SEKM seguro/habilitados.
   - *Regeneración de claves SEKM iDRAC [Regenerar claves en iDRAC.Embedded.1 FQDD]*: cuando se ejecuta `racadm sekm rekey iDRAC.Embedded.1`, todos los dispositivos SEKM con capacidad segura/habilitados vuelven a generar una nueva clave de KMS y esta es una clave común para todos los dispositivos habilitados para SEKM. La operación de regeneración de claves de iDRAC también se puede ejecutar desde la GUI de iDRAC: **Configuración de iDRAC** > **Servicios** > **Configuración de SEKM** > **Regenerar clave**. Después de ejecutar esta operación, el cambio en la clave se puede validar mediante la lectura de los atributos KeyIdentifierN y KeyIdentifierNMinusOne.
   - *La regeneración de claves de SEKM PERC (regeneración de claves en la controladora [Ejemplo RAID.Slot.1-1] FQDD)*: cuando se realiza `racadm sekm rekey <controller FQDD>`, la controladora habilitada con SEKM correspondiente vuelve a generar la clave común iDRAC actualmente activa que se creó a partir de KMS. La operación de regeneración de claves de la controladora de almacenamiento también se puede ejecutar desde la GUI de iDRAC: **Almacenamiento** > **Controladores** > **<controladora FQDD>** > **Acciones** > **Editar** > **Seguridad** > **Seguridad (cifrado)** > **Regeneración de claves**.

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 Configure iDRAC (Configurar iDRAC) para activar o desactivar la redirección de HTTPS.

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

Para desactivar la redirección de HTTP a HTTPS:

```
racadm set iDRAC.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
```

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 en la estación de administración. La consola envía un correo electrónico o un mensaje SMS a un dispositivo móvil con la información requerida e inicia la aplicación del visor VNC en la estación de administración. Este visor 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 correcciones necesarias. Antes de iniciar el cliente VNC, debe activar el servidor VNC y configurar sus ajustes en iDRAC, como la contraseña, el número de puerto VNC, el cifrado de SSL y el valor del tiempo de espera. Puede configurar estos ajustes mediante la interfaz web de iDRAC o RACADM.

NOTA: La función VNC se concede bajo licencia y está disponible con la licencia iDRAC Enterprise o Datacenter.

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

Se pueden activar dos sesiones de cliente VNC al mismo tiempo. La segunda está en 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:

- Si cuando se inicia una sesión VNC se produce un error de protocolo RFB, cambie la configuración del cliente VNC a Alta calidad y, a continuación, vuelva a iniciar la sesión.
- 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 por algunos segundos. Durante este tiempo, si no se lleva a cabo una acción en el cliente VNC activo, es posible que se cierre la sesión VNC. Debe esperar a que se agote el tiempo de espera (el valor establecido en la configuración del servidor VNC en la página **Servicios** de la interfaz web de iDRAC) y, a continuación, volver a establecer la conexión VNC.
- Si la ventana del cliente VNC se minimiza por más de 60 segundos, se cierra la ventana del cliente. Debe abrir una nueva sesión VNC. Si maximiza la ventana del cliente VNC antes de que transcurran los 60 segundos, puede 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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.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 aceptar la conexión en `<localhost>:<localport number>`. Por ejemplo, 127.0.0.1:5930.
2. Configure el túnel SSL para conectar 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 **Configuration (Configuración)** > **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 consola virtual (opcional). Una vez activada, la sección Live Front Panel Feed (Fuente en directo del panel frontal) y el panel LCD del servidor mostrarán el mensaje `Virtual console session active` (Sesión de consola virtual activa) cuando haya una sesión de la 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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.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)**.
   Aparece 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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.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 (Configuración de zona horaria y 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 la zona horaria y NTP, utilice el comando `set` con los objetos en `iDRAC.Time` y el grupo `iDRAC.NTPConfigGroup`.

Para obtener más información, consulte *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

NOTA: iDRAC sincroniza la hora con el host (hora local). Por lo tanto, se recomienda configurar tanto iDRAC como el host con la misma zona horaria, de modo que la sincronización de la hora esté correcta. Si desea cambiar la zona horaria, debe cambiarla tanto en el host como en el iDRAC y, luego, debe reiniciar el host.

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 iniciará 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 acerca de estos objetos, consulte *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

Configuración del primer dispositivo de inicio mediante la consola virtual

Puede seleccionar el dispositivo desde el cual iniciar, dado 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. La opción Boot Once (Iniciar una vez) es compatible con todos los dispositivos que se enumeran en Configuración del primer dispositivo de inicio en la página 109.

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 más información acerca de Server Administrator, consulte *Guía de instalación de OpenManage* disponible en https://www.dell.com/openmanagemanuals.

El sistema host debe tener el sistema operativo Windows para usar esta función.

NOTA:

- Esta función no se puede aplicar al sistema Linux.
- Esta función es independiente de cualquier agente o atributo.

Activación o desactivación del paso del sistema operativo a iDRAC

En los servidores que tienen dispositivos de tarjeta de red dependiente (NDC) o LAN incorporada en la placa base (LOM), 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 de host a través de una LOM compartida, una NIC dedicada o la NIC de USB. Esta función está disponible con la licencia de iDRAC Enterprise o Datacenter.

NOTA: El módulo de servicio de iDRAC (iSM) proporciona más funciones para la administración de iDRAC a través del sistema operativo. Para obtener más información, consulte iDRAC Service Module User's Guide (Guía del usuario del módulo de servicio de iDRAC) en www.dell.com/idracservicemodule.

Cuando esta opción se activa a través de una NIC dedicada, es posible iniciar el navegador en el sistema operativo de host y luego 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 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 de 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 de 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: Si inicia un módulo de servicio de iDRAC mientras la NIC de USB está en estado desactivado, el módulo de servicio de la iDRAC cambia la dirección IP de la NIC de USB a 169.254.0.1.

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

NOTA: Es posible que no se pueda acceder a iDRAC desde el servidor host mediante el paso de LOM cuando está activada la formación de equipos NIC. A continuación, se puede acceder a iDRAC desde el sistema operativo del servidor host con la NIC de USB de iDRAC o a través de la red externa mediante la NIC dedicada de iDRAC.

Tarjetas admitidas para el paso del sistema operativo al iDRAC

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

Tabla 15. Paso del sistema operativo a iDRAC mediante LOM: tarjetas admitidas

Categoría	Fabricante	Tipo
NDC	Broadcom	• 5720 QP rNDC 1G BASE-T

Tabla 15. Paso del sistema operativo a iDRAC mediante LOM: tarjetas admitidas (continuación)

Categoría	Fabricante	Tipo
	Intel	• x520/i350 QP rNDC 1G BASE-T

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

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 (básico 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.

NOTA: Para configurar la NIC de USB como DHCP en un sistema operativo Linux o XenServer, consulte la documentación del sistema operativo o del hipervisor.

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 **Configuración de iDRAC** > **Conectividad** > **Red** > **Paso del sistema operativo a iDRAC**.
   Se mostrará la página **Paso del sistema operativo a iDRAC**.
2. Cambie el estado a **Activado**.
3. Seleccione una de las siguientes opciones para el modo de paso:
   - **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.

   NOTA: Si establece el modo de paso en LOM, asegúrese de lo siguiente:
   - iDRAC y el sistema operativo se encuentran en la misma subred
   - La selección de NIC en la configuración de la red está establecida en una LOM
4. Si el servidor está conectado en el modo LOM compartido, el campo **Dirección IP del sistema operativo** estará desactivado.

   NOTA: Si la red VLAN está habilitada en iDRAC, LOM-Passthrough funcionará solamente en el modo LOM compartido con etiquetas de VLAN configuradas en el host.

   NOTA:
   - Cuando el modo de paso está establecido en LOM, no es posible iniciar iDRAC desde el SO del host después de un arranque en frío.
   - Se eliminó intencionalmente la función de paso de LOM mediante la función Modo dedicado.
5. Si selecciona **NIC de USB** como configuración de paso, introduzca la dirección IP de la NIC del USB.

   El valor predeterminado es 169.254.1.1. 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 de host o la red local, deberá cambiarla.

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

   NOTA: Si prefiere IPv6, la dirección predeterminada es fde1:53ba:e9a0:de11::1. Si es necesario, esta dirección se puede modificar en la configuración idrac.OS-BMC.UsbNicULA. Si no desea IPv6 en el NIC de USB, se puede desactivar cambiando la dirección a "::"
6. Haga clic en **Aplicar**.
7. 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 *Registro de atributos de iDRAC* disponible en https://www.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.

   NOTA: Si establece el modo de paso en LOM, asegúrese de lo siguiente:
   - iDRAC y el sistema operativo se encuentran en la misma subred
   - La selección de NIC en la configuración de la red está establecida en una LOM

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

   NOTA: Solo se puede seleccionar la opción LOM si la tarjeta admite la función Paso del sistema operativo a iDRAC. De lo contrario, esta opción aparecerá desactivada, en color 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 169.254.1.1. Sin embargo, si esta dirección IP entra en conflicto con una dirección IP de otras interfaces del sistema de host o la red local, deberá cambiarla. No introduzca las IP 169.254.0.3 y 169.254.0.4. Estas direcciones IP están reservadas para el puerto NIC de USB en el panel frontal cuando se utiliza un cable A/A.

   NOTA: Si prefiere IPv6, la dirección predeterminada es fde1:53ba:e9a0:de11::1. Si es necesario, esta dirección se puede modificar en la configuración idrac.OS-BMC.UsbNicULA. Si no desea IPv6 en el NIC de USB, se puede desactivar cambiando la dirección 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 16. 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 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.

Tabla 16. Tipos de certificado basados en el tipo de inicio de sesión (continuación)

Tipo de inicio de sesión	Tipo de certificado	Cómo obtenerlo
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 de SSL de servidor 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. Una opción de cifrado SSL se proporciona para desactivar los cifrados débiles. Creado a partir de la tecnología de cifrado asimétrico, SSL se acepta ampliamente para el suministro de comunicaciones autenticadas y cifradas entre clientes y servidores para impedir la escucha a escondidas 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 superior y en 168 bits o superior, es posible que la configuración de la criptografía para el entorno de máquinas virtuales (JVM o IcedTea) requiera la instalación de Unlimited Strength Java Cryptography Extension Policy Files para permitir el uso de los complementos de iDRAC como la consola virtual 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 la 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 admitidos podrán acceder a iDRAC sin advertencias de certificados.

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 cargar el certificado de firma personalizado (sin la clave privada). Además, se puede eliminar un certificado de firma personalizado existente. Después de eliminar el certificado de firma personalizado, iDRAC se restablece y genera automáticamente un nuevo certificado SSL autofirmado. Si se vuelve a generar un certificado autofirmado, se debe volver a establecer la confianza entre iDRAC y la estación de trabajo de administración. Los certificados SSL generados automáticamente son autofirmados y tienen una fecha de vencimiento de siete años y un día y una fecha de inicio de un día en el pasado (para diferentes configuraciones de zonas horarias en las estaciones de administración e iDRAC).

El certificado SSL de servidor web de iDRAC admite el carácter asterisco (*) como parte del componente ubicado más a la izquierda del nombre común al generar una solicitud de firma de certificado (CSR). Por ejemplo: *.qa.com o *.empresa.qa.com. Esto se denomina certificado comodín. Si se genera una CSR comodín fuera de iDRAC, puede tener un solo certificado SSL comodín firmado que se puede cargar para varias iDRAC y todas las iDRAC son de confianza para todos los navegadores admitidos. 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. Si inicia 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 a una autoridad de certificados (CA) para un certificado del servidor SSL. Los certificados de 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 los estándares de la CA, esta 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 la iDRAC. La información que se utiliza para generar la CSR, almacenada en el firmware de la 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 la iDRAC.

Generación de CSR mediante la interfaz web

Para generar una CSR nueva:

NOTA: Cada CSR nueva sobrescribe cualquier dato de CSR anterior almacenado 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 **Configuración de iDRAC Settings** > **Servicios** > **Servidor web** > **Certificado de SSL**, seleccione **Generar una solicitud de firma de certificado (CSR)** y, luego, haga clic en **Siguiente**.
   Aparece la página **Generar una nueva solicitud de firma de certificado (CSR)**.
2. Introduzca un valor para cada atributo de la CSR.
   Para obtener más información, consulte la *Ayuda en línea de iDRAC*.
3. Haga clic en **Generar**.
   Se genera una nueva CSR. Guárdela en la estación de administración.

Generación de CSR mediante RACADM

Para generar una CSR mediante RACADM, utilice 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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

Inscripción automática de certificados

En iDRAC, la función de inscripción automática de certificados le permite realizar la instalación y la renovación automáticas de certificados utilizados por el servidor web. Cuando se habilita esta función, el certificado del servidor web existente se reemplaza por un nuevo certificado.

NOTA:

- La inscripción automática de certificados es una función con licencia y requiere una licencia Datacenter.
- Se requiere la configuración de un NDES (Servicio de inscripción de dispositivos de red) válido para emitir el certificado del servidor.

Los siguientes corresponden a los parámetros de configuración de inscripción automática de certificados:

- Habilitar/deshabilitar
- URL del servidor de SCEP
- Contraseña de comprobación

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

A continuación, se indica el estado disponible para la inscripción automática de certificados:

- Inscrito: la inscripción automática de certificados está activada. El certificado se monitorea y se puede emitir un nuevo certificado tras su vencimiento.
- Inscribiendo: estado intermedio después de activar la inscripción automática de certificados.
- Error: se produjo un problema con el servidor del NDES.
- Ninguno: valor predeterminado.

NOTA: Cuando activa la inscripción automática de certificados, se reinicia el servidor web y se cierran todas las sesiones web existentes.

Carga del certificado del servidor

Después de generar una CSR, puede cargar el certificado de SSL de servidor firmado en el firmware de iDRAC. Se debe restablecer iDRAC para aplicar el certificado. La iDRAC acepta solamente certificados de servidor web X509 codificados con 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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.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 remoto racadm `sslkeyupload`.
3. Cargue el certificado firmado al iDRAC mediante el comando remoto racadm `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 **Configuración de iDRAC** > **Servicios** > **Servidor web** > **Certificado de 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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.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 de SSL personalizado)**, haga clic en **Upload Signing Certificate (Cargar certificado de firma)**.
   Aparecerá la página **Cargar certificado de firma del certificado SSL personalizado**.
3. Haga clic en **Choose File (Elegir archivo)** y seleccione el archivo de certificado de firma del certificado de 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. La 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 *Guía de la CLI de RACADM para iDRAC* disponible en https://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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.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 usando RACADM, utilice el subcomando `sslcertdelete`. A continuación, ejecute el comando `racreset` para restablecer la iDRAC.

Para obtener más información, consulte *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

Configuración de varios iDRAC mediante RACADM

Por medio de RACADM, es posible configurar una o varias iDRAC con propiedades idénticas. Cuando se realiza una consulta en una iDRAC específica con su ID de grupo e ID de objeto, RACADM crea un archivo de configuración de la información recuperada. Importe el archivo a otras iDRAC para configurarlas de manera idéntica.

NOTA:

- El archivo de configuración contiene información que se aplica al servidor 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 (SCP) para configurar varias iDRAC mediante RACADM. El SCP contiene la información de configuración de los componentes. Puede utilizar este archivo para aplicar la configuración para BIOS, iDRAC, RAID y NIC mediante la importación del archivo en un sistema de destino. Para obtener más información, consulte el informe técnico *Flujo de trabajo de la configuración de XML* disponible en https://www.dell.com/manuals.

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 la 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 que edite este archivo con un editor simple de textos. 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
   ```

   Esto carga la información en la otra iDRAC. Puede utilizar el comando `set` para sincronizar la base de datos de usuario y contraseña con el Server Administrator.
4. Restablezca el iDRAC de destino mediante 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 los valores de configuración de iDRAC a través de la RACADM local o la utilidad de configuración de iDRAC. 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 usar IPMI en la LAN.

6

Autorización delegada mediante OAuth 2.0

La función de autorización delegada permite que un usuario o una consola acceda a API de iDRAC mediante JSON Web Tokens (JWT) de OAuth 2.0 que el usuario o la consola obtienen en primer lugar desde un servidor de autorización. Una vez que se recupera un JWT de OAuth, el usuario o la consola pueden usarlo para invocar a API de iDRAC. Esto evita la necesidad de especificar el nombre de usuario y la contraseña para acceder a la API.

NOTA: Esta función solo está disponible para la licencia DataCenter. Debe tener el privilegio de Configurar iDRAC o Configurar usuarios para usar esta función.

iDRAC es compatible con la configuración de hasta dos servidores de autorización. La configuración requiere que un usuario especifique los siguientes detalles del servidor de autorización:

- **Nombre**: la cadena para identificar el servidor de autorización en el iDRAC.
- **URL de metadatos**: la URL compatible con OpenID Connect, según lo publicitado en el servidor.
- **Certificado HTTPS**: la clave pública del servidor que iDRAC debe utilizar para comunicarse con el servidor.
- **Clave offline**: JWK estableció el documento para el servidor de autorización.
- **Emisor offline**: la cadena del emisor como se utiliza en los tokens emitidos por el servidor de autorización.

Para la configuración en línea:

- Cuando configura un servidor de autorización, el administrador de iDRAC debe asegurarse de que iDRAC tenga acceso de red en línea al servidor de autorización.
- Si iDRAC no puede acceder al servidor de autorización, la configuración fallará, al igual que el intento subsiguiente para acceder a API de iDRAC, aunque se presente un token válido.

Para la configuración offline:

- No es necesario que iDRAC se comunique con el servidor de autenticación, sino que se configura con los detalles de los metadatos que se descargan offline. Cuando se configura offline, iDRAC tiene parte pública de las claves de firma y puede validar el token sin una conexión de red al servidor de autenticación.

7

Visualización de la información de iDRAC y el sistema administrado

Puede ver el estado y las propiedades de la iDRAC y del sistema administrado, el inventario de hardware y firmware, el estado 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 puede ver FlexAddress o la dirección asignada de forma remota (solo se aplica para las plataformas MX).

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 **Resumen del sistema**, diríjase a **Sistema** > **Descripción general** > **Resumen**. Aparece la página **Resumen del sistema**. Para obtener más información, consulte la *Ayuda en línea de iDRAC*.

También puede ver la información básica resumida del sistema mediante la utilidad de configuración de la iDRAC. Para ello, en la utilidad de configuración de iDRAC, vaya a **Resumen del sistema**. Se muestra la página **Resumen del sistema de la configuración de iDRAC**. Para obtener más información, consulte la *Ayuda en línea de la utilidad de configuración de la iDRAC*.

Configuración del seguimiento de activos

La función de seguimiento de activos en la iDRAC le permite configurar diversos atributos que se relacionan con el servidor. Esto incluye información como la adquisición, la garantía, el servicio, etcétera.

NOTA: El seguimiento de activos en la iDRAC es similar a la función de etiqueta de activos en OpenManage Server Administrator. Sin embargo, la información de los atributos debe ingresarse por separado en ambas herramientas para registrar los datos de activos relevantes.

Realice los siguientes pasos para configurar el seguimiento de activos:

1. En la interfaz web de iDRAC, vaya a **Configuración** > **Seguimiento de activos**.

2. Haga clic en **Agregar activos personalizados** para agregar atributos adicionales que no se especificaron de forma predeterminada en esta página.
3. Ingrese toda la información pertinente de los activos del servidor y haga clic en **Aplicar**.
4. Para ver el informe del seguimiento de activos, vaya a **Sistema** > **Detalles** > **Seguimiento de activos**.

Viewing system inventory

You can view information about the hardware and firmware components installed on the managed system. To do this, in iDRAC web interface, go to **System** > **Inventory**. For information about the displayed properties, see the *iDRAC Online Help*.

The Hardware Inventory section displays the information for the following components available on the managed system:

- iDRAC
- RAID controller
- Batteries
- CPUs
- DIMMs
- HDDs
- Backplanes
- Network Interface Cards (integrated and embedded)
- Video card
- SD card
- Power Supply Units (PSUs)
- Fans
- Fibre Channel HBAs
- USB
- NVMe PCIe SSD devices

The Firmware Inventory section displays the firmware version for the following components:

- BIOS
- Lifecycle Controller
- iDRAC
- OS driver pack
- 32-bit diagnostics
- System CPLD
- PERC controllers
- Batteries
- Physical disks
- Power supply
- NIC
- Fibre Channel
- Backplane
- Enclosure
- PCIe SSDs

NOTE:

- Software inventory displays only the last 4 bytes of the firmware version and the Release date information. For example, if the firmware version is FLVDL06, the firmware inventory displays DL06.
- When collecting software inventory using Redfish interface, the Release date information is displayed only for components which support rollback.

NOTE:

- If any device (Example: TPM) is in OFF state, then software inventory displays the version as **Not Available** or **0**. And if the application is not installed, then it shows the version as **Not Installed**.
- The default initial system date and time is shown as Installed date/ time in software inventory until a new device firmware version is installed using the DUP. Also, BIOS and iDRAC date/ time should be synchronized for components whose inventory details are obtained from BIOS (Example: BIOS, TPM).
- Installation date do not change if the updated version is same as the installed version.

NOTE: On the Dell PowerEdge FX2/FX2s servers, the naming convention of the CMC version displayed in the iDRAC GUI differs from that on the CMC GUI. However, the version remains the same.

When you replace any hardware component or update the firmware versions, make sure to enable and run the **Collect System Inventory on Reboot** (CSIOR) option to collect the system inventory on reboot. After a few minutes, log in to iDRAC, and navigate to the **System Inventory** page to view the details. It may take up to 5 minutes for the information to be available depending on the hardware installed on the server.

NOTE: CSIOR option is enabled by default.

NOTE: Configuration changes and firmware updates that are made within the operating system may not reflect properly in the inventory until you perform a server restart.

Click **Export** to export the hardware inventory in an XML format and save it to a location of your choice.

Visualización de la información del sensor

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

- **Baterías**: proporciona información acerca de las baterías del CMOS en la placa del sistema y del RAID de almacenamiento en la placa base (ROMB).
  NOTA: La configuración de las baterías de ROMB de almacenamiento solo se encuentra disponible si el sistema tiene ROMB con una batería.
- **Ventilador** (disponible solo para los servidores tipo bastidor y torre): proporciona información acerca de los ventiladores del sistema; la redundancia de ventiladores y la lista de ventiladores que muestra la velocidad de los ventiladores y los valores del umbral.
- **CPU:** indica la condición y el estado de las CPU en el sistema administrado. También informa la limitación automática del procesador y de 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 es offline. 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 es 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.

  NOTA: Cuando se actualiza el firmware de iDRAC desde versiones anteriores a 3.30.30.30, debe restablecer iDRAC a los valores predeterminados para que la configuración de IDSDM aparezca en el filtro de eventos de la plataforma del administrador del servidor.
- **Temperatura:** proporciona información acerca de la temperatura interna de la tarjeta madre del sistema y de la temperatura de expulsión (solo se aplica a servidores en bastidor). La sonda de temperatura indica si el estado de la sonda se encuentra dentro de los valores de umbral críticos y de advertencia.
- **Voltaje**: indica el estado y la lectura de los sensores de voltaje de los distintos componentes del sistema.

En la tabla siguiente se proporciona información sobre cómo ver la información de los sensores mediante la interfaz web de la iDRAC y RACADM. Para obtener información acerca de las propiedades que se muestran en la interfaz web, consulte la *Ayuda en línea de la iDRAC*.

NOTA: En la página Descripción general de hardware se muestran solo los datos de los sensores presentes en su sistema.

Tabla 17. Información del sensor mediante la interfaz web y RACADM

Ver la información del sensor para	Mediante la interfaz web	Mediante RACADM
Baterías	**Tablero** > **Condición del sistema** > **Baterías**	Utilice el comando `getsensorinfo`. Para suministros de energía, también puede usar el comando `System.Power.Supply` con el subcomando `get`. Para obtener más información, consulte *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.
Ventilador	**Tablero** > > **Condición del sistema** > **Ventiladores**	
CPU	**Tablero** > **Condición del sistema** > **CPU**	
Memoria	**Tablero** > **Condición del sistema** > **Memoria**	
Intrusión	**Tablero** > **Condición del sistema** > **Intrusión**	
Sistemas de alimentación	> **Hardware** > **Fuentes de alimentación**	
Medios flash extraíbles	**Tablero** > **Condición del sistema** > **Medios flash extraíbles**	
Temperatura	**Tablero** > **Condición del sistema** > **Energía/térmica** > **Temperaturas**	
Voltaje	**Tablero** > **Condición del sistema** > **Energía/térmica** > **Voltajes**	

Monitoreo del índice de rendimiento de CPU, memoria y módulos de entrada/salida

En servidores Dell PowerEdge de 14.ª generación, Intel ME admite la funcionalidad de Uso de procesamiento por segundo (CUPS). La funcionalidad de CUPS proporciona monitoreo en tiempo real de la CPU, la memoria, la utilización de I/O y el índice de utilización a nivel del sistema para el sistema. Intel ME permite el monitoreo de rendimiento fuera de banda (OOB) y no consume recursos de CPU. Intel ME tiene un sensor de CUPS del sistema que indica valores de uso de recursos de procesamiento, memoria e I/O como un índice CUPS. El iDRAC monitorea este índice CUPS para el uso completo del sistema y también monitorea el índice instantáneo de utilización de CPU, memoria e I/O.

NOTA: La funcionalidad de CUPS no se admite en los siguientes servidores:

- PowerEdge R240
- PowerEdge R240xd
- PowerEdge R340
- PowerEdge R6415
- PowerEdge R7415
- PowerEdge R7425

- PowerEdge T140

La CPU y el chipset tienen contadores de monitoreo de recursos (RMC) dedicados. Los datos de estos RMC se consultan para obtener información sobre la utilización de los recursos del sistema. El administrador de nodos agrega los datos de RMC para medir la utilización acumulativa de cada uno de estos recursos del sistema que se leen desde iDRAC mediante mecanismos de intercomunicación existentes, a fin de proporcionar datos a través de las interfaces de administración fuera de banda.

La representación del sensor Intel respecto 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, incluso si el sistema está virtualizado y tiene varios hosts virtuales.

Para mostrar los parámetros de rendimiento, los sensores admitidos deben estar presentes en el servidor.

Los cuatro parámetros de utilización del sistema son:

- **Utilización de CPU:** se agregan los datos de RMC para cada núcleo de CPU a fin de indicar la utilización acumulativa de todos los núcleos del sistema. Esta utilización se basa en el tiempo transcurrido en los estados activo e inactivo. Se toma una muestra de RMC cada seis segundos.
- **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 agregan para medir el tráfico de memoria acumulativo en todos los canales de memoria del sistema. Esto mide el consumo de ancho de banda de la memoria y no la cantidad de utilización de la memoria. iDRAC lo agrega por un minuto, por lo que puede o no coincidir con la utilización de la memoria que se muestra en herramientas de otros sistemas operativos, como **top** en Linux. La utilización del ancho de banda de la memoria que se muestra en iDRAC es una indicación de si la carga de trabajo es intensiva o no.
- **Utilización de I/O:** hay un RMC por puerto raíz en el complejo raíz de PCI Express para medir el tráfico de PCI Express que se genera desde ese puerto raíz y el segmento inferior, o que se dirige a ellos. Los datos de estos RMC se agregan para medir el tráfico de PCI Express para todos los segmentos de PCI Express que se generan desde el paquete. Esta es la de medida de la utilización del ancho de banda de E/S para el sistema.
- **Índice CUPS de nivel del sistema:** el índice CUPS se calcula agregando el índice de CPU, de memoria y de I/O considerando el 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 del espacio libre de procesamiento disponible en el servidor. Si el sistema tiene un índice CUPS grande, hay espacio libre limitado para colocar más carga de trabajo en ese sistema. A medida que disminuye el consumo de recursos, disminuye el índice CUPS del sistema. Un índice de CUPS bajo indica que hay una gran cantidad de espacio libre de procesamiento, que el servidor puede recibir nuevas cargas de trabajo y que el servidor se encuentra en un estado de menor consumo de alimentación para reducir el consumo de energía. El monitoreo de la carga de trabajo se puede aplicar en todo el centro de datos con el fin de proporcionar una vista de alto nivel y holística de la carga de trabajo del centro de datos, lo que proporciona una solución dinámica para centros de datos.

NOTA: Los índices de utilización de CPU, memoria y e I/O se agregan después de un minuto. Por lo tanto, si hay incrementos instantáneos en estos índices, se pueden eliminar. Son la indicación de patrones de carga de trabajo, no de la utilización de recursos.

Las capturas IPMI, SEL y SNMP se generan si se alcanzan los umbrales de los índices de utilización y se activan los eventos del sensor. Las marcas de eventos del sensor están deshabilitadas de manera predeterminada. Se puede habilitar 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 módulos de E/S, memoria y CPU mediante la interfaz web

Para supervisar el índice de rendimiento de los módulos de E/S, memoria y CPU, 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**:
  - En esta sección, se proporcionan las estadísticas de la utilización de E/S, memoria y CPU, y el índice de CUPS a nivel del sistema. Si el sistema de host está apagado, el gráfico muestra la línea de apagado por debajo del 0 %.
  - Es posible restablecer el pico de utilización para un determinado sensor. Haga clic en **Reset Historical Peak (Restablecer pico histórico)**. Debe tener el privilegio Configure (Configurar) para poder restablecer el valor de pico.
- Sección **Métricas de rendimiento**:

- Muestra el estado y la lectura presente.
- Muestra o especifica el límite de utilización del umbral de advertencia. Debe tener el privilegio Server Configure (Configurar servidor) para poder establecer los valores de los umbrales.

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 entrada y salida 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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

Detección de servidores idle

iDRAC proporciona un índice de monitoreo del rendimiento fuera de banda de los componentes del servidor, como la CPU, la memoria y E/S.

Los datos del historial del índice de CUPS de nivel de servidor se emplean para monitorear si el servidor se está utilizando o ejecutando de forma inactiva durante un período prolongado. Si el servidor está infrautilizado con un valor inferior a un umbral determinado por un lapso definido de intervalos (en horas), se registrará como un servidor idle.

Esta función solo es compatible con las plataformas Intel con capacidad de CUPS. Las plataformas Intel y AMD sin la capacidad de CUPS no son compatibles con esta función.

NOTA:

- Para esta función, se requiere la licencia de Datacenter.
- Para leer las configuraciones de los parámetros de configuración del servidor idle necesita contar con un privilegio de inicio de sesión, mientras que para modificar los parámetros necesita el privilegio de configuración de iDRAC.

Para ver o modificar los parámetros, vaya a **Configuración** > **Configuración del sistema**.

La información de la detección del servidor idle se proporciona en función de los siguientes parámetros:

- Umbral del servidor idle (%): está establecido en un 20 % de manera predeterminada y se puede configurar de un 0 a un 50 %. La operación de restablecimiento establece el umbral en un 20 %.
- Intervalo del análisis del servidor idle (en horas): este es el período durante el que se recopilan las muestras por hora para determinar cuál es el servidor idle. Esto está establecido en 240 horas de manera predeterminada y se puede configurar de 1 a 9000 horas. La operación de restablecimiento establece el intervalo en 240 horas.
- Percentil de utilización del servidor (%): el valor del percentil de utilización se puede establecer entre un 80 y un 100 %. El valor predeterminado es de un 80 %. Si el 80 % de las muestras por hora disminuye bajo el umbral de utilización, se considera como un servidor idle.

Modificación de los parámetros de detección de servidores idle mediante RACADM

```
racadm get system.idleServerDetection
```

Modificación de los parámetros de detección de servidores idle mediante Redfish

```
https://<iDRAC IP>/redfish/v1/Managers/System.Embedded.1/Attributes
```

Modificación de los parámetros de detección de servidores idle mediante WSMAN

```
winrm e http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/root/dcim/DCIM_SystemAttribute
-u:root -p:calvin -r:https://<iDRAC IP>/wsman -SkipCNcheck -SkipCAcheck -encoding:utf-8
-a:basic
```

NOTA: La GUI de iDRAC no admite la visualización ni la modificación de los atributos.

Administración de GPU (aceleradores)

Los servidores Dell PowerEdge se envían con la unidad de procesamiento de gráficos (GPU). La administración de GPU permite ver las diversas GPU conectadas al sistema y también supervisar la alimentación, la temperatura y la información térmica de las GPU.

NOTA: Esta es una función que se concede bajo licencia y solo está disponible con la licencia iDRAC Enterprise y Datacenter. A continuación, se indican las propiedades disponibles con la licencia de Datacenter/Enterprise. Las demás propiedades aparecen incluso sin estas licencias:

Propiedades de GPU	Licencia de Datacenter	Licencia empresarial
Métricas térmicas		
Temperatura de destino de GPU	Sí	No
Temperatura mínima de ralentización de hardware de GPU	Sí	No
Temperatura de apagado de GPU	Sí	No
Temperatura máxima de funcionamiento de la memoria	Sí	No
Temperatura máxima de funcionamiento de la GPU	Sí	No
Estado de alerta térmica	Sí	No
Estado de interrupción de alimentación	Sí	No
Métricas de alimentación		
Estado del suministro de energía	Sí	No
Estado de suministro de energía de la placa	Sí	No
Telemetría		
Todos los datos de informes de telemetría	Sí	No

NOTA: No se mostrarán las propiedades de la GPU para las tarjetas GPU integradas y el estado se marcará como **desconocido**.

La GPU debe estar en el estado Listo antes de que el comando recupere los datos. En el campo GPUStatus del inventario, se muestra la disponibilidad de la GPU y si el dispositivo de GPU responde. Si el estado de la GPU es Listo, se muestra OK en GPUStatus; de lo contrario, se indica que el estado es No disponible.

La GPU ofrece varios parámetros de estado que se pueden extraer a través de la interfaz de SMBPB de las controladoras NVIDIA. Esta función está limitada solo a las tarjetas NVIDIA. A continuación, se indican los parámetros de estado recuperados del dispositivo GPU:

- Alimentación
- Temperatura
- Térmico

NOTA: Esta función solo está limitada a las tarjetas NVIDIA. Esta información no está disponible para otras GPU que puedan ser compatibles con el servidor. El intervalo para sondear las tarjetas GPU durante el PBI es de 5 segundos.

El sistema host debe tener instalado el controlador NVIDIA y ejecutarlo para el consumo de alimentación, la temperatura de destino de la GPU, la temperatura mínima de ralentización de la GPU, la temperatura de apagado de la GPU, la temperatura máxima de funcionamiento de la memoria y las funciones de temperatura máxima de funcionamiento de la GPU para que esté disponible. Estos valores se muestran como **N/A** cuando el controlador de la GPU no está instalado.

En Linux, cuando la tarjeta no está en uso, la controladora utiliza la tarjeta y se descarga para ahorrar energía. En estos casos, no están disponibles las características de consumo de energía, temperatura objetivo de la GPU, temperatura mínima de ralentización de la GPU, temperatura de apagado de la GPU, la temperatura máxima de funcionamiento de la memoria y las funciones de temperatura máxima de funcionamiento de la GPU. El modo persistente debe estar activado para que el dispositivo evite la descarga. Puede utilizar la herramienta nvidia-smi para habilitar esto mediante el comando `nvidia-smi -pm 1`.

Puede generar informes de la GPU mediante telemetría. Para obtener más información acerca de la función de telemetría, consulte Telemetry Streaming en la página 224

NOTA: En RACADM, puede ver entradas de GPU ficticias con valores vacíos. Esto puede ocurrir si el dispositivo no está listo para responder cuando la iDRAC genera una consulta al dispositivo GPU con el fin de obtener información. Ejecute la operación iDRAC `racrest` para resolver este problema.

Monitoreo de FPGA

Los dispositivos de arreglos de puertas programables en campo (FPGA) necesitan monitoreo en tiempo real del sensor de temperatura, ya que genera mucho calor cuando está en uso. Realice los siguientes pasos para obtener información de inventario FPGA:

- Apague el servidor.
- Instale el dispositivo FPGA en la tarjeta vertical.
- Encienda el servidor.
- Espere hasta que se complete la prueba POST.
- Inicie sesión en la GUI de iDRAC.
- Vaya a **Sistema** > **Descripción general** > **Aceleradores**. Puede ver las secciones GPU y FPGA.
- Amplíe el componente FPGA específico para ver la siguiente información del sensor:
  - Consumo de alimentación
  - Detalles de temperatura

NOTA: Debe tener privilegios de inicio de sesión de iDRAC para acceder a la información de FPGA.

NOTA: Los sensores de consumo de energía están disponibles solo para las tarjetas FPGA compatibles y solo están disponibles con licencia de centro de datos.

Consulta del sistema para verificar el cumplimiento de aire fresco

El enfriamiento de aire fresco utiliza directamente el aire exterior para enfriar los sistemas en el centro de datos. Los sistemas que cumplen con el requisito de aire fresco pueden funcionar por encima de su rango de funcionamiento ambiente normal (temperaturas de hasta 113 °F [45 °C]).

NOTA: Es posible que algunos servidores o ciertas configuraciones de un servidor no cumplan con el requisito de aire fresco. Consulte el manual del servidor específico para obtener detalles relacionados con el cumplimiento 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 (Enfriamiento)** > **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

Puede supervisar el porcentaje de tiempo en que el sistema ha funcionado a una temperatura ambiente superior al umbral de temperatura de aire fresco admitido normalmente. La lectura del sensor de temperatura de la placa base 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 temperaturas para los sistemas que no cumplen con el requisito de aire fresco. Sin embargo, los límites de umbral y las advertencias relacionadas con aire fresco que se generan se basan en los límites de aire fresco admitidos. Los límites son 42 °C para el umbral de advertencia y 47 °C para el umbral crítico. Estos valores corresponden a los límites de aire fresco de 40 °C y 45 °C con un margen 2 °C de precisión.

Se realiza un seguimiento de dos bandas de temperatura fijas asociadas a los límites de aire fresco:

- La banda de advertencia consta de la duración en 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 un 10 % del tiempo durante 12 meses.
- La banda crítica consta de la duración en que un sistema ha funcionado por encima del umbral crítico del sensor de temperatura (47 °C). El sistema puede funcionar en la banda crítica un 1 % del tiempo durante 12 meses, lo que también provoca incrementos de tiempo en la banda de advertencia.

Los datos recopilados se representan en un gráfico para realizar un seguimiento de los niveles de 10 % y 1 %. Los datos de temperatura registrados se pueden borrar solamente antes de salir de fábrica.

Se genera un evento si el sistema continúa funcionando por encima del umbral de temperatura admitido normalmente durante un tiempo de funcionamiento especificado. Si la temperatura promedio durante el tiempo de funcionamiento especificado es superior al nivel de advertencia (> = 8 %) o al nivel crítico (> = 0,8 %), se registra un evento en el registro de Lifecycle y se genera la captura SNMP correspondiente. Los eventos 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 eventos adicionales. Para obtener más información, consulte la sección Configuración de suceso de periodicidad de alertas en la página 188.

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, consulte **Sistema** > **Descripción general** > **Refrigeración** > **Descripción general de temperatura**.
   Se muestra la página **Descripción general de temperatura**.
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.

   NOTA: La tarjeta gráfica AMD WX3200 actualmente no admite la interfaz I2C para los sensores de temperatura. Por lo tanto, las lecturas de temperatura no estarán disponibles para esta tarjeta desde las interfaces de iDRAC.

Visualización de datos históricos de temperatura mediante RACADM

Para ver los datos históricos mediante RACADM, utilice el comando `inlettemphistory`.

Para obtener más información, consulte *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

Configuración del umbral de advertencia para la temperatura de entrada

Es posible modificar los valores de los umbrales de advertencia mínimo y máximo para el sensor de temperatura de entrada de la placa base. Si se realiza una acción para restablecer los valores predeterminados, los umbrales de temperatura se establecen en los valores predeterminados. Debe tener el privilegio Configure user (Configurar usuario) para poder establecer los valores de umbral de advertencia para el sensor de temperatura de entrada.

Configuración del umbral de advertencia para la temperatura de entrada mediante la interfaz web

Para configurar el umbral de advertencia para la temperatura de entrada:

1. En la interfaz web de iDRAC, consulte **Sistema** > **Descripción general** > **Refrigeración** > **Descripción general de temperatura**.
   Se muestra la página **Descripción general de temperatura**.
2. En la sección **Sondas de temperatura**, para la **Temp. de entrada de la placa base**, ingrese los valores mínimos y máximos para el **Umbral de advertencia** en centígrados o Fahrenheit. Si ingresa el valor en centígrados, el sistema calcula y muestra automáticamente el valor en Fahrenheit. De la misma manera, si ingresa el valor en Fahrenheit, se muestra el valor en centígrados.
3. Haga clic en **Aplicar**.
   Se configuran los valores.

   NOTA: Los cambios en los umbrales predeterminados no se reflejan en el gráfico de datos históricos, ya que los límites del gráfico son solo para los valores de límite de aire fresco. Las advertencias por superar los umbrales personalizados son diferentes a la advertencia asociada por superar umbrales de aire fresco.

Visualización de interfaces de red disponibles en el sistema operativo host

Puede ver la información acerca de todas las interfaces de red que están disponibles en el sistema operativo del host como, por ejemplo, las direcciones IP que están asignadas al servidor. El Módulo de servicios de la iDRAC proporciona esta información a la iDRAC. La información de la dirección IP del sistema operativo incluye las direcciones IPv4 e IPv6, la dirección MAC, la máscara de subred o la longitud del prefijo, el FQDD del dispositivo de red, el nombre de la interfaz de red, la descripción de la interfaz de red, el estado de la interfaz de red, el tipo de interfaz de red (Ethernet, túnel, bucle, etc.), la dirección del gateway, la dirección del servidor DNS, y la dirección del servidor DHCP.

NOTA: Esta función está disponible con las licencias iDRAC Express e iDRAC Enterprise/Datacenter.

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 de información de sistema operativo se encuentra activada en la página **Configuración de iDRAC Settings** > **Descripción general** > **Módulo de servicios 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 de 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 del dispositivo correspondiente desde **Hardware** > **Network Devices (Dispositivos de red)**, donde se pueden ver los detalles del dispositivo. Para obtener información acerca de 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 de sistema operativo de host relacionada con un dispositivo de red desde **Hardware** > **Network Devices (Dispositivos de red)**. Haga clic en **View Host OS Network Interfaces (Ver interfaces de red de sistema operativo de 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 del host mediante RACADM. Para obtener más información, consulte *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

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

En los servidores Blade, FlexAddress permite el uso de nombres de red mundial y direcciones MAC (WWN/MAC) persistentes con chasis asignado para cada conexión de puerto de servidor administrada.

Puede ver la información siguiente para cada puerto de tarjeta Ethernet incorporada y tarjeta mezzanine opcional instalada:

- Redes Fabric a las que están conectadas las tarjetas
- Tipo de red Fabric.
- Direcciones MAC asignadas por el servidor, asignadas por el chasis o asignadas de manera remota.

Para ver la información de FlexAddress en iDRAC, configure y active la función FlexAddress en Chassis Management Controller (CMC). Para obtener más información, consulte *Guía del usuario de la controladora de administración del chasis* disponible en https://www.dell.com/cmcmanuals. Las sesiones existentes de consola virtual o medios virtuales se cerrarán si se activa o desactiva la configuración de FlexAddress.

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

La función FlexAddress reemplaza las direcciones MAC asignadas por el servidor con direcciones MAC asignadas por el chasis y se implementa para iDRAC junto con las LOM de servidores blade, las tarjetas mezzanine y los módulos de E/S. La función FlexAddress de iDRAC admite la conservación de una dirección MAC específica de ranura para iDRAC en un chasis. La dirección MAC asignada por el chasis se almacena en una memoria no volátil de CMC y se envía a iDRAC durante un inicio de iDRAC o cuando se activa FlexAddress de CMC.

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

- **Sistema Detalles Detalles de iDRAC**.
- **Sistema Servidor WWN/MAC**.
- **Configuración de iDRAC** > **Descripción general** > **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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

8

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 asegurarse de que los comandos RACADM locales de importación o exportación funcionen correctamente, asegúrese de que el host de almacenamiento masivo USB esté habilitado en el sistema operativo. Para obtener información acerca de cómo habilitar 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 18. 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 IPMI	Parte del firmware iDRAC Comunicación en serie RAC o IPMI activada
Comunicación en serie IPMI en la LAN	Protocolo de bus de administración de plataforma inteligente SSH	IPMI	IPMITool se instala y la Comunicación en serie IPMI en la LAN está activada
IPMI en la LAN	Protocolo de bus de administración de plataforma inteligente	IPMI	IPMITool se instala y la configuración IPMI se activa
RACADM remoto	HTTPS	RACADM remoto	RACADM remoto se instala y activa
Firmware RACADM	SSH	Firmware RACADM	Firmware RACADM se instala y se activa.
RACADM local	IPMI	RACADM local	Local RACADM se instala
Servicios remotos [1]	WSMan	WinRM (Windows) OpenWSMan (Linux)	WinRM se instala (Windows) o OpenWSMan se instala (Linux)
	Redfish	Diversos complementos del explorador, 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 *Guía del usuario de Lifecycle Controller* disponible en https://www.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 *Guía del usuario de la controladora de administración del chasis* disponible en https://www.dell.com/cmcmanuals (no válido para las plataformas MX) *Guía del usuario de OME - Modular para el chasis PowerEdge MX7000* disponible en https://www.dell.com/openmanagemanuals (válido para las plataformas MX).

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 el ciclo de apagado y encendido del servidor desde vConsole o la GUI para cualquier cambio en la velocidad en baudios.

   NOTA: Si se desactivó la autenticación de conexión en serie de la iDRAC, se debe utilizar el comando racreset de iDRAC para realizar 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 la ubicación del sistema administrado en el proceso de arranque, puede ver la pantalla POST o la pantalla del sistema operativo. Este procedimiento se basa en la configuración: SAC para Windows y pantallas en 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: compatible con una interfaz binaria para el acceso a programas, 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 eventos del sistema usando 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: Se proporcionan el nombre de usuario y la contraseña predeterminados de iDRAC en la etiqueta del sistema.
- Modo de terminal IPMI: compatible con los comandos ASCII que se envían desde un terminal en serie. Este modo es compatible con una cantidad limitada de comandos (incluido el control de alimentación) y comandos IPMI sin formato que se escriben como caracteres ASCII hexadecimales. Le permite ver las secuencias de arranque del sistema operativo hasta el BIOS, cuando inicia sesión en iDRAC a través de SSH. Debe cerrar sesión en el terminal de IPMI mediante `[sys pwd -x]`, a continuación, aparece un ejemplo de los comandos del modo de terminal 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 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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

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

La 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` (Inicio de sesión de iDRAC) (si la iDRAC está configurada en modo en serie RAC) o bien el modo de conexión en 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 en la LAN de IPMI (SOL) permite el redireccionamiento de los datos en serie de la consola basada en texto del sistema administrado a través de la red Ethernet de administración fuera de banda dedicada o compartida de iDRAC. Con la SOL, 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. Activar un protocolo compatible (SSH, 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 formato 25 x 80. La ventana de SSH que se utiliza para invocar el comando `console com2` debe estar configurada en formato 25 x 80. De esta manera, la pantalla redirigida se mostrará correctamente.

NOTA: Si el cargador de inicio o el sistema operativo realiza una redirección en 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 error de varios componentes intentando acceder 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 habrá establecido la configuración avanzada de SOL de IPMI. 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: Para activar SOL de IPMI, debe tener el privilegio mínimo se define en 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 compatibles son IPMI y SSH.

Activación del protocolo admitido mediante la interfaz web

Para habilitar SSH, vaya a **Configuración de iDRAC** > **Servicios** y seleccione **Activado** para SSH.

Para activar IPMI, vaya a **Configuración de iDRAC** > **Conectividad** y seleccione **Configuración de IPMI**. Asegúrese de que el valor de la **Clave de cifrado** esté todo en cero o presione la tecla de retroceso para borrar y cambiar el valor a caracteres nulos.

Activación del protocolo admitido mediante RACADM

Para habilitar SSH, utilice el siguiente comando:

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

SOL mediante el protocolo IPMI

La utilidad SOL basada en IPMI e IPMItool utilizan 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 carga útil 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 autentificación. El valor predeterminado es una cadena de 40 ceros.

Se debe cifrar una conexión de RMCP+ con iDRAC utilizando la clave de cifrado (clave del generador de claves). Puede configurar la clave de cifrado con la interfaz web o la utilidad de configuración de iDRAC.

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

NOTA: Si se requiere, puede cambiar el tiempo de espera predeterminado de SOL en **Configuración de iDRAC** > **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.

NOTA: Es posible que se finalice la sesión SOL de IPMI mientras se copia un texto de entrada grande desde un cliente con SO Windows a un host con SO Linux. Con el fin de evitar que se finalice abruptamente la sesión, convierta cualquier texto grande a un fin de línea basado en UNIX.

NOTA: Si existe una sesión SOL creada con la herramienta RACADM e inicia otra sesión SOL con la herramienta IPMI, no se mostrará ningún error ni notificación acerca de las sesiones existentes.

NOTA: Debido a la configuración del sistema operativo Windows, una sesión SOL conectada a través de SSH y la herramienta IPMI pueden pasar a una pantalla en blanco después de arrancar. Desconecte y vuelva a conectar la sesión SOL para volver al símbolo del sistema de SAC.

SOL mediante SSH

Secure Shell (SSH) es un protocolo de red que se usa para establecer comunicaciones de línea de comandos con iDRAC. Es posible analizar comandos de SMCLP remoto a través de esta interfaz.

SSH mejoró la seguridad. La iDRAC solo admite SSH, versión 2, con autenticación de contraseña y está activado de manera predeterminada. iDRAC admite hasta dos a cuatro sesiones de SSH a la vez.

NOTA: A partir de iDRAC versión 4.40.00.00, la función Telnet se eliminó de iDRAC, de modo que las propiedades relacionadas del registro de atributos están obsoletas. Aunque algunas de estas propiedades aún están disponibles en iDRAC para mantener la compatibilidad con versiones anteriores de las aplicaciones y los scripts de consola existentes, el firmware de iDRAC ignora la configuración correspondiente.

NOTA: Al establecer una conexión SSH, se muestra un mensaje de seguridad: "se requiere autenticación adicional". Aunque no esté habilitado 2FA.

NOTA: En el caso de las plataformas MX, una sesión de SSH se utilizará para la comunicación de iDRAC. Si se están utilizando todas las sesiones, no se iniciará iDRAC hasta que una quede disponible.

Para conectarse a iDRAC, utilice programas de código abierto, como PuTTY u OpenSSH que admitan SSH en una estación de administración.

NOTA: Ejecute `OpenSSH` desde un emulador de terminal ANSI o VT100 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 mostrarán gráficos).

Antes de utilizar SSH 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 mediante la interfaz web de iDRAC o RACADM.

   Cliente SSH (puerto 22) <--> Conexión WAN <--> iDRAC

   La SOL basada en IPMI que utiliza el protocolo SSH elimina la necesidad de utilidades adicionales, ya que la traducción de la comunicación en serie a la red se realiza dentro de iDRAC. La consola de SSH que se utilice debe poder interpretar y responder a los datos provenientes del puerto serial 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 SSH.

Uso de SOL desde PuTTY en Windows

NOTA: Si se requiere, puede cambiar el tiempo de espera predeterminado de SSH en **Configuración de iDRAC** > **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] <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 SOL desde la estación de administración al sistema administrado mediante el protocolo SSH. Para acceder a la consola de la línea de comandos de iDRAC, siga la secuencia de teclas ESC. Comportamiento de conexión 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 emergencia (EMS) inmediatamente después de un reinicio del host, es posible que la terminal de la consola de administración especial (SAC) se dañe. Cierre la sesión SOL, cierre la terminal, abra otra terminal e inicie la sesión SOL con el mismo comando.

NOTA: Debido a la configuración del sistema operativo Windows, una sesión SOL conectada a través de SSH y la herramienta IPMI pueden pasar a una pantalla en blanco después de arrancar. Desconecte y vuelva a conectar la sesión SOL para volver al símbolo del sistema de SAC.

Uso de SOL desde OpenSSH en Linux

Para iniciar SOL desde OpenSSH en una estación de administración de Linux:

NOTA: Si se requiere, puede cambiar el tiempo de espera de la sesión predeterminado de SSH en **Configuración de iDRAC** > **Servicios**.

1. Inicie una ventana de shell.
2. Conéctese a iDRAC mediante el siguiente comando: ssh *<iDRAC-ip-address>* -l *<login name>*
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 que se establece una sesión SOL, la consola de línea de comandos iDRAC no está disponible. Siga la secuencia de escape correctamente para abrir la consola de línea de comandos iDRAC. La secuencia de escape también se imprime en la pantalla tan pronto como se conecta una sesión SOL. Cuando el sistema administrado está apagado, toma algún tiempo establecer la sesión SOL.

   NOTA: Puede utilizar la consola com1 o la consola com2 para iniciar SOL. Reinicie el servidor para establecer la conexión.

   El comando `console -h com2` muestra el contenido del buffer de historial de la conexión serie antes de esperar información proveniente del teclado o nuevos caracteres provenientes del puerto serial.

   El tamaño predeterminado (y máximo) del buffer de historial es de 8192 caracteres. Puede configurar este número en un valor menor mediante el comando:

   ```
   racadm set iDRAC.Serial.HistorySize <number>
   ```

4. Cierre la sesión SOL para cerrar la sesión SOL activa.

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

Los comandos para desconectar una sesión SOL se basan en la utilidad. Solo puede salir de la utilidad cuando una sesión SOL ha terminado completamente.

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.

Si una sesión SOL no termina completamente en la utilidad, otras sesiones SOL pueden no estar disponibles. Para resolver esto, termine la consola de la línea de comandos en la interfaz web en **Configuración de iDRAC** > **Conectividad** > **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 de IPMI que se ejecutan mediante la interfaz de 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: 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 con 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 con 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 en la página 120.

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 *Guía del usuario de OpenManage Server Administrator* disponible en https://www.dell.com/openmanagemanuals.

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 arranque en RHEL 6

Los pasos siguientes se aplican a Linux GRand Unified Bootloader (GRUB). Se deben realizar cambios similares si se utiliza un cargador de inicio diferente.

NOTA: Al configurar la ventana de emulación de cliente VT100, defina la ventana o la aplicación que está mostrando la consola virtual redirigida en 25 filas x 80 columnas para garantizar que el texto se muestre correctamente. De lo contrario, es posible que algunas pantallas de texto se vean distorsionadas.

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 comience con `splashimage`.

   En el ejemplo siguiente se proporciona un archivo **/etc/grub.conf** que muestra los cambios que se describen en este procedimiento.

```
# grub.conf generated by anaconda
# Note that you do not have to rerun grub after making changes to this file
# NOTICE: You do not have a /boot partition. This means that all
# kernel and initrd paths are relative to /, e.g.
# root (hd0,0)
# kernel /boot/vmlinuz-version ro root=/dev/sdal
# initrd /boot/initrd-version.img
#boot=/dev/sda
default=0
timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz

serial --unit=1 --speed=57600
terminal --timeout=10 serial

title Red Hat Linux Advanced Server (2.4.9-e.3smp) root (hd0,0)
kernel /boot/vmlinuz-2.4.9-e.3smp ro root=/dev/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 que `console=ttyS1,57600` se ha agregado a la primera opción.

   NOTA: Si el cargador de inicio o el sistema operativo realiza una redirección en 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 error de varios componentes intentando acceder 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
```

Configuración del terminal en serie en RHEL 7

Para configurar el terminal en serie en RHEL 7, realice lo siguiente:

1. Agregue las siguientes líneas a `/etc/default/grub` o actualícelas en dicha ruta:

   ```
   GRUB_CMDLINE_LINUX_DEFAULT="console=tty0 console=ttyS0,115200n8"
   ```

   ```
   GRUB_TERMINAL="console serial"
   ```

   ```
   GRUB_SERIAL_COMMAND="serial --speed=115200 --unit=0 --word=8 --parity=no --stop=1"
   ```

   Si utiliza `GRUB_CMDLINE_LINUX_DEFAULT`, solo se aplicará esta configuración a la entrada de menú predeterminada. Utilice `GRUB_CMDLINE_LINUX` para aplicarla a todas las entradas de menú.

   Cada línea debe aparecer solo una vez en `/etc/default/grub`. Si la línea ya existe, modifíquela para evitar que se realice otra copia. Por lo tanto, solo se permite una línea `GRUB_CMDLINE_LINUX_DEFAULT`.

2. Recompile el archivo de configuración `/boot/grub2/grub.cfg` ejecutando el comando `grub2-mkconfig -o` como se indica a continuación:
   - en sistemas basados en BIOS:

     ```
     ~]# grub2-mkconfig -o /boot/grub2/grub.cfg
     ```

   - en sistemas basados en UEFI:

     ```
     ~]# grub2-mkconfig -o /boot/efi/EFI/redhat/grub.cfg
     ```

Para obtener más información, consulte la Guía del administrador del sistema RHEL 7 en redhat.com.

Control de GRUB desde la consola en serie

Puede configurar GRUB para que utilice la consola en serie en lugar de la consola VGA. Esto le permite interrumpir el proceso de arranque y elegir un kernel distinto o agregar parámetros de kernel; por ejemplo, para realizar el arranque en el modo de usuario único.

Para configurar GRUB a fin de utilizar la consola en serie, convierta en comentario la imagen de presentación y agregue las opciones `serial` y `terminal` a `grub.conf`:

```
[root@localhost ~]# cat /boot/grub/grub.conf
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/hda2
#          initrd /initrd-version.img
#boot=/dev/hda
default=0
timeout=10
#splashimage=(hd0,0)/grub/splash.xpm.gz
serial --unit=0 --speed=1152001
```

NOTA: Reinicie el sistema para que entre en efecto la configuración.

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 19. 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

Tabla 19. Esquemas de criptografía SSH (continuación)

Tipo de esquema	Algoritmos
	diffie-hellman-group-exchange-sha256 diffie-hellman-group14-sha1
Cifrado	chacha20-poly1305@openssh.com aes128-ctr aes192-ctr 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 autenticación de claves públicas (PKA) sobre SSH. Esta es una función con licencia. Cuando se configura y se utiliza correctamente la PKA sobre SSH, debe introducir el nombre de usuario al iniciar sesión en la iDRAC. Esto es de utilidad a la hora de configurar secuencias de comandos automatizadas que realizan distintas funciones. Las claves cargadas deben tener el formato de OpenSSH o RFC 4716. De lo contrario, deberá convertir las claves a ese formato.

En cualquier escenario, se debe generar un par de claves (una privada y una 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 SSH para establecer la relación de confianza entre la estación de administración e iDRAC.

Puede generar el par de claves pública o privada mediante los elementos siguientes:

- La aplicación *Generador de clave PuTTY* para clientes que ejecutan Windows
- La CLI *ssh-keygen* para clientes que ejecutan Linux.

PRECAUCIÓN: Este privilegio normalmente se reserva para usuarios que son miembros del grupo de usuarios Administrator (Administrador) 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 eliminación de cualquier usuario, la administración de claves SSH para usuarios, etc. Por estos motivos, asigne este privilegio con cuidado.

PRECAUCIÓN: La capacidad para cargar, ver o eliminar claves SSH se basa en el privilegio del usuario "Configure Users" (Configurar usuarios). Este privilegio permite a los usuarios configurar la clave SSH de otros usuarios. Debe tener cuidado a la hora de otorgar este privilegio.

Generación de claves públicas para Windows

Para usar la aplicación *generador de claves PuTTY* y crear la clave básica:

1. Inicie la aplicación y seleccione RSA para el tipo de clave.
2. Especifique la cantidad de bits para la clave. El número de bits debe estar entre 2048 y 4096 bits.
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* para 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 que no es 4716. Convierta las claves al formato 4716 con `ssh-keygen -e -f /root/.ssh/id_rsa.pub > std_rsa.pub`. No cambie los permisos del archivo de claves. 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 encuentren en el índice donde se agregará la 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>`
- Desde RACADM remoto mediante 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 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)**.
   Se muestra la página **SSH Key (Clave SSH)** con los detalles **Edit From (Editar desde)**.
4. Seleccione **Remove (Quitar)** para las claves que desee 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`

9

Configuración de cuentas de usuario y privilegios

Puede configurar las cuentas de usuario con privilegios específicos (*autoridad basada en funciones*) para administrar el sistema mediante la iDRAC y mantener la seguridad del sistema. De manera predeterminada, la iDRAC está configurada con una cuenta de administrador local. El nombre de usuario y la contraseña de iDRAC predeterminados se proporcionan con la insignia del sistema. Como administrador, puede configurar cuentas de usuario para permitir a otros usuarios acceder 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 autorizadas de usuario.

iDRAC admite el acceso basado en funciones a los usuarios con un conjunto de privilegios asociados. Las funciones son administrador, operador, solo lectura o ninguna. La función define los privilegios máximos disponibles.

Temas:

Funciones y privilegios de usuario de iDRAC

Se cambiaron los nombres de privilegio y función de iDRAC en comparación generaciones anteriores de servidores. Los nombres de funciones son:

Tabla 20. Roles de iDRAC

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

En la siguiente tabla se describen los privilegios de usuario:

Tabla 21. 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.

Tabla 21. Privilegios del usuario del iDRAC (continuación)

Generación actual	Generación anterior	Descripción
Configurar	Configurar iDRAC	Permite al usuario configurar el iDRAC. Con este privilegio, un usuario también puede configurar la administración de energía, la consola virtual, los medios virtuales, las licencias, la configuración del sistema, los dispositivos de almacenamiento, la configuración del BIOS, SCP, entre otros.
NOTA: La función de administrador reemplaza todos los privilegios de otros componentes, como la contraseña de configuración del BIOS.		
Configurar usuarios	Configurar usuarios	Permite activar la capacidad del usuario de otorgar permisos de acceso al sistema a usuarios específicos.
Registros	Borrar registros	Permite al usuario borrar solo el registro de eventos del sistema (SEL).
Control del sistema	Controlar y configurar sistema	Permite ejecutar un ciclo de energía en el sistema host.
Acceder a la consola virtual	Redirección de acceso a la consola virtual (para servidores Blade) Acceder a la consola virtual (para servidores tipo bastidor y torre)	Permite al usuario ejecutar la consola virtual.
Acceder a los medios virtuales	Acceder a los medios virtuales	Permite al usuario ejecutar y usar los medios virtuales.
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.

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.

NOTA: La contraseña debe incluir una letra mayúscula y una minúscula, un número y un carácter especial.

Utilice los siguientes caracteres al crear nombres de usuario y contraseñas:

Tabla 22. Caracteres recomendados para los nombres de usuario

Caracteres	Longitud
0-9 A-Z a-z - ! # $ % & ( ) * ; ? [\ ] ^ _ ` { | } ~ + < = >	1–16

Tabla 23. Caracteres recomendados para las contraseñas

Caracteres	Longitud
0-9 A-Z a-z ' - ! " # $ % & ( ) * , . / : ; ? @ [\ ] ^ _ ` { | } ~ + < = >	1–40

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 usar solo los caracteres que se indican aquí.

NOTA: Los caracteres permitidos en los nombres de usuario y contraseñas para recursos compartidos de red están determinados por el tipo de recurso compartido de red. IDRAC admite caracteres válidos para credenciales de recursos compartidos de red, tal y como lo define el de recurso compartido, excepto <, >, y , (coma).

NOTA: Para mejorar la seguridad, se recomienda utilizar contraseñas complejas de ocho caracteres o más, que incluyan letras minúsculas, mayúsculas, números y caracteres especiales. También se recomienda cambiar periódicamente las contraseñas, si es 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 establecer nombres de usuario, contraseñas y funciones 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 autenticación 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)** > **User (Usuario)**. Aparecerá la página **Usuarios locales**.
2. En la columna **User ID (Id. de usuario)**, seleccione un número de Id. de usuario y, a continuación, haga clic en **Edit (Editar)**.

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

   Aparecerá la página **User Configuration (Configuración de usuario)**.
3. Agregue los detalles de **User Account Settings (Configuración de 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 la función de usuario (los privilegios de acceso) del usuario en cuestión. También puede activar el nivel de privilegio de LAN, el nivel de privilegio de puerto serie, el estado de comunicación en serie en la LAN, la autenticación 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 **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 la etiqueta del sistema. El comando `racadm racresetcfg` restablece iDRAC a los valores predeterminados.

NOTA: Si SEKM está habilitado en el servidor, desactive SEKM mediante el comando `racadm sekm disable` antes de utilizar este comando. Esto puede evitar que se bloqueen los dispositivos de almacenamiento protegidos por iDRAC, en caso de que la configuración de SEKM se borre de iDRAC mediante la ejecución de este comando.

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 un nombre de usuario se muestra después del signo =, significa que se tomó ese número de índice.

NOTA: Puede utilizar

```
racadm get -f <myfile.cfg>
```

y ver o editar el

```
myfile.cfg
```

archivo, que incluye todos los parámetros de configuración de la iDRAC.

Para activar la autentificación de SNMPv3 para un usuario, use objetos **SNMPv3AuthenticationType**, **SNMPv3Enable** y **SNMPv3PrivacyType**. Para obtener más información, consulte *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

Si está utilizando el archivo perfil de configuración de servidor para configurar usuarios, utilice los atributos **AuthenticationProtocol**, **ProtocolEnable** y **PrivacyProtocol** para activar la autenticación 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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.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 privilegios específicos del usuario, consulte *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

Configuración de usuarios de Active Directory

Si su empresa utiliza el software Microsoft Active Directory, puede configurarlo para proporcionar acceso a iDRAC, lo que permite agregar y controlar los privilegios de usuario de iDRAC para los usuarios existentes en el servicio de directorio. Esta es una función con licencia.

Puede configurar la autenticación de usuario a través de Active Directory para iniciar sesión en iDRAC. También puede proporcionar autoridad basada en funciones, lo que permite que un administrador configure privilegios específicos para cada usuario.

NOTA: Para cualquier implementación realizada a través de la plantilla MX y la validación de CA que está habilitada en la plantilla, el usuario debe cargar los certificados de CA en el primer inicio de sesión o antes de cambiar el servicio de autenticación de LDAP a Active Directory o viceversa.

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:

- Implementación de una infraestructura de Active Directory. Consulte el sitio web de Microsoft para obtener más información.
- Integración de PKI en la infraestructura de Active Directory. La iDRAC utiliza el mecanismo estándar de infraestructura de clave pública (PKI) para la autentificación 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 la iDRAC autentica los usuarios en una controladora de dominio de Active Directory, inicia una sesión de SSL en la controladora de dominio. En este momento, la controladora debe publicar un certificado firmado por la autoridad de certificados (CA), el certificado raíz que también se carga en iDRAC. Para que la iDRAC autentique *cualquier* controladora de dominio (ya

sea la controladora de dominio raíz o 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 **Inicio** > **Herramientas administrativas** > **Política de seguridad de dominio**.
2. Expanda la carpeta **Políticas de claves públicas**, haga clic con el botón derecho del mouse en **Configuración de la solicitud de certificados automática** y haga clic en **Solicitud de certificados automática**.
   Aparece el **Asistente para instalación de petición automática de certificado**.
3. Haga clic en **Siguiente** y seleccione **Controladora de dominio**.
4. Haga clic en **Next (Siguiente)** y, después, en **Finish (Finalizar)**. Se instalará el certificado SSL.

Exportación de un certificado de CA raíz de la controladora de dominio a iDRAC

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. Ingrese `mmc` y haga clic en **Aceptar**.
4. En la ventana **Consola 1** (MMC), haga clic en **Archivo (**o **Consola)** 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. Selecione **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 **Consola 1** , vaya a la carpeta **Certificados Personal Certificados**.
10. Localice el certificado de CA raíz y haga clic con el botón derecho del mouse sobre ese elemento. Seleccione **Todas las tareas** y haga clic en **Exportar…**.
11. En el **Asistente de exportación de certificados**, haga clic en **Siguiente** y seleccione **No exportar la clave privada**.
12. Haga clic en **Siguiente** y seleccione **Codificado en base 64 X.509 (.cer)** como el formato.
13. Haga clic en **Siguiente** y guarde el certificado en un directorio del sistema.
14. Cargue el certificado guardado en el paso 13 en iDRAC.

Importación del certificado SSL de firmware de iDRAC

El certificado SSL de la iDRAC es el certificado idéntico que se utiliza para el servidor web de la iDRAC. Todas las controladoras iDRAC se entregan con un certificado autofirmado predeterminado.

Si el servidor de Active Directory se ha configurado para autenticar al cliente durante la etapa de inicialización de una sesión SSL, deberá cargar el certificado del servidor de la iDRAC en la controladora de dominio de Active Directory. Este paso adicional no es necesario si Active Directory no realiza la autenticación de cliente durante la etapa de inicialización de una sesión SSL.

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 1 -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 confiable)**. De lo contrario, deberá instalar el certificado 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 (Terminar)** y, después, haga clic en **OK (Aceptar)**. Se importará el certificado SSL del firmware de la iDRAC en todas las listas de certificado 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 *Extended schema (Esquema extendido)*, que contiene objetos personalizados de Active Directory. Todos los objetos de control de acceso se mantienen en Active Directory. Esto proporciona la máxima flexibilidad a la hora de configurar el acceso de los usuarios en distintas 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.

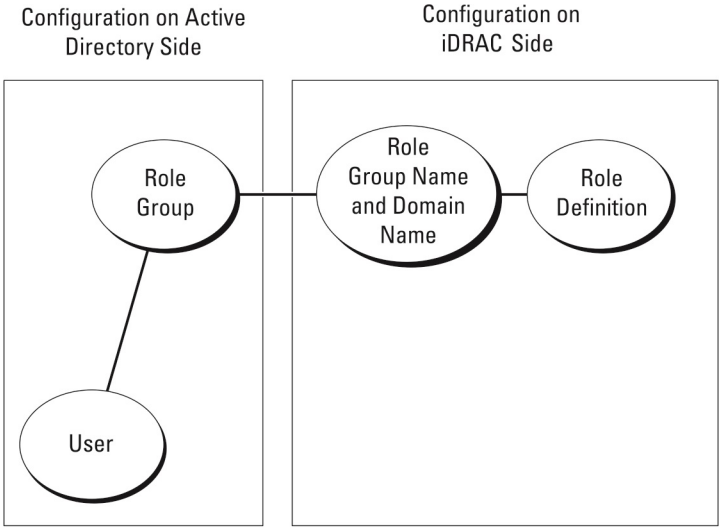


Ilustración 1. Configuración de iDRAC con el esquema estándar de Active Directory

En Active Directory, se utiliza una función de grupo estándar como un grupo de funciones. Un usuario que tiene acceso a la iDRAC es miembro del grupo de funciones. Para dar este acceso de usuario a una iDRAC específica, se deben configurar en la iDRAC específica el nombre del grupo de funciones y su nombre de dominio. La función y el nivel de privilegios se definen en cada iDRAC y no en Active Directory. Puede configurar hasta 15 grupos de roles en cada iDRAC. La referencia de la tabla no muestra los privilegios predeterminados del grupo de funciones.

Tabla 24. 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 la iDRAC. En este caso de dominio único, se admite cualquier tipo de grupo.

Si todos los usuarios y grupos de roles de inicio de sesión, incluidos los grupos anidados, se encuentran en varios dominios, es necesario configurar las direcciones de servidor del catálogo global en la iDRAC. En este caso de dominio múltiple, todos los grupos de roles y grupos anidados (si los hay) deben ser del tipo de grupo universal.

Configuración del esquema estándar de Active Directory

Antes de configurar el esquema estándar de Active Directory, asegúrese de lo siguiente:

- Cuenta con una licencia de iDRAC Enterprise o Datacenter.
- La configuración se lleva a cabo en un servidor que se utiliza como la controladora de dominio.
- La información de fecha, hora y zona horaria del servidor es correcta.
- La configuración de red de iDRAC está establecida o, en la interfaz web de iDRAC, vaya a **Configuración de iDRAC > Conectividad > Red > Configuración común** para establecer la configuración de red.

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 los usuarios y grupos de 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 el FQDN de catálogo global y las controladoras de dominio. Esto se realiza en los próximos pasos. Por lo tanto, el DNS debe configurarse correctamente 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 las respuestas de Active Directory durante el inicio de sesión de iDRAC.

   NOTA: Si la validación de certificados está activada, 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 la 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 la opción Standard Schema (Esquema estándar), son las direcciones de las controladoras de dominio donde se ubican las cuentas de usuario y los grupos de funciones.
- El servidor de catálogo global solo es necesario para el esquema estándar cuando las cuentas de usuario y los grupos de funciones se encuentran en dominios diferentes. En el caso de varios dominios, solo se puede usar 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 la validación de certificados está activada, 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 1 -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 los objetos de asociación de Dell para unir iDRAC y el permiso. Esto le permite usar iDRAC en función de los permisos otorgados en general. La lista de control de acceso (ACL) predeterminada de los objetos de asociación de Dell permite la administración propia y de administradores de dominios de los permisos y el ámbito 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 generar que se proporcionen privilegios no previstos 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 los atributos de la clase de usuario pueden incluir el nombre, el apellido, el número de teléfono, etc. Puede extender 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 y 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. exclusiva. Para mantener las Id. exclusivas en toda la industria, Microsoft mantiene una base de datos de identificadores de objeto (OID) de Active Directory, de modo que cuando las empresas agregan extensiones al esquema, pueden tener la garantía de que serán exclusivas y no entrarán en conflicto entre sí. Para extender el esquema en Microsoft Active Directory, Dell recibió OID exclusivos, extensiones de nombre exclusivas e Id. de atributo vinculadas exclusivas para los atributos y las clases que se agregan al servicio de directorio:

- La extensión es: `dell`.
- El OID base es: `1.2.840.113556.1.8000.1280`.
- El rango de Id. de enlace 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 los usuarios o grupos con un conjunto específico de privilegios para uno o varios dispositivos iDRAC. Este modelo le proporciona a un administrador 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 la 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 se puede vincular (o bien, se puede vincular usuarios, grupos de usuarios u objetos de dispositivo de iDRAC) con un solo objeto de privilegio. Este ejemplo permite al administrador controlar los privilegios de cada usuario en dispositivos iDRAC específicos.

El objeto de dispositivo iDRAC es el enlace 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 autentifiquen los usuarios.

En la figura siguiente se muestra que el objeto de asociación proporciona la conexión necesaria para la autentificación y la autorización.

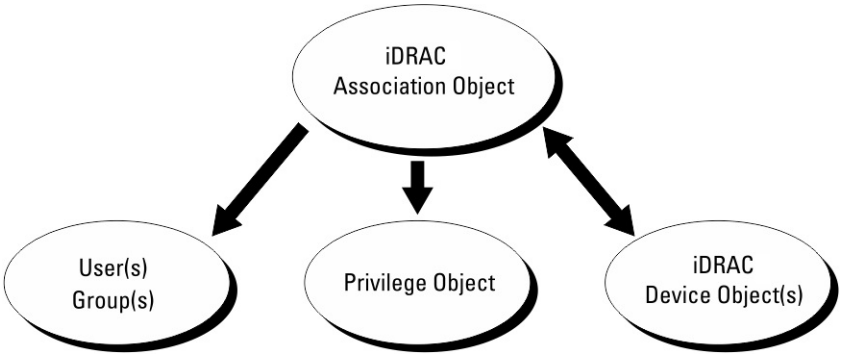


Ilustración 2. Configuración típica de los objetos de active directory

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 la autorización con iDRAC.

El objeto de asociación permite el número de usuarios o grupos que sea necesario, así como los objetos de dispositivo iDRAC. No obstante, el objeto de asociación solo incluye un objeto de privilegio por objeto de asociación. El objeto de asociación conecta los usuarios con privilegios en los dispositivos iDRAC.

La extensión de Dell al complemento ADUC MMC solo permite asociar el objeto de privilegio y los objetos iDRAC desde el mismo dominio con el objeto de asociación. La extensión de Dell no permite que un grupo o un objeto iDRAC de otros dominios se agregue como miembro del 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 creados por la utilidad Dell Schema Extender son grupos locales de dominio y no funcionan con grupos universales de otros dominios.

Al objeto de asociación, se pueden agregar los usuarios, los grupos de usuarios o los grupos de usuarios anidados de cualquier dominio. Las soluciones de esquema extendido admiten cualquier usuario tipo de grupo y cualquier anidamiento de grupo de usuarios en varios dominios admitido por Microsoft Active Directory.

Acumulación de privilegios con el esquema extendido

El mecanismo de autenticación de esquema extendido admite la acumulación de privilegios desde distintos objetos de privilegio asociados con el mismo usuario a través de distintos objetos de asociación. En otras palabras, la autenticación 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.

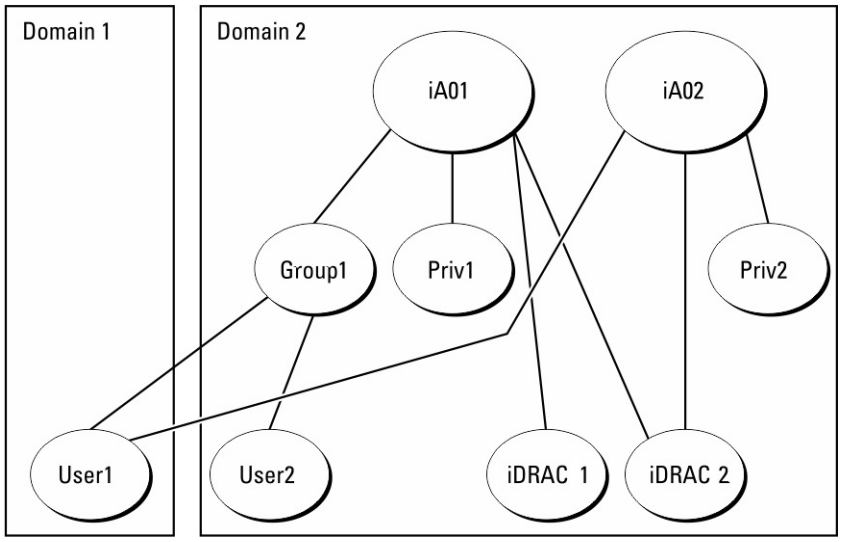


Ilustración 3. Acumulación de privilegios para un usuario

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 dispone de los privilegios Priv1 y Priv2 en iDRAC2. Usuario1 dispone de privilegios Priv1 solo en iDRAC1. Usuario2 dispone de privilegios Priv1 en iDRAC1 e 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 privilegios y objetos de asociación de ejemplo al esquema de Active Directory. Antes de extender el esquema, asegúrese de tener los privilegios de administrador de esquemas en el maestro de esquema FSMO-Role-Owner (FSMO-Función-Propietario) en el bosque de dominio.

NOTA: La extensión del esquema de este producto es distinta de la de generaciones anteriores. 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 usa 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 habrá extendido. Para verificar la extensión del esquema, utilice la MMC y el complemento de esquema de Active Directory a fin de comprobar que Clases y atributos en la página 166 exista. Consulte la documentación de Microsoft para obtener detalles acerca del uso de la MMC y el complemento de esquema de Active Directory.

Clases y atributos

Tabla 25. 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 26. Clase DelliDRACdevice

OID	1.2.840.113556.1.8000.1280.1.7.1.1
Descripción	Representa el dispositivo iDRAC de Dell. La iDRAC debe configurarse como delliDRACDevice en Active Directory. Esta configuración permite que la iDRAC envíe solicitudes de protocolo ligero de acceso a directorios (LDAP) a Active Directory.
Tipo de clase	Clase estructural
SuperClasses	dellProduct
Atributos	dellSchemaVersion dellRacType

Tabla 27. Clase delliDRACAssociationObject

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

Tabla 28. 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

Tabla 28. Clase dellRAC4Privileges (continuación)

OID	1.2.840.113556.1.8000.1280.1.1.1.3
SuperClasses	Ninguno
Atributos	dellIsLoginUser dellIsCardConfigAdmin dellIsUserConfigAdmin dellIsLogClearAdmin dellIsServerResetUser dellIsConsoleRedirectUser dellIsVirtualMediaUser dellIsTestAlertUser dellIsDebugCommandAdmin

Tabla 29. Clase dellPrivileges

OID	1.2.840.113556.1.8000.1280.1.1.1.4
Descripción	Esta clase se usa como una clase de contenedor para los privilegios de Dell (derechos de autorización).
Tipo de clase	Clase estructural
SuperClasses	Usuario
Atributos	dellRAC4Privileges

Tabla 30. 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 31. Lista de atributos agregados al esquema de Active Directory

Nombre del atributo/Descripción	OID asignado/Identificador de objeto de sintaxis	Con un solo valor
dellPrivilegeMember Lista de los objetos dellPrivilege que pertenecen a este atributo.	1.2.840.113556.1.8000.1280.1.1.2.1 Nombre distintivo (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSO
dellProductMembers Lista de los objetos dellRacDevice y DelliDRACDevice que pertenecen a esta función. Este atributo es el enlace de avance al enlace de retroceso dellAssociationMembers.	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

Tabla 31. Lista de atributos agregados al esquema de Active Directory (continuación)

Nombre del atributo/Descripción	OID asignado/Identificador de objeto de sintaxis	Con un solo valor
Identificación de vínculo: 12070		
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 TRUE si el usuario tiene derechos de restablecimiento de servidor en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.7 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	VERDADERO
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	1.2.840.113556.1.8000.1280.1.1.2.13 Cadena de no distinguir mayúsculas de minúsculas	VERDADERO

Tabla 31. Lista de atributos agregados al esquema de Active Directory (continuación)

Nombre del atributo/Descripción	OID asignado/Identificador de objeto de sintaxis	Con un solo valor
delliDRACDevice y el vínculo de retroceso al vínculo de avance de dellAssociationObjectMembers.	(LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	
dellAssociationMembers Lista de los objetos dellAssociationObjectMembers que pertenecen a este producto. Este atributo es el enlace 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 de Systems Management con el DVD *Dell Systems Management Tools and Documentation (Herramientas y documentación de Dell Systems Management)*, podrá extender el complemento al seleccionar la opción **Active Directory Users and Computers Snap-in (Complemento Usuarios y computadoras de Active Directory)** durante el procedimiento de instalación. Consulte Dell OpenManage Software Quick Installation Guide (Guía de instalación rápida del software de Dell OpenManage) para obtener instrucciones adicionales acerca de la instalación del software de administración de sistemas. Para los sistemas operativos Windows de 64 bits, el instalador del complemento se encuentra en el siguiente directorio:

<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 Active Directory Users and Computers Snap-in (Complemento Usuarios y computadoras de Active Directory) de Dell, puede agregar usuarios y privilegios de iDRAC mediante la creación de objetos de dispositivo, asociación y privilegio. 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 de ADSI**. Aparecerá la ventana **ADSI Edit (Editor de 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 en **Check Names (Verificar nombres)** y luego en **OK (Aceptar)**. Los usuarios autentificados 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 acerca de las cuentas de usuario y los servidores de Active Directory (AD). Además, especifique el tiempo que iDRAC debe esperar las respuestas de AD durante el proceso de inicio de sesión.

   NOTA:
   - Si la validación de certificados está activada, 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 del 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 la opción Extended Schema (Esquema extendido), son las direcciones IP o FQDN de las controladoras de dominio donde se ubica 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 la validación de certificados está activada, 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)**.

     El siguiente comando de RACADM es opcional:

     ```
     racadm sslcertdownload -t 1 -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 Directory 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 (Probar)**.
   Aparecerá la página **Test Active Directory Settings (Probar configuración de Active Directory)**.
2. Haga clic en **Prueba**.
3. Introduzca un nombre de usuario de prueba (por ejemplo, **nombredeusuario@dominio.com**) y la contraseña, y haga clic en **Start Test (Iniciar prueba)**. Aparecerán los resultados detallados 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, iDRAC requiere que se identifique el servidor de Active Directory mediante el FQDN, y no una dirección IP. Si el servidor de Active Directory se identifica mediante una dirección IP, la validación de certificados falla porque 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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

Configuración de los usuarios LDAP genéricos

La iDRAC proporciona una solución genérica para admitir la autenticación basada en el protocolo ligero de acceso a directorios (LDAP). Esta función no requiere ninguna extensión del esquema en los servicios de directorio.

Para hacer que la implementación LDAP de la iDRAC sea genérica, los elementos comunes entre los distintos servicios de directorio se utilizan para agrupar usuarios y, luego, asignar la relación usuario-grupo. La acción específica del servicio de directorio es el esquema. Por ejemplo, puede haber nombres de atributo diferentes para el grupo, el usuario y el vínculo entre el usuario y el grupo. Estas acciones se configuran en la 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 la iDRAC, vaya a **iDRAC Settings (Configuración de la iDRAC)** > **Users (Usuarios)** > **Directory Services (Servicios de directorio)** > **Generic LDAP Directory Service (Servicio de directorio de LDAP genérico)** y haga clic en **Edit (Editar)**.
   En la página **Generic LDAP Configuration and Management Step 1 of 3 (Configuración y administración de LDAP genérico, paso 1 de 3)**, figura 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 SSL. Solo se admite LDAP mediante 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 habilitado la validación de certificados, especifique el FQDN del servidor LDAP y asegúrese de que el DNS se haya configurado correctamente en **iDRAC Settings (Configuración de la iDRAC)** > **Network (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, se admite solamente 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 de grupo de roles. En la página **Generic LDAP Configuration and Management Step 3a of 3 (Paso 3a de 3 de Configuración y administración de LDAP genérico)**, aparece dicha configuración.
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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.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 la iDRAC, vaya a **iDRAC Settings (Configuración de la iDRAC)** > **Users (Usuarios)** > **Directory Services (Servicios de directorio)** > **Generic LDAP Directory Service (Servicio de directorio de 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 de la opción utilizada para *Attribute of User Login* (*Atributo de inicio de sesión del usuario)* 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 la opción **Enable Certificate Validation (Activar la validación de certificados)** seleccionada, la iDRAC requiere que el FQDN (y no una dirección IP) identifique el servidor de LDAP. Si al servidor de LDAP lo identifica una dirección IP, fallará la validación del certificado, porque la iDRAC no puede comunicarse con el servidor LDAP.

   NOTA: Cuando está habilitada la opción de LDAP genérico, la iDRAC primero intenta iniciar la sesión del usuario como un usuario de directorio. Si ocurre un error, 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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

10

Modo de bloqueo de la configuración del sistema

El modo de bloqueo de la configuración del sistema permite evitar cambios accidentales después del aprovisionamiento de un sistema. El modo de bloqueo puede aplicarse a la configuración y a las actualizaciones de firmware. Cuando el sistema está bloqueado, se impide cualquier intento de cambio de la configuración del sistema. Si se intenta cambiar la configuración vital del sistema, se mostrará un mensaje de error. Habilitar el modo de bloqueo del sistema bloquea la actualización del firmware de las tarjetas I/O de terceros utilizando las herramientas del proveedor.

El modo de bloqueo del sistema solo está disponible para los clientes con licencia de la empresa.

En la versión 4.40.00.00, la funcionalidad de bloqueo del sistema se extiende también a los NIC.

NOTA: El bloqueo mejorado para los NIC solo incluye el bloqueo del firmware para evitar las actualizaciones. El bloqueo de la configuración (x-UEFI) no es compatible.

NOTA: Después de activar el modo de bloqueo del sistema, los usuarios no pueden cambiar los valores de configuración. Los campos de configuración del sistema están desactivados.

Se puede activar o desactivar el modo de bloqueo mediante el uso de las siguientes interfaces:

- Interfaz web del iDRAC
- RACADM
- WSMan
- SCP (perfil de configuración del sistema)
- Redfish
- Si presiona F2 durante la POST y selecciona configuración de iDRAC
- Borrado del sistema de fábrica

NOTA: Para habilitar el modo de bloqueo, debe tener la licencia de iDRAC Enterprise o Datacenter y privilegios de control y configuración del sistema.

NOTA: Es posible que pueda acceder a vMedia con el sistema en modo de bloqueo, pero la configuración de recursos compartidos de archivos remotos no está activada.

NOTA: Las interfaces como OMSA, SysCfg y USC solo pueden comprobar la configuración, pero no pueden modificarla.

En la siguiente tabla se indican las características funcionales y no funcionales, las interfaces y las utilidades que se ven afectadas por el modo de bloqueo:

NOTA: No se admite el cambio del orden de arranque con iDRAC cuando el modo de bloqueo está activado. Sin embargo, la opción de control de arranque está disponible en el menú de vConsole, el cual no surte efecto cuando iDRAC está en modo de bloqueo.

Tabla 32. Elementos afectados por el modo de bloqueo

Desactivado	Permanece funcional
• Eliminación de licencias • Actualizaciones de DUP • Importación de SCP • Restablecer a los valores predeterminados • OMSA/OMSS • IPMI • DRAC/LC • DTK-Syscfg • Redfish • OpenManage Essentials	• Operaciones de alimentación: encendido/apagado, restablecimiento • Configuración del límite de alimentación • Prioridad de alimentación • Identificación de dispositivos (chasis o PERC) • Sustitución de piezas, restauración sencilla y sustitución de la placa base • Ejecución de diagnósticos • Operaciones modulares (FlexAddress o dirección asignada de forma remota)

Tabla 32. Elementos afectados por el modo de bloqueo

Desactivado	Permanece funcional

• BIOS (la configuración de F2 es de solo lectura)
• Administrador de grupo
• Seleccionar tarjetas de red
	• Código de acceso de Administrador de grupo
	• Todas las herramientas de proveedores que tengan acceso directo al dispositivo (excluye los NIC seleccionados)
	• Exportación de licencias
	• PERC
	  ○ CLI de PERC
	  ○ DTK-RAIDCFG
	  ○ F2/Ctrl+R
	• Todas las herramientas de proveedores que tengan acceso directo al dispositivo
	• NVMe
	  ○ DTK-RAIDCFG
	  ○ F2/Ctrl+R
	• BOSS-S1
	  ○ Marvell CLI
	  ○ F2/Ctrl+R
	• Configuración de ISM/OMSA (habilitación de BMC del sistema operativo, comando ping al guardián, nombre del sistema operativo, versión del sistema operativo)

NOTA: Cuando el modo de bloqueo está activado, la opción de inicio de sesión de OpenID Connect no se muestra en la página de inicio de sesión de iDRAC.

11

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 es compatible con la autenticación de Active Directory basada en Kerberos para admitir inicios de sesión de tarjetas inteligentes y SSO. Para obtener información acerca de 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 la iDRAC con la hora de la controladora de dominio de Active Directory. Si no lo hace, la autenticación de Kerberos en la iDRAC no funcionará. Es posible usar la zona horaria y la función de NTP para sincronizar la hora. Para hacerlo, consulte Configuración de zona horaria y NTP en la página 108.
- Registre el iDRAC como equipo en el dominio raíz de Active Directory.
- Genere un archivo keytab mediante la herramienta ktpass.
- Para habilitar el inicio de sesión único para el esquema extendido, asegúrese de que la opción **Trust this user for delegation to any service (Kerberos only) (Confiar en este usuario para la delegación a cualquier servicio [solo Kerberos])** esté activada en la ficha **Delegation (Delegación)** del usuario keytab. Esta ficha 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 navegador para que admita el inicio de sesión SSO. Para obtener más información, consulte Inicio de sesión único en la página 376.

  NOTA: Google Chrome y Safari no admiten Active Directory para realizar el inicio de sesión SSO.

Registro de iDRAC en el sistema de nombre de dominio

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 **Ajustes de IPv4** o **Ajustes de IPv6** basado en los ajustes de la IP.
3. Proporcione una dirección IP válida del **Servidor DNS preferido/alternativo**. Este valor es una dirección IP válida del 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*.

Creación de objetos de Active Directory y establecimiento de privilegios

Inicio de sesión en SSO basado en el esquema estándar de Active Directory

Realice los pasos a continuación para el inicio de sesión SSO basado en el esquema estándar de Active Directory:
1. Cree un grupo de usuarios.
2. Cree un usuario para el esquema estándar.

NOTA: Utilice el grupo de usuarios y el usuario de AD existentes.

Inicio de sesión en SSO basado en el esquema extendido de Active Directory

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.
   NOTA: Es recomendable no proporcionar privilegios de administrador, ya que esto podría omitir algunas comprobaciones de seguridad.
3. Asocie el objeto de dispositivo y el objeto de privilegio con el objeto de asociación.
4. Agregue el usuario de SSO (usuario con acceso) anterior al objeto de dispositivo.
5. Proporcione privilegio de acceso a *Usuarios autentificados* para acceder al objeto de asociación creado.

Inicio de sesión en SSO de Active Directory

Realice los pasos a continuación para el inicio de sesión en SSO de Active Directory:
1. Cree un usuario keytab de Kerberos que se utiliza para la creación del archivo keytab.

NOTA: Cree una clave nueva de KERBROS para cada IP de iDRAC.

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.

Creación de un usuario en Active Directory para SSO

Realice los siguientes pasos para crear un usuario en Active Directory para SSO:

1. Cree un nuevo usuario en la unidad organizacional.
2. Vaya a **Usuario de Kerberos>Propiedades>Cuenta>Utilizar tipos de cifrado AES de Kerberos para esta cuenta**

3. Utilice el siguiente comando para generar un archivo keytab de Kerberos en el servidor de Active Directory:

```
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
```

Observe el esquema extendido

- Cambie la configuración de delegación del usuario de Kerberos.
- Vaya a **Usuario de Kerberos>Propiedades>Delegación>Confiar en este usuario para la delegación a cualquier servicio (solo para Kerberos)**

NOTA: Cierre la sesión y vuelva a iniciar sesión desde la estación de administración del usuario de Active Directory después de cambiar la configuración anterior.

Generación del archivo Keytab de Kerberos

Para admitir SSO y la autentificación de inicio de sesión mediante tarjeta inteligente, iDRAC es compatible con la configuración para activarse a sí mismo como un servicio de kerberos en una red Kerberos de Windows. La configuración de Kerberos en iDRAC implica los mismos pasos que la configuración de un servicio de Kerberos de servidor que no es de Windows como un elemento principal de seguridad en Active Directory del servidor de Windows.

La herramienta *ktpass* (disponible en Microsoft como parte del CD/DVD de instalación del servidor) se utiliza para crear las vinculaciones de nombre principal de servicio (SPN) con una cuenta de usuario y exportar la información de confianza a un archivo *keytab* de Kerberos tipo MIT, que permite una relación de confianza entre un usuario o un sistema externos y el centro de distribución de claves (KDC). El archivo keytab contiene una clave criptográfica, que se utiliza para cifrar la información entre el servidor y el KDC. La herramienta ktpass permite servicios basados en UNIX que admiten la autenticación Kerberos para usar las funciones de interoperabilidad proporcionadas por un servicio KDC Kerberos del servidor Windows. 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 utilizar con la opción **-usuariodemapa** del comando `ktpass`. Además, debe tener el mismo nombre DNS de iDRAC en el cual carga el archivo keytab generado.

Para generar un archivo keytab mediante la herramienta ktpass:

1. Ejecute la utilidad *ktpass* en la controladora de dominio (servidor de Active Directory) donde desee asignar el iDRAC a una cuenta de usuario en Active Directory.
2. Utilice el comando ktpass siguiente para crear el archivo keytab de Kerberos:

```
C:\> ktpass.exe -princ HTTP/idrac7name.domainname.com@DOMAINNAME.COM -mapuser
DOMAINNAME\username -mapop set -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass
[password] -out c:\krbkeytab
```

El tipo de cifrado es AES256-SHA1. El tipo principal es KRB5_NT_PRINCIPAL. Las propiedades de la cuenta de usuario a la que se asigna el nombre principal del servicio debe tener activada la propiedad **Utilizar tipos de cifrado AES 256 para esta cuenta**.

NOTA: Utilice letras minúsculas para el **Nombre de iDRAC** y el **Nombre principal del servicio**. Utilice letras mayúsculas para el nombre del dominio, como se muestra en el ejemplo.

Se genera un nuevo archivo keytab.

NOTA: Si encuentra algún problema con el usuario de iDRAC para el cual creó el archivo keytab, cree un nuevo usuario y un nuevo archivo keytab. Si vuelve a ejecutar el mismo archivo keytab que creó inicialmente, no se configura correctamente.

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 calificado de iDRAC. Para ello, en la interfaz web de iDRAC, vaya a **Configuración de iDRAC** > **Red** > **Configuración común** 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 software de administración

Realice los siguientes pasos después de configurar el inicio de sesión SSO para usuarios de Active Directory:

1. Establezca la IP del servidor DNS en las propiedades de Red y mencione la dirección IP preferida del servidor DNS.
2. Vaya a Mi computadora y agregue el dominio ***domain.tld**.
3. Agregue el usuario de Active Directory como administrador. Para ello, vaya a: **Mi PC** > **Administrar** > **Usuario local y grupos** > **Grupos** > **Administrador** y agregue el usuario de Active Directory.
4. Cierre sesión en el sistema e inicie sesión nuevamente con la credencial de usuario de Active Directory.
5. En la configuración de Internet Explorer, agregue el dominio *domain.tld como se muestra a continuación:
   a. Vaya a **Herramientas** > **Opciones de Internet** > **Seguridad** > **Internet local** > **Sitios** y desmarque la selección **Detectar automáticamente la configuración de red de intranet**. Seleccione las tres opciones restantes y haga clic en **Avanzado** para agregar *domain.tld.
   b. Abra una ventana nueva en Internet Explorer y use el nombre de host de iDRAC para iniciar la GUI de la iDRAC.
6. En la configuración de Mozilla Firefox, agregue el dominio *domain.tld:
   - Inicie el explorador Firefox y escriba about:config en la URL.
   - Escriba “negotiate” en el cuadro de texto de filtro. Haga doble clic en el resultado que se compone de *auth.trusted.uris*. Escriba el dominio, guarde la configuración y cierre el explorador.
   - Abra una ventana nueva en Firefox y use el nombre de host de iDRAC para iniciar la GUI de la 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 por tarjeta inteligente está activado, se deshabilitan SSH, IPMI en LAN, Serie en LAN y RACADM remoto. Nuevamente, si desactiva el inicio de sesión por 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 la iDRAC, vaya a **iDRAC Settings (Configuración de la iDRAC)** > **Users (Usuarios)** > **Smart Card (Tarjeta inteligente)**.
   Se muestra la página **Tarjeta inteligente**.
2. En el menú desplegable **Configure Smart Card Logon (Configurar inicio de sesión mediante tarjeta inteligente)**, seleccione **Enabled (Habilitado)** para activar el inicio de sesión mediante tarjeta inteligente o seleccione **Enabled With Remote RACADM (Habilitado 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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.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 **Enabled (Habilitado)** 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 la iDRAC*.
3. Haga clic en **Atrás**, en **Terminar** y, a continuación, en **Sí**.
   La función de inicio de sesión mediante tarjeta inteligente se activa o desactiva según la opción seleccionada.

Configuración de inicio de sesión con la tarjeta inteligente

NOTA: Para configurar la tarjeta inteligente en Active Directory, iDRAC debe configurarse con un inicio de sesión SSO estándar o con esquema extendido.

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*.

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 con la tarjeta inteligente requiere la configuración del certificado de usuario local o de Active Directory.

2. En **Configurar Inicio de sesión mediante tarjeta inteligente**, seleccione **Activado con RACADM remoto** para habilitar la configuración.
3. Establezca la opción para **Activar la revisión CRL para el Inicio de sesión mediante 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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

Cómo solicitar el certificado para la inscripción de la tarjeta inteligente

Siga estos pasos para solicitar el certificado para inscripción de tarjeta inteligente:

1. Conecte la tarjeta inteligente en el sistema cliente e instale los controladores y software necesarios.
2. Compruebe el estado del controlador en el Administrador de dispositivos.
3. Inicie el agente de inscripción de la tarjeta inteligente en el explorador.
4. Ingrese el **Nombre de usuario** y la **Contraseña**, y haga clic en **Aceptar**.
5. Haga clic en **Solicitar certificado**.
6. Haga clic en **Solicitar certificado avanzado**.
7. Haga clic en **Solicitar un certificado** para una tarjeta inteligente en nombre de otro usuario desde la estación de inscripción del certificado de la tarjeta inteligente.
8. Haga clic en el botón **Seleccionar usuario** para seleccionar el usuario que desea inscribir.
9. Haga clic en **Inscribirse** e ingrese la credencial de la tarjeta inteligente.
10. Ingrese el PIN de la tarjeta inteligente y haga clic en **Enviar**.

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 la iDRAC, vaya a **iDRAC Settings (Configuración de la iDRAC)** > **Network (Red)** > **User Authentication (Autenticación de usuario)** > **Local Users (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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

Inicio de sesión mediante la tarjeta inteligente

NOTA: El inicio de sesión mediante la tarjeta inteligente solo se admite en Internet Explorer.

Realice lo siguiente para el inicio de sesión con una tarjeta inteligente:

1. Cierre sesión desde la GUI de la iDRAC después de habilitar la tarjeta inteligente.
2. Inicie la iDRAC por medio de `http://IP/` o de FQDN `http://FQDN/`
3. Haga clic en **Instalar** después de descargar el complemento de la tarjeta inteligente.
4. Ingrese el PIN de la tarjeta inteligente y haga clic en **Enviar**.
5. iDRAC iniciará sesión correctamente con una tarjeta inteligente.

12

Configuración de iDRAC para enviar alertas

Es posible configurar alertas y acciones para determinados eventos 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 evento coincide con un filtro de eventos y ha configurado este filtro para que genere una alerta (correo electrónico, excepción de SNMP, alerta de IPMI, registros del sistema remoto, evento de Redfish o eventos de WS), se enviará una alerta a uno o más destinos configurados. Si el mismo filtro de eventos está configurado para ejecutar una acción (como reiniciar, ejecutar un ciclo de encendido o apagar el sistema), la acción se ejecutará. 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 evento, deberá habilitar la opción de alertas globales. Esta propiedad prevalece sobre las alertas individuales o las acciones de eventos 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 alertas**. Aparecerá la página **Alertas**.
2. En la sección **Alertas**, realice lo siguiente:
   - Seleccione **Activar** para activar la generación de alertas o realizar una acción de suceso.
   - Seleccione **Desactivar** para desactivar la generación de alertas o realizar una acción de suceso.
3. Haga clic en **Aplicar** para guardar la configuración.

Configuración de alerta rápida

Realice lo siguiente para configurar alertas en grandes cantidades:

1. Vaya a **Configuración de alerta rápida** en la página **Configuración de alertas**.
2. Realice lo siguiente en la sección **Configuración de alerta rápida**:
   - Seleccione la categoría de la alerta.
   - Seleccione la notificación de gravedad del problema.
   - Seleccione la ubicación en la que desea recibir estas notificaciones.
3. Haga clic en **Aplicar** para guardar la configuración.

NOTA: Debe seleccionar al menos un tipo de categoría, gravedad y destino para aplicar la configuración.

Todas las alertas configuradas se muestran en **Resumen de configuración de alertas**.

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 (Eventos de plataforma)**, seleccione **Enabled (Habilitado)** para activar la generación de alertas o acciones de eventos. De lo contrario, seleccione **Desactivado**. Para obtener más información acerca de las opciones, consulte la *Ayuda en línea de la utilidad de configuración de la 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 la iDRAC, vaya a **Configuration (Configuración)** > **System Settings (Configuración del sistema)** > **Alerts and Remote System Log Configuration (Configuración de alertas y registros del sistema remoto)**.
2. En la sección **Alerts and Remote System Log Configuration (Configuración de alertas y registros del sistema remoto)**, seleccione **Filter (Filtro)**:
   - System Health (Estado del sistema): Esta categoría representa todas las alertas que están relacionadas con en el hardware dentro del chasis del sistema. Algunos ejemplos incluyen errores de temperatura, errores de voltaje y errores de dispositivo.
   - Storage Health (Estado del almacenamiento): Esta categoría representa las alertas que están relacionadas con el subsistema de almacenamiento. Algunos ejemplos incluyen errores de la controladora, errores de discos físicos y errores de discos virtuales.
   - Configuration (Configuración): Esta categoría representa las alertas que están relacionadas con los cambios de configuración de hardware, firmware y software. Algunos ejemplos incluyen la incorporación o eliminación de tarjetas PCIe, cambios en la configuración de RAID y cambios en la licencia de la iDRAC.

- Audit (Auditoría): Esta categoría representa el registro de auditoría. Algunos ejemplos incluyen la información de inicio/cierre de sesión del usuario, errores de autenticación de contraseña, información sobre la sesión y estados de la alimentación.
- Updates (Actualizaciones): Esta categoría representa las alertas que se generan debido a actualizaciones o degradaciones de firmware o drivers.

  NOTA: 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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.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 o los parámetros de registro del sistema remoto.
2. En la interfaz web de la iDRAC, vaya a **Configuración** > **Configuración del sistema** > **Configuración de alertas y del registro del sistema remoto**.
3. En **Categoría**, seleccione una o todas de las siguientes alertas para los sucesos necesarios:
   - Correo electrónico
   - Captura SNMP
   - Alerta IPMI
   - Registro del sistema remoto
   - eventos 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**, ingrese la identificación de mensaje para probar si se generó la alerta y haga clic en **Probar**. Para obtener más información sobre la comprobación de los mensajes de eventos y error generados por el firmware del sistema y los agentes que supervisan los componentes del sistema, consulte la *Guía de referencia de mensajes de errores y eventos de Dell* en iDRACmanuals

Configuración de alertas de suceso mediante RACADM

Para establecer alertas de suceso, utilice el comando **eventfilters**. Para obtener más información, consulte *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

Configuración de suceso de periodicidad de alertas

Es posible configurar la iDRAC para generar eventos 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 no está habilitada la periodicidad de eventos.

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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.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 la iDRAC, vaya a **Configuration (Configuración)** > **System Settings (Configuración del sistema)** > **Alert Recurrence (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 la iDRAC, vaya a **Configuration (Configuración)** > **System Settings (Configuración del sistema)** > **Alert and Remote System Log Configuration (Configuración de alertas y registros del sistema remoto)**.
2. En el menú desplegable **Actions (Acciones)**, seleccione una acción para cada evento:
   - 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 acciones del suceso, utilice el comando `eventfilters`. Para obtener más información, consulte *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

Configuración de alertas por correo electrónico, capturas SNMP o capturas IPMI

La estación de administración utiliza excepciones de SNMP (Simple Network Management Protocol [Protocolo simple de administración de red]) y de interfaz de administración de plataforma inteligente (IPMI) para recibir datos de la iDRAC. Para los sistemas con una gran cantidad 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 excepciones de evento pueden ayudar a una estación de administración con el equilibrio de carga entre nodos o emitir una alerta si se produce un error de autenticación. Se admiten los formatos de SNMP v1, v2 y v3.

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 enviarle las excepciones de SNMP.

Antes de configurar los valores de correo electrónico o capturas SNMP/IPMI, asegúrese de lo siguiente:

- Dispone de permisos Configurar el RAC.
- Ha configurado los filtros de sucesos.

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 valores de MIB de iDRAC necesarios para supervisar los servidores por medio de SNMP, consulte *Guía de referencia de SNMP para Dell EMC OpenManage* disponible en https://www.dell.com/openmanagemanuals.

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 la iDRAC, vaya a **Configuration (Configuración)** > **System Settings (Configuración del sistema)** > **SNMP and E-mail Settings (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 **SNMP Trap Format (Formato de excepción de SNMP)** se aplica solo a excepciones de SNMP, y no de IPMI. Las excepciones de IPMI siempre se envían en formato SNMP v1 y no están basadas en la opción **SNMP Trap Format (Formato de excepción de 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 de 1 a 8.
<n>=0 **<n>**=1	Desactivar la captura 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 de 1 a 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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.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) usando la utilidad de configuración de la iDRAC. Para hacerlo:

1. En la **utilidad de configuración de iDRAC**, vaya a **Alertas**.
   Aparece la pantalla **Alertas de configuración de iDRAC**.
2. En **Trap Settings (Valores de excepción)**, habilite las direcciones IP para recibir las excepciones e introduzca las direcciones de destino IPv4, IPv6 o FQDN. Es posible 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 del remitente y la dirección de correo electrónico del receptor (destino) para recibir las alertas de correo electrónico. Además, configure la dirección del servidor SMTP.

NOTA: Las alertas por correo electrónico son compatibles con las direcciones IPv4 e IPv6. Se debe especificar el nombre de dominio del DNS de iDRAC cuando se utiliza IPv6.

NOTA: Si está utilizando un servidor de SMTP externo, asegúrese de que iDRAC pueda comunicarse con ese servidor. Si no se puede acceder al servidor, se muestra el error RAC0225 mientras se intenta enviar un correo de prueba.

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. Digite una dirección válida de correo electrónico.
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 de SMTP (correo electrónico), proporcione los siguientes detalles:
   - Dirección IP de servidores de correo electrónico SMTP o nombre de FQDN o DNS
   - Dirección personalizada del remitente: este campo tiene las siguientes opciones:
     - **Predeterminado:** el campo de la dirección no se puede editar
     - **Personalizado:** puede ingresar la ID de correo electrónico en la cual puede recibir las alertas de correo electrónico
   - Mensaje personalizado del prefijo de asunto: este campo tiene las siguientes opciones:
     - **Predeterminado:** el mensaje predeterminado no se puede editar
     - **Personalizado:** puede elegir el mensaje que desea que aparezca en la línea del **Asunto** del correo electrónico
   - Número de puerto SMPT: la conexión se puede cifrar y los correos electrónicos se pueden enviar a través de puertos seguros:
     - **Sin cifrado:** puerto 25 (predeterminado)
     - **SSL**: puerto 465
   - Cifrado de la conexión: cuando no tiene un servidor de correo electrónico en el establecimiento, puede usar servidores de correo electrónico basados en la nube o retransmisores SMTP. Para configurar el servidor de correo electrónico en la nube, puede establecer esta función en cualquiera de los siguientes valores de la lista desplegable:
     - **Ninguno:** sin cifrado en la conexión con el servidor SMTP. Este es el valor predeterminado.
     - **SSL**: ejecuta el protocolo SMTP a través de SSL

     NOTA:
     - Esta función no se puede configurar mediante el Administrador de grupo.
     - Esta es una función con licencia y no está disponible con la licencia básica de iDRAC.
     - Debe tener el privilegio Configurar iDrac para usar esta función.
   - Autenticación
   - Nombre de usuario

   Para la configuración del servidor, el uso de los puertos depende de `connectionencryptiontype` y esto se puede configurar únicamente con RACADM.
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 de correo electrónico. Los valores permitidos son de 1 a 4.
n=0 **n=1**	Inhabilita las alertas de correo electrónico. 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 de correo electrónico. Los valores permitidos son de 1 a 4.
email-address	Dirección de correo electrónico de destino que recibe las alertas de eventos de la plataforma.

3. Para configurar los valores de correo electrónico del remitente:

```
racadm set iDRAC.RemoteHosts.[index] [email-address]
```

Parámetro	Descripción
index	Índice de correo electrónico del remitente.
email-address	Dirección de correo electrónico del remitente que envía las alertas de eventos de la plataforma.

4. Para configurar un mensaje personalizado:

```
racadm set iDRAC.EmailAlert.CustomMsg.[index] [custom-message]
```

Parámetro	Descripción
index	Índice de destino de correo electrónico. Los valores permitidos son de 1 a 4.
custom-message	Mensaje personalizado

5. 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 desea probar. Los valores permitidos son de 1 a 4.

Para obtener más información, consulte *Guía de la CLI de RACADM para iDRAC* disponible en https://www.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 la iDRAC, vaya a **Configuration (Configuración)** > **System Settings (Configuración del sistema)** > **Alert Configuration (Configuración de alertas)** > **SNMP (E-mail Configuration) (Configuración de SNMP 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 eventos de WS se utiliza para que un servicio cliente (suscriptor) registre el interés (suscripción) en un servidor (origen de eventos) para recibir mensajes que contienen los eventos del servidor (notificaciones o mensajes de eventos). Los clientes interesados en recibir los mensajes de eventos de WS pueden suscribirse en la iDRAC y recibir eventos relacionados con trabajos de Lifecycle Controller.

Los pasos necesarios para configurar la función de eventos de WS a fin de recibir mensajes de eventos de WS para los cambios relacionados con los trabajos de Lifecycle Controller se describen en el documento de especificaciones sobre compatibilidad con eventos del servicio web de iDRAC 1.30.30. Además de esta especificación, consulte la sección 10 sobre Notificaciones (eventos) del documento DSP0226 (Especificación de administración de WS DMTF) para obtener la información completa sobre el protocolo de eventos de WS. Los trabajos relacionados con Lifecycle Controller se describen en el documento de perfiles de control de trabajos de DCIM.

Configuración de sucesos de Redfish

El protocolo de eventos de Redfish se utiliza para que un servicio cliente (suscriptor) registre el interés (suscripción) en un servidor (origen de eventos) para recibir mensajes que contienen los eventos de Redfish (notificaciones o mensajes de eventos). Los clientes interesados en recibir los mensajes de eventos de Redfish pueden suscribirse en la iDRAC y recibir eventos relacionados con trabajos de Lifecycle Controller.

Supervisión de sucesos del chasis

En el chasis PowerEdge FX2/FX2s, puede activar el ajuste de **Administración y monitoreo del chasis** en la iDRAC para realizar tareas de administración y monitoreo del chasis, como la supervisión de los componentes del chasis, la configuración

de alertas, el uso de RACADM en la iDRAC para transmitir comandos RACADM de la CMC, y la actualización del firmware de administración del chasis. Este ajuste le permite administrar los servidores en el chasis, incluso si la CMC no está en la red. Puede configurar el valor en **Desactivado** para reenviar los eventos del chasis. De manera predeterminada, esta opción está establecida en **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 monitoreo del chasis** está establecida en **Activado**, la iDRAC genera y registra los eventos del chasis. Los eventos generados se integran en el subsistema de eventos de la iDRAC y las alertas se generan de manera similar al resto de los eventos.

La CMC también reenvía los eventos generados a la iDRAC. En caso de que la iDRAC en el servidor no funcione, la CMC pone en línea de espera los primeros 16 eventos y registra el resto en el registro de la CMC. Estos 16 eventos se envían a la iDRAC tan pronto como el **Monitoreo del chasis** se establece en Activado.

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.

NOTA: iDRAC no es compatible con los siguientes atributos del chasis:

- `ChassisBoardPartNumber`
- `ChassisBoardSerialNumber`

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 la iDRAC, haga clic en **Overview (Descripción general)** > **iDRAC Settings (Configuración de la 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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.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 33. Id. de mensaje de alertas

Id. de mensaje	Descripción	Descripción (para plataformas MX)
AMP	Amperaje	Amperaje

Tabla 33. Id. de mensaje de alertas (continuación)

Id. de mensaje	Descripción	Descripción (para plataformas MX)
ASR	Restablecimiento automático del sistema	Restablecimiento automático del sistema
BAT	Suceso de la batería	Suceso de la batería
BIOS	Administración del BIOS	Administración del BIOS
Arranque	Control de arranque	Control de arranque
CBL	Cable	Cable
CPU	Procesador	Procesador
CPUA	Procesador ausente	Procesador ausente
CTL	Controladora de almacenamiento	Controladora de almacenamiento
DH	Administración de certificados	Administración de certificados
DIS	Descubrimiento automático	Descubrimiento automático
ENC	Gabinete de almacenamiento	Gabinete de almacenamiento
FAN	Suceso de ventilador	Suceso de ventilador
FSD	Depuración	Depuración
HWC	Configuración de hardware	Configuración de hardware
IPA	Cambio de IP de DRAC	Cambio de IP de DRAC
ITR	Intrusión	Intrusión
JCP	Control de trabajos	Control de trabajos
LC	Lifecycle Controller	Lifecycle Controller
LIC	Licencias	Licencias
LNK	Estado de vínculo	Estado de vínculo
LOG	Registrar evento	Registrar evento
MEM	Memoria	Memoria
NDR	Controlador de NIC de SO	Controlador de NIC de SO
NIC	Configuración de NIC	Configuración de NIC
OSD	Implementación de SO	Implementación de SO
OSE	Evento de SO	Evento de SO
PCI	Dispositivo PCI	Dispositivo PCI
PDR	Disco físico	Disco físico

Tabla 33. Id. de mensaje de alertas (continuación)

Id. de mensaje	Descripción	Descripción (para plataformas MX)
PR	Intercambio de piezas	Intercambio de piezas
PST	POST del BIOS	POST del BIOS
PSU	Fuente de alimentación	Fuente de alimentación
PSUA	PSU ausente	PSU ausente
PWR	Uso de alimentación	Uso de alimentación
RAC	Suceso RAC	Suceso RAC
RDU	Redundancia	Redundancia
RED	Descarga de firmware	Descarga de firmware
RFL	Medios IDSDM	Medios IDSDM
RFLA	IDSDM ausente	IDSDM ausente
RFM	SD de dirección flexible	No aplicable
RRDU	Redundancia IDSDM	Redundancia IDSDM
RSI	Servicio remoto	Servicio remoto
SEC	Suceso de seguridad	Suceso de seguridad
Registro de sucesos del sistema	Registro de sucesos del sistema	Registro de sucesos del sistema
SRD	RAID de software	RAID de software
SSD	SSD PCIe	SSD PCIe
STOR	Almacenamiento	Almacenamiento
SUP	Trabajo de actualización del firmware	Trabajo de actualización del firmware
SWC	Configuración de software	Configuración de software
SWU	Cambio de software	Cambio de software
SYS	Información del sistema	Información del sistema
TMP	Temperatura	Temperatura
TST	Alerta de prueba	Alerta de prueba
UEFI	Suceso UEFI	Suceso UEFI
USR	Seguimiento del usuario	Seguimiento del usuario
VDR	Disco virtual	Disco virtual
VF	Tarjeta vFlash SD	Tarjeta vFlash SD

Tabla 33. Id. de mensaje de alertas (continuación)

Id. de mensaje	Descripción	Descripción (para plataformas MX)
VFL	Suceso de vFlash	Suceso de vFlash
VFLA	vFlash ausente	vFlash ausente
VLT	Voltaje	Voltaje
VME	Medios virtuales	Medios virtuales
VRM	Consola virtual	Consola virtual
WRK	Nota de trabajo	Nota de trabajo

13

Group Manager de iDRAC 9

Group Manager permite que el usuario tenga una experiencia de consola múltiple y ofrece una administración de iDRAC básica simplificada.

La función Group Manager de iDRAC está disponible para los servidores de 14.ª generación de Dell, a fin de ofrecer administración básica simplificada de las iDRAC y los servidores asociados en la misma red local mediante la GUI de iDRAC. Group Manager permite una experiencia de consola de uno a muchos sin que sea necesaria una aplicación independiente. Permite que los usuarios vean los detalles de un conjunto de servidores mediante la habilitación de una administración más potente que la inspección visual de los servidores para detectar errores y otros métodos manuales.

Group Manager es una función con licencia y forma parte de la licencia Enterprise. Solo los usuarios administradores de iDRAC pueden acceder a la funcionalidad de Group Manager.

NOTA: Para obtener una mejor experiencia del usuario, Group Manager admite hasta 250 nodos de servidor.

Temas:

Group Manager

Para utilizar la función **Group Manager**, debe habilitar **Group Manager** en la página de índice de iDRAC o en la pantalla de bienvenida de Group Manager. La pantalla de bienvenida de Group Manager proporciona opciones que se indican en la siguiente tabla.

Tabla 34. Opciones de Group Manager

Opción	Descripción
Unirse a un grupo existente	Permite unirse a un grupo existente; necesita conocer el **Nombre de grupo** y el **código de acceso** para unirse a un grupo específico. **NOTA:** Las contraseñas están asociadas a las credenciales de usuario de iDRAC. En cambio, un código de acceso está asociado a un grupo para establecer la comunicación de dispositivos autenticados entre diferentes iDRAC en el mismo grupo.
Crear grupo nuevo	Le permite crear un nuevo grupo. El iDRAC específico que ha creado el grupo será el maestro (controladora principal) del grupo.

Tabla 34. Opciones de Group Manager (continuación)

Opción	Descripción
Desactivar Group Manager para este sistema	Puede seleccionar esta opción si no desea unirse a ningún grupo del sistema específico. No obstante, puede acceder a Group Manager en cualquier momento seleccionando Abrir Group Manager desde la página de índice de iDRAC. Cuando deshabilite Group Manager, el usuario tendrá que esperar durante 60 segundos antes de realizar más operaciones en Group Manager.

Una vez que la función Group Manager esté activada, la iDRAC permite crear o unirse a un grupo local de iDRAC. Se puede configurar más de un grupo de iDRAC en la red local, pero una iDRAC individual solo puede ser miembro de un grupo a la vez. Para cambiar de grupo (unirse a un nuevo grupo), en primer lugar, la iDRAC debe abandonar su grupo actual y, a continuación, unirse al grupo nuevo. Se elige a la iDRAC a partir de la cual se creó el grupo como la controladora principal del grupo de forma predeterminada. El usuario no define una controladora principal dedicada de Group Manager para controlar ese grupo. La controladora principal aloja la interfaz Web de Group Manager y proporciona los flujos de trabajo basados en la GUI. Los miembros de la iDRAC autoseleccionan una nueva controladora principal para el grupo si se pierde la conexión con la principal actual durante un período prolongado, pero eso no afecta al usuario final. Por lo general, puede acceder a Group Manager desde todos los miembros de la iDRAC, para lo cual debe hacer clic en Group Manager en la página de índice de iDRAC.

Vista de resumen

Debe tener privilegios de administrador para acceder a las páginas de Group Manager. Si un usuario que no es administrador inicia sesión en la iDRAC, la sección Group Manager no aparece con sus credenciales. En términos generales, la página de inicio de Group Manager (vista de resumen) se clasifica en tres secciones. En la primera sección, figura el resumen de consolidación con detalles sobre sumatorias.

- Cantidad total de servidores en el grupo local.
- Gráfica donde se ve la cantidad de servidores por modelo de servidor.
- Gráfica circular donde se ven los servidores según su estado (si hace clic en una sección de la gráfica, se filtrará la lista de servidores para mostrar solo los servidores con el estado seleccionado).
- Cuadro de advertencia si se detecta un grupo duplicado en la red local. Normalmente, un grupo duplicado es un grupo con el mismo nombre, pero con otro código de acceso. Este cuadro de advertencia no aparece si no hay grupos duplicados.
- Aparecen las iDRAC que controlan el grupo (controladora principal y secundaria).

La segunda sección incluye botones para las acciones que se aplican a todo el grupo y, en la tercera sección, figura la lista de todas las iDRAC en el grupo.

Muestra todos los sistemas en el grupo y su estado actual, y le permite al usuario realizar las acciones correctivas que necesite. Los atributos de servidor específicos de un servidor se describen en la siguiente tabla.

Tabla 35. Atributos del servidor

Atributo del 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.
Etiqueta de servicio	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 hora en que se actualizó por última vez el servidor.

El panel de información del sistema proporciona más detalles sobre el servidor, como el estado de conectividad de red de la iDRAC, el estado de alimentación del host del servidor, el código de servicio rápido, el sistema operativo, la etiqueta de recurso, la id. de nodo, el nombre DNS de la IDRAC, la versión del BIOS del servidor, la información de la CPU del servidor, y la información de memoria y ubicación del sistema. Puede hacer doble clic en una fila o hacer clic en el botón de inicio de la iDRAC para efectuar un redireccionamiento de inicio de sesión único a la página de índice de la iDRAC seleccionada. En el

servidor seleccionado, es posible acceder a la consola virtual o realizar tareas relacionadas con la alimentación del servidor en la lista desplegable More Actions (Más acciones).

Las acciones de grupo compatibles son la administración de los inicios de sesión de los usuarios de la iDRAC, la configuración de alertas y la exportación de inventario de grupo.

Requisitos de configuración de red

Group Manager utiliza redes locales de vínculo IPv6 para comunicarse entre las iDRAC (sin incluir la GUI del navegador Web). La comunicación local de vínculo se define como paquetes no enrutados, lo que significa que cualquier iDRAC separada por un enrutador no se puede unir en un grupo local. Si el puerto dedicado de la iDRAC o la LOM compartida está asignado a una vLAN, la vLAN limita la cantidad de iDRAC que se pueden agrupar (las iDRAC deben estar en la misma vLAN y el tráfico no debe pasar a través de un enrutador).

Cuando Group Manager está habilitado, iDRAC habilita una dirección local de vínculo de IPv6, independientemente de la configuración de red actual definida por el usuario de iDRAC. Group Manager se puede usar cuando iDRAC está configurada para las direcciones IP IPv4 o IPv6.

Group Manager utiliza mDNS para identificar otras iDRAC en la red y envía paquetes cifrados con el fin de realizar el inventario normal, el monitoreo y la administración del grupo mediante la dirección IP local de vínculo. El uso de redes locales de vínculo IPv6 significa que los puertos y los paquetes de Group Manager nunca abandonarán la red local ni estarán disponibles para redes externas.

Los puertos (específicos de la funcionalidad única de Group Manage no incluyen todos los puertos iDRAC) son los siguientes:

- 5353 (mDNS)
- 443 (WebServer): configurable
- 5670 (comunicación de grupo de multidifusión)
- C000-> F000 identifica dinámicamente un puerto libre para que cada miembro se comunique en el grupo

Mejores prácticas de redes

- Los grupos están diseñados para ser pequeños y se encuentran en la misma red local de vínculo físico.
- Se recomienda utilizar el puerto de red dedicado de iDRAC para mejorar la seguridad. También se admite LOM compartida.

Consideraciones adicionales acerca de redes

Dos iDRAC que están separadas por un enrutador en la topología de red se consideran que están en redes locales independientes y no se pueden unir en el mismo grupo local de iDRAC. Es decir, si la iDRAC está configurada para la configuración de NIC dedicada, el cable de red conectado al puerto dedicado de iDRAC en la parte posterior del servidor debe estar en una red local para todos los servidores pertinentes.

Si la iDRAC está configurada para la configuración de red de LOM compartida, la conexión de red compartida utilizada por el host de servidor e IDRAC debe estar conectada en una red local para que se detecte e incorpore esos servidores en un grupo común con Group Manager. Las iDRAC configuradas con una combinación de la configuración NIC del modo LOM dedicada y compartida también se podrían incorporar a un grupo común si todas las conexiones de red no pasan a través de un enrutador.

Efecto de snooping de MLD en entornos de VLAN en la detección del administrador de grupo

Dado que el administrador de grupo utiliza direccionamiento multidifusión IPv6 para la detección iniciada por nodos, una función denominada Snooping de MLD puede impedir que los dispositivos habilitados por el administrador de grupo se detecten entre sí en el caso de que no estén configurados correctamente. Snooping de MLD es una función de switch de éter común que pretende reducir la cantidad de tráfico con multidifusión IPv6 innecesario en una red.

Si Snooping MLD está activo en cualquier red, asegúrese de que haya un solicitante de MLD habilitado, de modo que los switches de éter se mantengan actualizados con los dispositivos activos del administrador de grupo de la red. Como alternativa, si no es necesario el Snooping de MLD, se puede deshabilitar. Tenga en cuenta que algunos switches de red tienen el Snooping de MLD habilitado de manera predeterminada. Al igual que los módulos de switches del chasis MX7000.

NOTA:

Por ejemplo

- Para deshabilitar el snooping de MLD en una VLAN en un IOM MX5108n:

  MX5108N-B1# configure terminal

  MX5108N-B1(config)# interface vlan 194

  MX5108N-B1(conf-if-vl-194)#no ipv6 mld snooping

- Para habilitar un solicitante de MLD en una VLAN en el IOM MX5108n:

  MX5108N-B1# configure terminal

  MX5108N-B1(config)# interface vlan 194

  MX5108N-B1(conf-if-vl-194)#ipv6 mld snooping querier

Administrar los inicios de sesión

Use esta sección para ejecutar las opciones **Add New User (Agregar nuevo usuario)**, **Change User Password (Cambiar contraseña de usuario)** y **Delete User (Eliminar usuario)** del grupo.

Los trabajos de grupo, incluida la administración de los inicios de sesión, son configuraciones que se realizan una vez en los servidores. Group Manager utiliza los SCP y los trabajos para realizar cualquier cambio. Cada iDRAC en el grupo cuenta con un trabajo individual en su cola de trabajos para cada trabajo de Group Manager. Group Manager no detecta cambios en las iDRAC miembro ni bloquea las configuraciones de miembro.

NOTA: Los trabajos de grupo no configuran ni hacen prevalecer el modo de bloqueo para cualquier iDRAC específica.

Dejar un grupo no cambia el usuario local ni la configuración en una iDRAC miembro.

Agregar un nuevo usuario

Use esta sección para crear y agregar un nuevo perfil de usuario en todos los servidores de dicho grupo. Un trabajo de grupo podría crearse para agregar al usuario a todos los servidores de ese grupo. El estado del trabajo de grupo se puede encontrar en la página **Group Manager** > **Jobs (Trabajos)**.

NOTA: De manera predeterminada, la iDRAC está configurada con una cuenta de administrador local. Puede acceder a información adicional sobre cada parámetro con una cuenta de administrador local.

Para obtener más información, consulte Configuración de las cuentas y los privilegios de usuario.

Tabla 36. Opciones de usuario nuevo

Opción	Descripción
Información de nuevo usuario	Permite proporcionar los detalles de información del usuario nuevo.
Permisos de iDRAC	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 miembro con el bloqueo de sistema habilitado y que forma parte del mismo grupo arroja un error que indica que la contraseña del usuario no se ha actualizado.

Cambiar contraseña de usuario

Use esta sección para cambiar la información de contraseña del usuario. Es posible ver los detalles de **Users (Usuarios)** con la información sobre **User Name (Nombre de usuario)**, **Role (Rol)** y **Domain (Dominio)** del usuario individual. Un trabajo de grupo podría crearse 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 **Group Manager** > **Jobs (Trabajos)**.

Si el usuario ya existe, la contraseña se puede actualizar. Cualquier iDRAC miembro con el bloqueo de sistema habilitado y que forma parte del grupo arroja un error que indica que la contraseña del usuario no se ha actualizado. Si el usuario no existe y, Group Manager recibe un error que indica que el usuario no existe en el sistema. La lista de usuarios que figura en la interfaz gráfica del usuario de Group Manager se basa en la lista actual de usuarios de la iDRAC que actúa como la controladora principal. No aparecen todos los usuarios de todas las iDRAC.

Eliminar usuario

Use esta sección para eliminar usuarios de todos los servidores de grupo. Un trabajo de grupo podría crearse para eliminar usuarios de todos los servidores de grupo. El estado del trabajo de grupo se puede encontrar en la página **Group Manager** > **Jobs (Trabajos)**.

Si el usuario ya existe en una iDRAC miembro, el usuario puede eliminarse. Cualquier iDRAC miembro con el bloqueo de sistema habilitado y que forma parte del grupo arroja un error que indica que el usuario no se ha eliminado. Si el usuario no existe, aparecerá una eliminación correcta de esa iDRAC. La lista de usuarios que figura en la interfaz gráfica del usuario de Group Manager se basa en la lista actual de usuarios de la iDRAC que actúa como la controladora principal. No aparecen todos los usuarios de todas las iDRAC.

Configuración de alertas

Use esta sección para configurar alertas por correo electrónico. De manera predeterminada, las alertas están deshabilitadas. Sin embargo, puede habilitarlas en cualquier momento. Un trabajo de grupo podría crearse para aplicar la configuración de alertas por correo electrónico a todos los servidores de grupo. El estado del trabajo de grupo se puede supervisar en la página **Group Manager** > **Jobs (Trabajos)**. La alerta por correo electrónico de Group Manager configura alertas por correo electrónico para todos los miembros. Configura los valores del servidor SMTP para todos los miembros del mismo grupo. Cada iDRAC se configura por separado. La configuración de correo electrónico no se guarda de manera global. Los valores actuales se basan en la iDRAC que actúa como controladora principal. Si deja un grupo, no vuelven a configurarse las alertas por correo electrónico.

Para obtener más información sobre la configuración de alertas, consulte Configuración de la iDRAC para enviar alertas.

Tabla 37. Opciones de configuración de alertas

Opción	Descripción
Configuración de la dirección del servidor SMTP (correo electrónico)	Permite configurar la dirección IP del servidor y el número de puerto SMTP, y habilitar la autenticación. En caso de que habilite la autenticación, deberá proporcionar el nombre de usuario y la contraseña.
Direcciones de correo electrónico	Permite configurar múltiples identificaciones de correo electrónico para recibir notificaciones por correo electrónico sobre cambios en el estado del sistema. Es posible enviar un correo electrónico de prueba a la cuenta configurada desde el sistema.
Categorías de alertas	Permite seleccionar varias categorías de alertas para recibir notificaciones por correo electrónico.

NOTA: Cualquier iDRAC miembro con el bloqueo de sistema habilitado y que forma parte del mismo grupo arroja un error que indica que la contraseña del usuario no se ha actualizado.

Exportar

Use esta sección para exportar el resumen del grupo al sistema local. La información se puede exportar a un formato de archivo csv. Este contiene datos relacionados con cada sistema individual en el grupo. La exportación incluye la siguiente información en formato csv. Detalles del servidor:

- Condición
- Nombre del host
- Dirección IPV4 de la iDRAC
- Dirección IPV6 de la iDRAC
- Asset Tag

- Modelo
- Versión del firmware del iDRAC
- Última actualización de estado
- Código de servicio rápido
- Conectividad de la iDRAC
- Estado de la alimentación
- Sistema operativo
- Etiqueta de servicio
- ID del nodo
- Nombre de DNS de la iDRAC
- Versión del BIOS
- Detalles de la CPU
- Memoria del sistema (MB)
- Detalles de la ubicación

NOTA: Si usa Internet Explorer, debe deshabilitar la configuración de seguridad mejorada para descargar correctamente el archivo csv.

Vista de servidores detectados

Después de crear el grupo local, Group Manager de la iDRAC les notifica a todas las otras iDRAC en la red local que el nuevo grupo se ha creado. Para que las iDRAC figuren en los servidores detectados, debe estar habilitada la función Group Manager en cada iDRAC. En la vista de servidores detectados, aparece la lista de las iDRAC detectadas en la misma red, que pueden formar parte de cualquier grupo. Si la iDRAC no aparece en la lista de sistemas detectados, el usuario debe iniciar sesión en la iDRAC específica y unirse al grupo. La iDRAC que creó el grupo aparecerá como el único miembro de la vista de elementos esenciales hasta que se unan más iDRAC al grupo.

NOTA: La vista de servidores detectados en la consola de Group Manager le permite incorporar a ese grupo uno o más servidores que aparecen en la vista. Es posible controlar el avance de la actividad desde **Group Manager** > **Jobs (Trabajos)**. Otra opción consiste en iniciar la sesión en la iDRAC y seleccionar de la lista desplegable el grupo al que desea incorporarse a fin de unirse a ese grupo. Puede acceder a la pantalla de bienvenida de Group Manager desde la página de índice de la iDRAC.

Tabla 38. Opciones de incorporación al grupo

Opción	Descripción
Incorporación y cambio de inicio de sesión	Seleccione una fila específica y escoja la opción Onboard and Change Login (Incorporación y cambio de inicio de sesión) para obtener los sistemas recién detectados en el grupo. Si desea unirse al grupo, debe proporcionar las credenciales de inicio de sesión de administrador para los sistemas nuevos. Si el sistema tiene la contraseña predeterminada, debe cambiarla cuando la incorpora a un grupo. La incorporación a un grupo le permite aplicar la misma configuración de alertas de grupo a los sistemas nuevos.
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)

Esta vista permite que el usuario controle el progreso de un trabajo de grupo y ofrece pasos de recuperación sencillos para corregir errores provocados por la conectividad. En esta vista también se incluye el historial de las últimas acciones de grupo que se realizaron como registro de auditoría. El usuario puede utilizar la vista de trabajos para controlar el progreso de la acción en el grupo o para cancelar una acción programada para producirse 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.

Tabla 39. Vista Jobs (Trabajos)

Opción	Descripción
Estado	Muestra el estado del trabajo y el estado del trabajo en curso.
Trabajo	Muestra el nombre del trabajo.
ID	Muestra la identificación del trabajo.
Hora de inicio	Muestra la hora de inicio.
Hora de finalización	Muestra la hora de finalización.
Acciones	• Cancel (Cancelar): Es posible cancelar un trabajo programado antes de que comience a ejecutarse. Es posible detener un trabajo en ejecución mediante el uso el botón Stop (Detener). • Rerun (Volver a ejecutar): Le permite al usuario volver a ejecutar un trabajo cuyo estado indique un error. • Remove (Eliminar): Le permite al usuario quitar los trabajos anteriores finalizados.
Exportar	Es posible exportar la información del trabajo de grupo al sistema local para tenerla como referencia futura. La lista de trabajos se puede exportar al formato de archivo csv y contiene todos los datos relacionados con un trabajo específico.

NOTA: Para cada entrada de trabajo, la lista de sistemas incluye detalles hasta de 100 sistemas. Cada entrada del sistema contiene el nombre del host, la etiqueta de servicio, el estado del trabajo del miembro y un mensaje en caso de que ocurra un error con el trabajo.

Todas las acciones de grupo que crean trabajos se llevan a cabo en todos los miembros de grupo con efecto inmediato. Es posible puede realizar las siguientes tareas:

- Agregar, editar o eliminar usuarios
- Configurar alertas por correo electrónico
- Cambiar el nombre y el código de acceso de los grupos

NOTA: Los trabajos de grupo se completan rápidamente, siempre y cuando todos los miembros estén en línea y sea posible acceder a ellos. Es posible que un trabajo demore 10 minutos desde el inicio hasta el final. Un trabajo esperará y volverá a intentar su ejecución durante un máximo de 10 horas para los sistemas a los que no sea posible tener acceso.

NOTA: Mientras se esté ejecutando un trabajo de incorporación, no es posible programar ningún otro trabajo. Los trabajos incluyen los siguientes:

- Agregar nuevo usuario
- Cambiar contraseña de usuario
- Eliminar usuario
- Configuración de alertas
- Incorporar sistemas adicionales
- Cambiar código de acceso de grupo
- Cambiar nombre de grupo

Intentar invocar otro trabajo mientras está en curso una tarea de incorporación provocará la aparición del código de error GMGR0039. Una vez que la tarea de incorporación ejecute el primer intento de incorporación de todos los sistemas nuevos, es posible crear trabajos en cualquier momento.

Exportación de trabajos

Es posible exportar el registro al sistema local para tener 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

En el panel de información de grupo, en la parte superior derecha de la vista de resumen de Group Manager, es posible ver un resumen consolidado del grupo. La configuración de grupo actual puede editarse en la página de configuración de grupo, a la que se tiene acceso haciendo clic en el botón Group Settings (Configuración de grupo). Allí es posible ver cuántos sistemas se encuentran en el grupo. Además, incluye información sobre la controladora principal y la controladora secundaria del grupo.

Configuración de grupo

La página de configuración de grupo proporciona una lista de atributos del grupo seleccionado.

Tabla 40. Atributos de configuración de grupo

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 fecha y 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 respaldo. En caso de que el sistema de control no esté disponible, este sistema de respaldo cumplirá el rol de sistema de control.

Permite que el usuario lleve a cabo las acciones que se enumeran en la tabla debajo del grupo. Un trabajo de configuración de grupo podría crearse para estas acciones (cambiar nombre de grupo, cambiar código de acceso de grupo, eliminar los miembros y eliminar el grupo). El estado del trabajo de grupo se puede ver o modificar en la página **Group Manager** > **Jobs (Trabajos)**.

Tabla 41. Acciones de configuración de grupo

Acciones	Descripción
Cambiar el nombre	Permite cambiar la opción **Current Group Name (Nombre de grupo actual)** con **New Group Name (Nuevo nombre de grupo)**.
Cambiar código de acceso	Permite cambiar la contraseña de grupo existente introduciendo un valor en **New Group Passcode (Nuevo código de acceso de grupo)** y validándolo en **Reenter New Group Passcode (Volver a introducir el nuevo código de acceso de grupo)**.
Eliminar sistemas	Permite eliminar varios sistemas del grupo a la vez.

Tabla 41. Acciones de configuración de grupo (continuación)

Acciones	Descripción
Eliminar grupo	Permite eliminar el grupo. Para utilizar cualquier función de Group Manager, el usuario debe tener privilegios de administrador. Cualquier trabajo pendiente se detendrá si se elimina el grupo.

Acciones en un servidor seleccionado

En la página de resumen, puede hacer doble clic en una fila para iniciar la iDRAC de ese servidor mediante un redireccionamiento de inicio de sesión único. Asegúrese de apagar el bloqueador de elementos emergentes en la configuración del navegador. Puede realizar las siguientes acciones en el servidor seleccionado haciendo clic en el elemento correspondiente en la lista desplegable **More Actions (Más acciones)**.

Tabla 42. Acciones en un servidor seleccionado

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:** Deshabilite el bloqueador de elementos emergentes desde el navegador para utilizar esta funcionalidad.

Inicio de sesión único de Group Manager

Todas las iDRAC en el grupo confían la una en la otra según el código de acceso secreto compartido y el nombre de grupo compartido. Como resultado, a un usuario administrador en una iDRAC de miembro de grupo se le otorgan privilegios de nivel de administrador en cualquier iDRAC de miembro de grupo cuando se accede mediante el inicio de sesión único de la interfaz web de Group Manager. La iDRAC registra <usuario>-<SVCTAG> como el usuario que ha iniciado sesión en los miembros del mismo nivel. <SVCTAG> es la etiqueta de servicio de la iDRAC donde el usuario inició la sesión primero.

Conceptos de Group Manager: Sistema de control

- Se selecciona de manera automática; de manera predeterminada, es la primera iDRAC configurada para Group Manager.
- Proporciona el flujo de trabajo de la interfaz gráfica del usuario de Group Manager.
- Realiza el seguimiento de todos los miembros.
- Coordina tareas.
- Si un usuario inicia sesión en cualquier miembro y hace clic para abrir Group Manager, el navegador se redirigirá a la controladora principal.

Conceptos de Group Manager: Sistema de respaldo

- La controladora principal selecciona automáticamente una controladora secundaria para tomar el control si la principal se desconecta durante mucho tiempo (10 minutos o más).
- Si la controladora primaria y la secundaria se desconectan durante mucho tiempo (durante más de 14 minutos), se seleccionan una controladora principal y una secundaria nuevas.
- Conserva una copia de la caché de Group Manager de todos los miembros de grupo y tareas.
- Group Manager determinar el sistema de control y el de respaldo automáticamente.
- No se requiere la configuración ni participación del usuario.

Actualización de firmware del grupo de iDRAC

Para la actualización de firmware del grupo de iDRAC, desde el archivo DUP de un directorio local, realice los siguientes pasos:

1. Acceda a la vista esencial de la consola del Administrador de grupo y haga clic en **Actualizar el firmware del iDRAC** en la vista de resumen.
2. En el cuadro de diálogo de actualización del firmware que se muestra, busque y seleccione el archivo DUP local de iDRAC que se va a instalar. Haga clic en **Cargar**.
3. El archivo se carga en iDRAC y se verifica para verificar su integridad.
4. Confirme la actualización del firmware. El trabajo de actualización de firmware de iDRAC de grupo está programado para la ejecución inmediata. Si el Administrador de grupo tiene otros trabajos de grupo en ejecución, se ejecuta después de que se completa el trabajo anterior.
5. Puede realizar un seguimiento de la ejecución del trabajo de actualización de iDRAC desde la vista de trabajos de grupo.

NOTA: Esta función solo es soportada en la versión 3.50.50.50 de iDRAC y superior.

14

Administración de registros

La iDRAC proporciona un registro de Lifecycle que contiene eventos 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 eventos del sistema también están disponibles en un registro distinto denominado registro de eventos del sistema (SEL). Es posible acceder al registro de Lifecycle en la interfaz web de la iDRAC, RACADM y la interfaz de WSMan.

Cuando el tamaño del registro de Lifecycle alcanza los 800 KB, los registros se comprimen y se archivan. Solo es posible ver las entradas de los registros no archivados y aplicar filtros y comentarios a dichos registros. Para ver los registros archivados, deberá exportar el registro completo de Lifecycle a una ubicación del sistema.

Temas:

Visualización del registro de sucesos del sistema

Cuando tiene lugar un suceso del sistema, se registra en el registro de sucesos del sistema (SEL). La misma entrada del SEL también está disponible en el registro del LC.

NOTA: Es posible que los registros de SEL y LC no coincidan en el registro de fecha y hora cuando iDRAC se está reiniciando.

Visualización del registro de sucesos del sistema mediante la interfaz web

Para ver el SEL, en la interfaz web de la iDRAC, vaya a **Maintenance (Mantenimiento)** > **System Event (Evento del sistema)**.

En la página **System Event Log (Registro de eventos del sistema)**, aparece un indicador de estado del sistema, una marca de hora y fecha, y una descripción de cada evento 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 la cantidad de entradas de SEL: `racadm getsel -i`

Para borrar las entradas de SEL: `racadm clrsel`

Para obtener más información, consulte *Guía de la CLI de RACADM para iDRAC* disponible en https://www.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 en el registro de eventos del sistema (SEL) mediante la utilidad de configuración de la iDRAC y también 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 **Yes (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 es posible agregar notas de trabajo a cada entrada del registro.

Los eventos y las actividades siguientes se registran:

- Todos
- Estado del sistema: Esta categoría representa todas las alertas que están relacionadas con en el hardware dentro del chasis del sistema.
- Almacenamiento: Esta categoría representa las alertas que están relacionadas con el subsistema de almacenamiento.
- Actualizaciones: Esta categoría representa las alertas que se generan debido a actualizaciones o degradaciones de firmware o drivers.
- Auditoría: Esta categoría representa el registro de auditoría.
- Configuración: Esta categoría representa las alertas que están relacionadas con los cambios de configuración de hardware, firmware y 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:

- SSH
- Interfaz web
- RACADM
- Redfish
- 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 es posible exportar y añadir una nota de trabajo a un suceso del 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 de 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.

NOTA: En las plataformas MX, Lifecycle Controller registra varios ID de trabajos para la configuración o instalación de trabajos creados con OME-Modular. Para obtener más información sobre el trabajo realizado, consulte los registros de OME-Modular.

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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

Adición de notas de trabajo

Cada usuario que inicie sesión en la iDRAC puede agregar notas de trabajo y estas se almacenan como un evento en el registro de Lifecycle. Es necesario tener un privilegio de registro en iDRAC para agregar notas de trabajo. Se admite un máximo de 255 caracteres en 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 la iDRAC, vaya a **Dashboard (Tablero)** > **Notes (Notas)** > **Add note (Agregar nota)**. Aparecerá la página **Work Notes (Notas del 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 **Guardar**.
   La nota de trabajo se agrega al registro. Para obtener más información, consulte la *Ayuda en línea de iDRAC*.

Configuración del registro del sistema remoto

Es posible enviar registros de Lifecycle a un sistema remoto. Antes de hacerlo, asegúrese de lo siguiente:

- Hay conectividad de red entre iDRAC y el sistema remoto.
- El sistema remoto e iDRAC se encuentran en la misma red.

Configuración del registro del sistema remoto mediante la interfaz web

Para configurar los valores del servidor de registro del sistema remoto:

1. En la interfaz web de la iDRAC, vaya a **Configuration (Configuración)** > **System Settings (Configuración del sistema)** > **Remote Syslog Settings (Configuración del registro del sistema remoto)**.
   Aparece la pantalla **Configuración del registro del sistema remoto**.
2. Habilite 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 escriben en el registro de Lifecycle también se escriben 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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

15

Supervisión y administración de la alimentación en iDRAC

Puede utilizar iDRAC para supervisar y administrar los requisitos de alimentación del sistema administrado. Esto ayuda a proteger el sistema de las interrupciones de alimentación, ya que distribuye y regula adecuadamente el consumo de alimentación en el sistema.

Las características claves son las siguientes:

- **Supervisión de alimentación**: consulte el estado de alimentación, el historial de las mediciones de alimentación, los promedios actuales, los picos, etc. para el sistema administrado.
- **Límites de alimentación:** consulte y establezca los límites de alimentación del sistema administrado, incluida la visualización del consumo de alimentación potencia mínimo y máximo. Esta es una función con licencia.
- **Control de alimentación**: permite realizar operaciones de control de alimentación de manera remota (tales 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, tales 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 tendencia de consumo de energía del sistema (por hora, día o semana) se mantienen únicamente mientras el iDRAC está en ejecución. Si el iDRAC se reinicia, los datos de consumo de energía existentes se pierden y el histograma se reinicia.

NOTA: Después de aplicar una actualización o restablecimiento del firmware de iDRAC, el gráfico de consumo de energía se borrará o restablecerá.

Supervisión del índice de rendimiento de módulos de E/S, memoria y CPU mediante la interfaz web

Para supervisar el índice de rendimiento de los módulos de E/S, memoria y CPU, 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**:
  - En esta sección, se proporcionan las estadísticas de la utilización de E/S, memoria y CPU, y el índice de CUPS a nivel del sistema. Si el sistema de host está apagado, el gráfico muestra la línea de apagado por debajo del 0 %.
  - Es posible restablecer el pico de utilización para un determinado sensor. Haga clic en **Reset Historical Peak (Restablecer pico histórico)**. Debe tener el privilegio Configure (Configurar) para poder restablecer el valor de pico.
- Sección **Métricas de rendimiento**:
  - Muestra el estado y la lectura presente.
  - Muestra o especifica el límite de utilización del umbral de advertencia. Debe tener el privilegio Server Configure (Configurar servidor) para poder establecer los valores de los umbrales.

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 entrada y salida 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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

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 después de apagar y encender el sistema, según la capacidad de la PSU 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 blade se establece según la asignación de alimentación para CMC (para plataformas que no son MX) u OME Modular (para plataformas MX).

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 la 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/hora)**.

   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 **vatios**, el sistema calcula y muestra automáticamente el valor en **BTU/h**. De la misma manera, si introduce BTU/h, se muestra el valor en **vatios**.
4. Haga clic en **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.

También puede realizar estas operaciones con Lifecycle Controller Remote Services o WSMan. Para obtener más información, consulte *Guía de inicio rápido de servicios remotos de Lifecycle Controller* disponible en https://www.dell.com/idracmanuals y el documento *Dell Power State Management Profile* (Perfil de administración de estado de alimentación de Dell) disponible en https://www.dell.com/support.

Las operaciones de control de alimentación del servidor iniciadas desde la iDRAC son independientes del comportamiento del botón de encendido configurado en el BIOS. Puede utilizar la función PushPowerButton para apagar o encender el sistema de forma ordenada, incluso si el BIOS está configurado para no hacer nada cuando se presione el botón de encendido físico.

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** > **Administración de energía** > **Control de alimentación**. Aparecerá las opciones de **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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

Límites de alimentación

Puede ver los límites de umbral de alimentación que abarca la gama de consumo de energía 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 encender un servidor blade, según el inventario limitado de hardware, la iDRAC le proporciona los requisitos de alimentación del servidor blade al administrador del chasis. Si aumenta el consumo de energía con el tiempo y si el servidor consume la asignación máxima de energía, la iDRAC solicita CMC (en las plataformas no MX) u OME Modular (en las plataformas MX) para aumentar la energía potencial máxima. Esto da como resultado un aumento en el suministro de alimentación; sin embargo, este suministro no reduce si el consumo disminuye.

Después de que se encienda e inicialice el sistema, iDRAC calculará un nuevo requisito de alimentación según la configuración de hardware real. El sistema permanece encendido incluso si CMC (no para las plataformas MX) u OME Modular (no en las plataformas MX) fallan en la asignación de una nueva solicitud de alimentación.

CMC u OME Modular recupera toda la energía sin utilizar de los servidores de menor prioridad y la asigna a un servidor o un módulo de infraestructura de mayor prioridad.

Visualización y configuración de la política de límites de alimentación

Cuando se activa la política de límite de alimentación, se imponen los límites definidos por el usuario en el sistema. Si el límite de alimentación no está activado, se utiliza la política predeterminada de protección de alimentación del hardware. Esta política de protección de alimentación es independiente de la política definida por el usuario. El rendimiento del sistema se ajusta de manera dinámica para mantener el consumo de energía cerca del umbral especificado.

El consumo de energía real depende de la carga de trabajo. Puede superar momentáneamente el umbral hasta que se completen los ajustes de rendimiento. Por ejemplo, si se considera un sistema cuyos valores mínimos y máximos de consumo de energía potencial son 500 W y 700 W, respectivamente. Puede especificar el umbral de presupuesto de energía en 525 W para disminuir el consumo. Cuando se configura este presupuesto de energía, el rendimiento del sistema se ajusta de forma dinámica para mantener un consumo de 525 W o menos.

Si establece un límite de alimentación muy bajo, o bien si la temperatura ambiente es inusualmente alta, es posible que el consumo de energía sea superior al límite de alimentación durante el encendido o el restablecimiento del sistema.

Si el valor del límite de alimentación establecido es inferior al umbral mínimo recomendado, es posible que iDRAC no pueda mantener el límite solicitado.

Puede especificar el valor en vatios, BTU/hora, o bien como un porcentaje del límite de alimentación máximo recomendado.

Cuando se establece el umbral del límite de alimentación en BTU/hora, la conversión a vatios se redondea al número entero más cercano. Cuando se obtiene el umbral del límite de alimentación del sistema, la conversión de vatios a BTU/hora también se redondea. Debido al redondeo, es posible que los valores reales varíen levemente.

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 **Configuración** > **Administración de energía** > **Política de límite de alimentación**. El límite de la política de alimentación actual se muestra en la sección **Límites de alimentación**.
2. Seleccione **Activar** en **Límite de alimentación**.
3. En la sección **Límites de alimentación**, ingrese el límite de alimentación dentro del rango recomendado en vatios y BTU/hora o el porcentaje (%) máximo del límite de sistema recomendado.
4. Haga clic en **Aplicar** para aplicar los valores.

Configuración de la política de límites de alimentación mediante RACADM

Para ver y configurar los valores de límites de 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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.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 la corrección del factor de energía está activada, el servidor consume una pequeña cantidad de energía cuando el host está apagado. De forma predeterminada, la corrección del factor de energía está activada cuando el servidor se envía desde la 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 la iDRAC, vaya a **Configuration (Configuración)** > **Power Management (Administración de energía)** > **Power Configuration (Configuración de alimentación)**.
2. En **Power Redundancy Policy (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 `get/set`:

- System.Power.RedundancyPolicy
- System.Power.Hotspare.Enable
- System.Power.Hotspare.PrimaryPSU
- System.Power.PFC.Enable

Para obtener más información, consulte *Guía de la CLI de RACADM para iDRAC* disponible en https://www.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.
   - Habilite o deshabilite 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.

Enfriamiento multivector

Con el enfriamiento multivector, se implementa un enfoque de varias puntas para los controles térmicos en las plataformas del servidor Dell EMC. Para configurar las opciones de enfriamiento multivector a través de la interfaz web de iDRAC, vaya a **Configuración** > **Configuración del sistema** > **Configuración de hardware** > **Configuración del ventilador**. Incluye (entre otros elementos) lo siguiente:

- Un gran conjunto de sensores (térmicos, de alimentación, de inventario, etc.) que permiten una interpretación precisa del estado térmico del sistema en tiempo real en diversas ubicaciones dentro del servidor. Muestra solo un pequeño subconjunto de sensores que son relevantes para las necesidades de los usuarios según la configuración.
- Gracias al algoritmo de control de loop cerrado inteligente y adaptable, se optimiza la respuesta del ventilador para mantener las temperaturas de los componentes. También conserva la potencia del ventilador, el consumo de flujo de aire y la acústica.
- Si se utiliza la asignación de zonas del ventilador, se puede iniciar el enfriamiento de los componentes cuando sea necesario. Por lo tanto, se obtiene el máximo rendimiento sin comprometer la eficiencia de la utilización de energía.
- Representación precisa del flujo de aire de PCIe ranura por ranura en términos de la métrica LFM (pies lineales por minuto: un estándar aceptado del sector sobre cómo se especifica el requisito de flujo de aire de la tarjeta PCIe). Con la visualización de esta métrica en diversas interfaces de iDRAC, el usuario puede realizar lo siguiente:
  1. conocer la funcionalidad máxima de cada ranura LFM dentro del servidor;
  2. conocer el enfoque adoptado para el enfriamiento de PCIe de cada ranura (control del flujo de aire, control de la temperatura);
  3. conocer el mínimo de LFM que se entrega en una ranura si la tarjeta es una tarjeta de terceros (tarjeta personalizada definida por el usuario);
  4. marcar el valor mínimo de LFM personalizado para la tarjeta de terceros, lo cual permite una definición más precisa de las necesidades de enfriamiento de esta, que el usuario conoce mejor gracias a las especificaciones personalizadas de la tarjeta.

- Muestra la métrica de flujo de aire del sistema en tiempo real (CFM, pies cúbicos por minuto) en varias interfaces de iDRAC para que el usuario habilite el balanceo de flujo de aire del centro de datos en función de la agregación del consumo de CFM por servidor.
- Permite ajustes térmicos personalizados como perfiles térmicos (máximo rendimiento en comparación con máximo rendimiento por vatio, límite de sonido); opciones personalizadas de velocidad del ventilador (velocidad mínima del ventilador, intervalos de velocidad del ventilador); y configuración personalizada de la temperatura de salida.
  1. La mayoría de estos ajustes permiten un mayor enfriamiento respecto del enfriamiento de base que se genera por algoritmos térmicos y no permiten que las velocidades del ventilador estén por debajo de los requisitos de enfriamiento del sistema.

     NOTA: Existe una excepción a la declaración anterior para las velocidades del ventilador que se agregan a las tarjetas PCIe de terceros. El flujo de aire de provisión del algoritmo térmico para tarjetas de terceros puede ser mayor o menor que las necesidades de enfriamiento de la tarjeta real y el cliente puede ajustar la respuesta de la tarjeta ingresando la métrica de LFM correspondiente a la tarjeta de terceros.
  2. Con la opción de temperatura de salida personalizada, se limita la temperatura de salida según la configuración deseada del cliente.

     NOTA: Es importante tener en cuenta que, con ciertas configuraciones y cargas de trabajo, puede que no sea físicamente posible reducir la salida por debajo del punto de ajuste deseado (p. ej., ajuste de salida personalizado de 45 °C con una temperatura de entrada alta [p. ej., 30 °C] y una configuración cargada [consumo de energía del sistema alto, flujo de aire bajo]).
  3. La opción de límite de sonido es nueva en la 14.ª generación de servidores PowerEdge. Limita el consumo de energía de la CPU, además de controlar la velocidad del ventilador y el límite acústico. Esto es exclusivo de las implementaciones acústicas y puede reducir el rendimiento del sistema.
- El diseño del sistema permite una mayor capacidad de flujo de aire, ya que permite una potencia alta, y configuraciones de sistema densas. Proporciona menos restricciones del sistema y una mayor densidad de las funciones.
  1. El flujo de aire optimizado permite un flujo de aire eficiente en relación con el consumo de potencia del ventilador.
- Los ventiladores personalizados están diseñados para ofrecer mayor eficiencia, mejor rendimiento, una vida útil más larga y menos vibración. También proporciona una mejor salida acústica.
  1. Los ventiladores pueden durar mucho tiempo (en general, pueden durar más de 5 años), incluso si funciona a toda velocidad todo el tiempo.
- Los disipadores de calor personalizados están diseñados para optimizar el enfriamiento de los componentes con un flujo de aire mínimo (requerido); sin embargo, admiten CPU de alto rendimiento.

16

iDRAC Direct Updates

iDRAC provides out of band ability to update the firmware of various components of a PowerEdge server. iDRAC direct update helps in eliminating staged jobs during updates. This is supported only for iDRAC releases 5.00.00.00 and above. Only SEP(passive) backplanes are supported for direct updates.

iDRAC used to have staged updates to initiate firmware update of the components. From this release, Direct updates have been applied to PSU and Backplane. With the use of Direct Updates and Backplane can have quicker updates. In case of PSU, one reboot (for initializing the updates) is avoided and the update can happen in single reboot.

With Direct update feature in iDRAC, you can eliminate the first reboot to initiate the updates. The second reboot will be controlled by the device itself and iDRAC notifies the user if there is need for a separate reset via job status.

17

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 amplitud de banda). Puede deshabilitar una partición cambiando la configuración del atributo VirtualizationMode a NPAR o deshabilitando todas las personalidades en una partición.

Según el tipo de dispositivo de CNA instalado, es posible que la configuración de atributos de una partición no se conserve desde la última vez que la partición estuvo activada. Configure todos los atributos de la identidad de E/S y los atributos relacionados con la partición cuando habilite una partición. Puede habilitar una partición cambiando la configuración del atributo VirtualizationMode a NPAR o habilitando una personalidad (por ejemplo, NicMode) en 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 **System (Sistema)** > **Overview (Descripción general)** > **Network Devices (Dispositivos de red)**. Se mostrará la página **Dispositivos de red**. Para obtener más información acerca de las propiedades que aparecen, consulte la *Ayuda en línea de la 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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

Es posible que se muestren propiedades adicionales cuando se utiliza RACADM o WSMan, además de las propiedades que se muestran en la interfaz web de la iDRAC.

Vista Conexión

La revisión y la solución de problemas manuales de las conexiones de red de los servidores no se pueden controlar en un entorno de centro de datos. iDRAC9 agiliza el trabajo con la vista de conexión de iDRAC. Esta función le permite revisar las conexiones de red y solucionar problemas de forma remota desde la misma GUI centralizada que utiliza para implementar, actualizar, supervisar y mantener los servidores. En la vista de conexión de iDRAC9, se proporcionan detalles de la asignación física de los puertos del conmutador a los puertos de red del servidor y las conexiones de puertos dedicados de iDRAC (controladora de acceso remoto integrada de Dell). Se pueden ver todas las tarjetas de red compatibles en la vista de conexión, independientemente de la marca.

En lugar de revisar las conexiones de red del servidor y solucionar problemas de forma manual, puede ver y administrar las conexiones de cable de red de forma remota.

La Vista Conexión proporciona información de los puertos del conmutador que están conectados a los puertos del servidor y al puerto dedicado de iDRAC. Los puertos de red del servidor incluyen los de PowerEdge LOM, NDC, las tarjetas intermedias y las tarjetas PCIe complementarias.

Para acceder a la vista de conexión de los dispositivos de red, vaya a **Sistema** > **Descripción general** > **Dispositivo de red** > **Vista de la conexión**.

Además, puede hacer clic en **Configuración de iDRAC** > **Conectividad** > **Red** > **Configuración común** > **Vista de conexión** para activar o desactivar la vista de conexión.

La vista de conexión se puede explorar con el comando racadm `SwitchConnection View` y también se puede ver con el comando.

Campo u opción	Descripción
Activado	Seleccione **Activado** para activar la Vista Conexión. La opción **Activado** está seleccionada de manera predeterminada.
Estado	Muestra **Activado** si se activa la opción de vista de conexión en **Vista de conexión** en Configuración de iDRAC.
ID de conexión del conmutador	Muestra el ID del chasis de la LLDP del conmutador por medio del que se conecta el puerto del dispositivo.
ID de conexión del puerto del conmutador	Muestra el ID del puerto de la LLDP del puerto del conmutador por medio del que se conecta el puerto del dispositivo.

NOTA: El ID de conexión del conmutador y el ID de conexión del puerto del conmutador están disponibles una vez que la vista de conexión está activada y el vínculo está conectado. La tarjeta de red asociada debe ser compatible con la Vista Conexión. Solo los usuarios con privilegios de configuración de iDRAC pueden modificar la configuración de la Vista Conexión.

Desde iDRAC9 4.00.00.00 y las versiones posteriores, iDRAC admite el envío de paquetes LLDP a los switches externos. Esto proporciona opciones para detectar las iDRAC en la red. iDRAC envía dos tipos de paquetes de LLDP a la red de salida:

- **LLDP de topología**: en esta función, el paquete LLDP pasa a través de todos los puertos NIC del servidor compatible, de modo que un switch externo pueda localizar el servidor de origen, el puerto NDC [NIC FQDD], la ubicación IOM del chasis, la etiqueta de servicio del chasis Blade, etc. Desde iDRAC9 4.00.00.00 y las versiones posteriores, LLDP de topología está disponible como una opción para todos los servidores PowerEdge. Los paquetes LLDP contienen información de conectividad del dispositivo de red del servidor y son utilizados por los módulos de E/S y los switches externos para actualizar la configuración.

  NOTA:
  - LLDP de topología debe estar habilitado para que la configuración del chasis MX funcione correctamente.
  - El LLDP de topología no se admite en las controladoras de 1 GbE y seleccione las controladoras de 10 GbE (Intel X520, QLogic 578xx).

- **LLDP de detección**: en esta función, el paquete LLDP solo pasa por el puerto NIC de iDRAC activo que está en uso (NIC dedicado o LOM compartido), de modo que el switch adyacente pueda localizar el puerto de conexión iDRAC en el switch. El LLDP de detección es específico solo para el puerto de red iDRAC activo y no se ve en todos los puertos de red del servidor. El LLDP de detección tiene algunos detalles de iDRAC, como la dirección IP, la dirección MAC, la etiqueta de servicio, etc., de modo que un switch pueda detectar automáticamente los dispositivos iDRAC conectados a este y algunos datos de iDRAC.
  NOTA: Si la dirección MAC virtual se borra en un puerto/partición, la dirección MAC virtual será igual a la dirección MAC.

Para habilitar o deshabilitar el LLDP de topología LLDP, vaya a **Configuración de iDRAC** > **Conectividad** > **Red** > **Configuración común** > **LLDP de topología** para activar o desactivar el LLDP de topología. De forma predeterminada, está activado para los servidores MX y está desactivado para todos los demás servidores.

Para activar o desactivar el LLDP de detección de iDrac, vaya a **Configuración de iDRAC** > **Conectividad** > **Red** > **Configuración común** > **LLDP de detección de iDrac**. La opción Enable (Activar) está seleccionada de manera predeterminada.

El paquete LLDP que se crea desde iDRAC se puede ver desde el switch con el comando: `show lldp neighbors`.

Actualizar Vista Conexión

Utilice **Actualizar vista de conexión** para ver la información más reciente del ID de conexión del conmutador y el ID de conexión del puerto del conmutador.

NOTA: Si la iDRAC tiene información de conexión del conmutador y de conexión del puerto del conmutador para el puerto de red del servidor o el puerto de red de la iDRAC, y, por algún motivo, esta información no se actualiza durante 5 minutos, entonces se mostrará como datos obsoletos (última información buena conocida) en todas las interfaces de usuario. En la interfaz de usuario, verá un signo de advertencia amarillo, el cual es una representación natural y no significa ninguna alerta.

Valores posibles de la vista de conexión

Datos posibles de la vista de conexión	Descripción
Función desactivada	La función Vista de conexión está desactivada. Para ver los datos de la vista de conexión, active la función.
Sin vínculo	Indica que el vínculo asociado al puerto de la controladora de red no funciona
No disponible	El LLDP no está activado en el conmutador. Revise si el LLDP está activado en el puerto del conmutador.
No compatible	La controladora de red no es compatible con la función Vista de conexión.
Datos obsoletos	Última información buena conocida. El vínculo del puerto de la controladora de red no funciona o el sistema está apagado. Utilice la opción de actualización para actualizar los detalles de la vista de conexión a fin de obtener los datos más recientes.
Datos válidos	Muestra información válida del ID de conexión del conmutador y el ID de conexión del puerto del conmutador.

Controladoras de red compatibles con la vista de conexión

Las siguientes controladoras o tarjetas son compatibles con la función Vista de conexión.

Fabricante	Tipo
Broadcom	• 57414 rNDC de 25 GE • 57416/5720 rNDC de 10 GbE • 57412/5720 rNDC de 10 GbE • 57414 PCIe FH/LP de 25 GE • 57412 PCIe FH/LP de 10 GbE • 57416 PCIe FH/LP de 10 GbE

Fabricante	Tipo
Intel	• X710 bNDC de 10 Gb • X710 DP PCIe de 10 Gb • X710 QP 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 OCP 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 de 10 GE • QL41112 PCIe 2P de 10 GE • QL41262 PCIe 2P de 25 GE

Inventorying and monitoring FC HBA devices

You can remotely monitor the health and view the inventory of the Fibre Channel Host Bus Adapters (FC HBA) devices in the managed system. The Emulex and QLogic FC HBAs are supported. For each FC HBA device, you can view the following information for the ports:

- FC storage target information
- NVMe storage target information
- Port Properties
- Receive and Transmit Statistics

NOTE: Emulex FC8 HBAs are not supported.

Supervisión de dispositivos HBA FC mediante la interfaz web

Para ver la información de dispositivos HBA FC mediante la interfaz web, vaya a **System (Sistema)** > **Overview (Descripción general)** > **Network Devices (Dispositivos de red)** > **Fibre Channel**. Para obtener más información acerca de las propiedades que aparecen, consulte la *Ayuda en línea de la 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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

Inventorying and monitoring SFP Transceiver devices

You can remotely monitor the health and view the inventory of SFP transceiver devices connected to the system. Following are the supported transceivers:

- SFP
- SFP+
- SFP28
- SFP-DD

- QSFP
- QSFP+
- QSFP28
- QSFP-DD
- Base-T modules
- AOC & DAC cables
- RJ-45 Base-T connected with Ethernet
- Fiber channel
- IB adapter ports

Most useful transceiver information are Serial number and Part number from transceiver EPROM. These would allow to verify the remotely installed transceivers, when troubleshooting connectivity issues. For each SFP Transceiver device, you can view the following information for the ports:

- Vendor Name
- Part Number
- Revision
- Serial Number
- Device Identifier
- Interface Type

Monitoring SFP Transceiver devices using web interface

To view the SFP Transceiver device information using Web interface, go to **System** > **Overview** > **Network Devices** and click on particular device. For more information about the displayed properties, see *iDRAC Online Help*.

The page name also displays the slot number where the transceiver device is available under Port statistics.

Monitoring data for SFP devices is only available for active SFPs. Following are the information displayed:

- TX Output Power
- TX Bias Current
- RX Input Power
- Vcc Voltage
- Temperature

Monitoring SFP Transceiver devices using RACADM

To view the SFP Transceiver device information using RACADM, use the `networktransceiverstatistics` command.

For more information, see the *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

Telemetry Streaming

Telemetry enables users to collect and stream real-time device metrics, events, and data logs from a PowerEdge server to a subscribed external client or server application. Using Telemetry, you can set the type and frequency of reports that needs to be generated.

NOTE: The feature is supported on all the platforms and it requires iDRAC Datacenter license.

Telemetry is one-to-many solution for collecting and streaming the live system data from one or more PowerEdge servers (iDRAC) to a centralized 'Remote Server Monitoring, Analysis, and Alerting service'. The feature also supports on-demand data collection of the data.

The telemetry data includes metrics/inventory and logs/events. The data can be streamed (pushed out) or collected (pulled) from iDRAC to or by remote consumers like Redfish client and Remote Syslog Server. The telemetry data is also provided to the iDRAC SupportAssist data collector on demand. The data collection and report is based on predefined Redfish telemetry metrics, trigger, and report definitions. The telemetry streaming settings can be configured using iDRAC web interface, RACADM, Redfish, and Server Configuration Profile (SCP).

To configure Telemetry, enable or select the required device reports or logs that define the behavior and frequency of data streaming. Go to **Configuration** > **System Settings** page to configure Telemetry. Data streaming is automatic until the Telemetry is disabled.

Following table describes the metric reports that can be generated using telemetry:

Type	Metric Group	Inventory	Sensor	Statistics	Configuration	Metrics
I/O Devices	NICs	No	Yes	Yes	No	No
	FC HBAs	No	Yes	Yes	No	No
Server Devices	CPUs	No	Yes	No	No	Yes
	Memory	No	Yes	No	No	Yes
	Fans	No	Yes	No	No	No
	PSUs	No	No	No	No	Yes
	Sensors	No	Yes	No	No	No
Environmental	Thermal	No	Yes	No	No	Yes
	Power	No	No	Yes	No	Yes
	Performance	No	No	Yes	No	No
Accelerators	GPUs	No	No	Yes	No	Yes

To know about the field descriptions of Telemetry section, see *iDRAC Online Help*.

NOTE:

- StorageDiskSMARTDATA is only supported on SSD drives with SAS/SATA bus protocol and behind the BOSS controller.
- StorageSensor data is reported only for the drives in Ready / Online / Non-RAID mode and not behind the BOSS controller.
- NVMeSMARTData is only supported for SSD (PCIeSSD / NVMe Express) drives with PCIe bus protocol (not behind SWRAID).
- GPGPUStatistics data is only available in specific GPGPU models that support ECC memory capability.
- PSUMetrics is not available on modular platforms.
- Fan Power and PCIe Power Metrics may be displayed as 0 for some platforms.
- CUPS report has been renamed to SystemUsage in 4.40.00.00 release and it's supported on both INTEL and AMD platforms.

Telemetry Workflow:

1. Install Datacenter license, if not installed already.
2. Configure global Telemetry settings including Enabling the telemetry and Rsyslog server network address and port using RACADM, Redfish, SCP, or iDRAC GUI.
3. Configure the following Telemetry report streaming parameters on the required device report or log using either RACADM or Redfish interface:
   - EnableTelemetry
   - ReportInterval
   - ReportTriggers

   NOTE: Enable iDRAC Alerts and Redfish events for the specific hardware for which you need telemetry reports.
4. Redfish client makes subscription request to the Redfish EventService on iDRAC.
5. iDRAC generates and pushes the metric report or log/event data to the subscribed client when the predefined trigger conditions are met.

Feature Constraints:

1. For security reasons, iDRAC supports only HTTPS-based communication to the client.
2. For stability reasons, iDRAC supports up to eight subscriptions.
3. Deletion of subscriptions is supported through Redfish interface only, even for the manual deletion by the Admin.

Behavior of Telemetry feature:

- iDRAC generates and pushes (HTTP POST) the Metric Report or log/event data to all the subscribed clients to the destination specified in the subscription when the predefined trigger conditions are met. The clients receive new data only upon successful subscription creation.
- The metric data includes the timestamp in ISO format, UTC time (ends in 'Z'), at the time of data collection from source.
- Clients can terminate a subscription by sending an HTTP DELETE message to the URI of the subscription resource through the Redfish interface.
- If the subscription is deleted either by iDRAC or the client, then iDRAC does not send (HTTP POST) reports. If the number of delivery errors exceeds predefined thresholds, then iDRAC may delete a subscription.
- If a user has Admin privilege, they can delete the subscriptions but only through Redfish interface.
- Client is notified about the termination of a subscription by iDRAC by sending 'Subscription terminated' event as the last message.
- Subscriptions are persistent and can remain even after iDRAC restarts. But, they can be deleted either by performing `racresetcfg` or LCwipe operations.
- User interfaces like RACADM, Redfish, SCP, and iDRAC display the current status of the client subscriptions.

Captura de datos en serie

iDRAC le permite capturar la redirección en serie de la consola para su posterior recuperación con el uso de la función de captura de datos en serie. Para esta función, se requiere la licencia iDRAC Datacenter.

El propósito de la función de captura de datos en serie es capturar los datos en serie del sistema y almacenarlos para que el cliente pueda recuperarlos posteriormente para fines de depuración.

Puede habilitar o deshabilitar la captura de datos en serie mediante las interfaces de RACADM, Redfish e iDRAC. Cuando se habilita este atributo, la iDRAC captura el tráfico en serie recibido en el dispositivo en serie del host 2, independientemente de la configuración del modo MUX en serie.

Para habilitar/deshabilitar la captura de datos en serie mediante la GUI de iDRAC, vaya a la página **Mantenimiento** > **Diagnósticos** > **Registros de datos en serie** y marque la casilla para habilitar o deshabilitar.

NOTA:
- Este atributo se mantiene después del reinicio de la iDRAC.
- El restablecimiento del firmware al valor predeterminado desactivará esta función.
- Mientras la captura de datos en serie esté habilitada, el búfer mantiene la adición de datos recientes. Si el usuario deshabilita la captura en serie y la vuelve a habilitar, se comienza a agregar la iDRAC desde la última actualización.

La captura de datos en serie del sistema se inicia cuando el usuario habilita la marca de captura de datos en serie en cualquiera de las interfaces. Si la captura de datos en serie se activa después de que haya arrancado el sistema, deberá reiniciarlo a fin de que el BIOS pueda procesar el nuevo ajuste (Redirección de consola solicitada por iDRAC) para obtener los datos en serie. iDRAC comenzará la captura de datos continuamente y los almacenará en la memoria compartida con un límite de 512 KB. Este búfer será circular.

NOTA:
- Para que esta función sea útil, debe contar con privilegios de inicio de sesión y privilegios de control del sistema.
- Para esta función, se requiere la licencia iDRAC Datacenter.

Configuración dinámica de las direcciones virtuales, del iniciador y del destino de almacenamiento

De manera dinámica, es posible ver y configurar los ajustes de dirección virtual, iniciador y destino de almacenamiento, así como aplicar una política de persistencia. Esto le permite a la aplicación implementar la configuración según los cambios en el estado de la alimentación (es decir, reinicio de sistema operativo, restablecimiento flexible, restablecimiento en frío o ciclo de CA) y también en función de la configuración de la política de persistencia para ese estado de la alimentación. Esto proporciona más flexibilidad en las implementaciones donde se necesita una reconfiguración rápida de las cargas de trabajo de un sistema a otro.

Las direcciones virtuales son:
- Dirección MAC virtual
- Dirección MAC de iSCSI virtual
- Dirección MAC de FIP virtual

- WWN virtual
- WWPN virtual

NOTA: Al borrar la política de persistencia, todas las direcciones virtuales se restablecen a la dirección permanente predeterminada de fábrica.

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

Es posible que los valores configurados para las direcciones virtuales, el iniciador y los destinos de almacenamiento varíen en función de la forma en que se maneja la alimentación principal durante el restablecimiento del sistema y si los dispositivos NIC, CNA o HBA 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 la iDRAC.

Las políticas de persistencia surten efecto únicamente si la función de identidad de E/S se encuentra habilitada. 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 43. Tarjetas admitidas para la optimización de la identidad de E/S

Fabricante	Tipo
Broadcom	• 5719 Mezz de 1 GB • 5720 PCIe de 1 GB • 5720 bNDC de 1 GB • 5720 rNDC de 1 GB • 57414 PCIe de 25 GbE
Intel	• i350 DP FH PCIe de 1 GB • i350 QP PCIe de 1 GB • i350 QP rNDC de 1 GB • i350 Mezz de 1 GB • i350 bNDC de 1 GB • x520 PCIe de 10 GB • x520 bNDC de 10 GB • x520 Mezz de 10 GB • x520 + i350 rNDC de 10 GB+1 GB • X710 bNDC de 10 GB • X710 QP bNDC de 10 GB • X710 PCIe de 10 GB • X710 + I350 rNDC de 10 GB+1 GB • X710 rNDC de 10 GB • XL710 QSFP DP LP PCIe de 40 GE • XL710 QSFP DP FH PCIe de 40 GE • X550 DP BT PCIe 2 x 10 Gb • X550 DP BT LP PCIe 2 x 10 Gb • XXV710 Fab A/B Mezz de 25 Gb (*para plataformas MX*)
Mellanox	• ConnectX-3 Pro 10G Mezz de 10 GB • ConnectX-4 LX 25GE SFP DP rNDC de 25 GB

Tabla 43. Tarjetas admitidas para la optimización de la identidad de E/S (continuación)

Fabricante	Tipo
	• ConnectX-4 LX 25GE DP FH PCIe de 25 GB • ConnectX-4 LX 25GE DP LP PCIe de 25 GB • ConnectX-4 LX Fab A/B Mezz de 25 GB (*para plataformas MX*)
QLogic	• 57810 PCIe de 10 GB • 57810 bNDC de 10 GB • 57810 Mezz de 10 GB • 57800 rNDC de 10 GB+1 GB • 57840 rNDC de 10 GB • 57840 bNDC de 10 GB • 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 • QME2692-DEL Fab C Mezz FC16 (*para plataformas MX*) • QME2742-DEL Fab C Mezz FC32 (*para plataformas MX*) • QL41262HMKR-DE Fab A/B Mezz de 25 Gb (*para plataformas MX*) • QL41232HMKR-DE Fab A/B Mezz de 25 Gb (*para plataformas MX*) • QLogic 1x32Gb QLE2770 FC HBA • QLogic 2x32Gb QLE2772 FC HBA
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 • LPe32002-M2-D DP PCIe FC32 • LPe31002-D Fab C Mezz FC16 (*para plataformas MX*) • LPe32002-D Fab C Mezz FC32 (*para plataformas MX*) • LPe35002-M2 FC32 de 2 puertos • LPe35000-M2 FC32 de 1 puertos

Versiones del firmware de la NIC compatibles para la optimización de la identidad de E/S

En los servidores Dell PowerEdge de 14.ª generación, el firmware de NIC necesario se encuentra disponible de manera predeterminada.

La siguiente tabla proporciona las versiones del firmware de la NIC para la función de optimización de la identidad de E/S.

Comportamiento de la dirección virtual/asignada de manera remota y de la política de persistencia cuando iDRAC está configurado en

el modo de dirección asignada de manera remota o en el modo de consola

En la siguiente tabla, se describe la configuración de administración de direcciones virtuales (VAM) y el comportamiento de la política de persistencia, y las dependencias.

Tabla 44. Comportamiento de la dirección virtual/asignada de manera remota y de la política de persistencia

Estado de la función Dirección asignada de manera remota en OME Modular	Modo establecido en iDRAC	Estado de la función de identidad de E/S en el iDRAC	SCP	Política de persistencia	Borrar Persistence Policy - Dirección virtual
Dirección asignada de manera remota activada	Modo RemoteAssignedAddress	Activado	Administración de direcciones virtuales (VAM) configurada	VAM configurada persiste	Establecer valor en dirección asignada de manera remota
Dirección asignada de manera remota activada	Modo RemoteAssignedAddress	Activado	VAM no configurada	Establecer valor en dirección asignada de manera remota	Sin persistencia: se establece en dirección asignada de manera remota
Dirección asignada de manera remota activada	Modo Dirección asignada de manera remota	Desactivado	Configurado mediante la ruta de acceso proporcionada en Lifecycle Controller	Establecer valor en dirección asignada de manera remota para ese ciclo	Sin persistencia: se establece en dirección asignada de manera remota
Dirección asignada de manera remota activada	Modo Dirección asignada de manera remota	Desactivado	VAM no configurada	Establecer valor en dirección asignada de manera remota	Establecer valor en dirección asignada de manera remota
Dirección asignada de manera remota desactivada	Modo Dirección asignada de manera remota	Activado	VAM configurada	VAM configurada persiste	Persistencia: el borrado no es posible
Dirección asignada de manera remota desactivada	Modo Dirección asignada de manera remota	Activado	VAM no configurada	Establecer en dirección MAC de hardware	No se admite persistencia. Depende del comportamiento de la tarjeta
Dirección asignada de manera remota desactivada	Modo Dirección asignada de manera remota	Desactivado	Configurado mediante la ruta de acceso proporcionada en Lifecycle Controller	La configuración de Lifecycle Controller persiste durante ese ciclo	No se admite persistencia. Depende del comportamiento de la tarjeta
Dirección asignada de manera remota desactivada	Modo Dirección asignada de manera remota	Desactivado	VAM no configurada	Establecer en dirección MAC de hardware	Establecer en dirección MAC de hardware
Dirección asignada de manera remota activada	Modo de consola	Activado	VAM configurada	VAM configurada persiste	Persistencia y borrado deben funcionar
Dirección asignada de manera remota activada	Modo de consola	Activado	VAM no configurada	Establecer en dirección MAC de hardware	Establecer en dirección MAC de hardware
Dirección asignada de manera remota activada	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 persistencia. Depende del comportamiento de la tarjeta

Tabla 44. Comportamiento de la dirección virtual/asignada de manera remota y de la política de persistencia (continuación)

Estado de la función Dirección asignada de manera remota en OME Modular	Modo establecido en iDRAC	Estado de la función de identidad de E/S en el iDRAC	SCP	Política de persistencia	Borrar Persistence Policy - Dirección virtual
Dirección asignada de manera remota desactivada	Modo de consola	Activado	VAM configurada	VAM configurada persiste	Persistencia y borrado deben funcionar
Dirección asignada de manera remota desactivada	Modo de consola	Activado	VAM no configurada	Establecer en dirección MAC de hardware	Establecer en dirección MAC de hardware
Dirección asignada de manera remota 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 persistencia. Depende del comportamiento de la tarjeta
Dirección asignada de manera remota activada	Modo de consola	Desactivado	VAM no configurada	Establecer en dirección MAC de hardware	Establecer en dirección MAC de hardware

Comportamiento del sistema para FlexAddress e identidad de E/S

Tabla 45. Comportamiento del sistema para FlexAddress y la identidad de E/S

Tipo	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
			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 perfil de configuración del servidor de iDRAC, modifique los atributos necesarios de la identidad de E/S en el archivo SCP e importe el archivo nuevamente a la iDRAC.

Para obtener la lista de atributos de Optimización de la identidad de E/S que puede modificar en el archivo SCP, consulte el documento *Perfil de NIC* disponible en https://www.dell.com/support.

NOTA: No modifique los atributos que no corresponden a la optimización de la identidad de E/S.

Habilitación o deshabilitación 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 la 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 identidad de E/S)** y seleccione la opción **Enable (Habilitar)** para habilitar esta función. Para deshabilitarla, anule la selección.
3. Haga clic en **Aplicar** para aplicar la configuración.

Habilitación o deshabilitación 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
```

Umbral de desgaste de SSD

iDRAC le proporciona la capacidad de configurar los umbrales de resistencia de escritura nominal restante para todos los SSD y el repuesto disponible de los SSD de PCIe NVMe.

Cuando la resistencia de escritura nominal restante del SSD y el repuesto disponible del SSD de PCIe NVMe disponibles son menores que el umbral, iDRAC registra este evento en el registro de LC y según la selección de tipo de alerta, iDRAC también realiza la alerta por correo electrónico, la captura de SNMP, la alerta de IPMI, el inicio de sesión en el syslog remoto, el evento de WS y el registro del sistema operativo.

iDRAC alerta al usuario cuando la resistencia de escritura nominal restante del SSD se encuentra por debajo del umbral establecido, de modo que el administrador del sistema pueda crear un respaldo de la unidad SSD o reemplazarla.

En el caso de los SSD de PCIe NVMe, el iDRAC muestra el **repuesto disponible** y proporciona un umbral para advertir. El **repuesto disponible** no está disponible para los SSD que están conectados detrás de PERC y HBA.

Configuración de las funciones de alerta del umbral de desgaste de SSD mediante la interfaz web

Para configurar la resistencia de escritura nominal restante y el umbral de alerta de repuesto disponible mediante la interfaz web:

1. En la interfaz web de iDRAC, vaya a **Configuración** > **Configuración del sistema** > **Configuración de hardware** > **Umbrales de desgaste de SSD**.
   Aparece la página **Umbrales de desgaste de SSD**.
2. **Resistencia de escritura nominal restante:** puede ajustar el valor entre 1 y 99 %. El valor predeterminado es 10 %.
   El tipo de alerta para esta función es **Resistencia de escritura del desgaste de SSD** y la alerta de seguridad es una **Advertencia** como resultado del evento del umbral.
3. **Umbral de alerta de repuesto disponible:** puede ajustar el valor entre 1 y 99 %. El valor predeterminado es 10 %.
   El tipo de alerta para esta función es **Repuesto disponible para desgaste de SSD** y la alerta de seguridad es una **Advertencia** como resultado del evento del umbral.

Configuración de las funciones de alerta de umbral de desgaste de SSD mediante RACADM

Para configurar la resistencia de escritura nominal restante, utilice el comando:

```
racadm set System.Storage.RemainingRatedWriteEnduranceAlertThreshold n
```

, donde n= 1 a 99 %.

Para configurar el umbral de alerta de repuesto disponible, utilice el comando:

```
racadm System.Storage.AvailableSpareAlertThreshold n
```

, donde n= 1 a 99 %.

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 de **Política de persistencia** no funcione cuando se establece como predeterminada. Si el atributo **VirtualAddressManagement** está establecido como un modo **FlexAddress** (excepto para las plataformas MX) o **RemoteAssignedAddress** (para las plataformas MX) en iDRAC y si la función FlexAddress o dirección asignada de forma remota está desactivada en CMC (no para plataformas MX) u OME Modular (para plataformas MX), asegúrese de establecer el atributo **VirtualAddressManagement** en el modo **Consola** en iDRAC o de habilitar la función FlexAddress o dirección asignada de forma remota en CMC u OME Modular.

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 eventos de WS. Los registros también se incluyen en los registros del sistema remoto.

Valores predeterminados para la política de persistencia

Tabla 46. 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 una política persistente está deshabilitada y cuando realiza la acción para perder la dirección virtual, si vuelve a habilitar la política persistente, la dirección virtual no se recupera. Debe establecer la dirección virtual nuevamente después de habilitar la política persistente.

NOTA: Si hay una política de persistencia vigente y las direcciones virtuales, el iniciador o los destinos de almacenamiento se configuran en una partición de dispositivo CNA, no restablezca ni borre los valores configurados para las direcciones virtuales, el iniciador y los destinos de almacenamiento antes de cambiar el VirtualizationMode o la personalidad de la partición. La acción se llevará a cabo de forma automática cuando se deshabilite la política de persistencia. También puede usar 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, según se define en Valores predeterminados para el destino de almacenamiento y el iniciador iSCSI en la página 234.

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** > **Configuración de hardware** > **Optimización de 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.
   - **Restablecimiento mediante suministro de energía:** la dirección virtual o los valores de destino se conservan cuando se producen condiciones de reinicio 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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

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 47. 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	IPv6

Tabla 48. 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	

18

Managing storage devices

Starting with iDRAC 3.15.15.15 release, iDRAC supports Boot Optimized Storage Solution (BOSS) controller in the 14th generation of PowerEdge servers. BOSS controllers are designed specifically for booting the operating system of the server. These controllers support limited RAID features and the configuration is staged.

Starting with iDRAC 4.30.30.30 release, iDRAC supports PERC 11, HBA 11, and BOSS 1.5 for AMD systems.

NOTE: BOSS controllers support only RAID level1.

NOTE: For BOSS Controllers, the complete VD information may not be available when both PD's are plugged-out and plugged-in back.

NOTE: PERC 11 and later controllers support Hardware Root of Trust (RoT).

iDRAC has expanded its agent-free management to include direct configuration of the PERC controllers. It enables you to remotely configure the storage components attached to your system at run-time. These components include RAID and non-RAID controllers and the channels, ports, enclosures, and disks attached to them. For the PowerEdge Rx4xx/Cx4xx servers, PERC 9 and PERC 10 controllers are supported. For PowerEdge Rx5xx/Cx5xx AMD platform servers, PERC 11 is supported.

The complete storage subsystem discovery, topology, health monitoring, and configuration are accomplished in the Comprehensive Embedded Management (CEM) framework by interfacing with the internal and external PERC controllers through the MCTP protocol over I2C interface. For real-time configuration, CEM supports PERC9 controllers and above. The firmware version for PERC9 controllers must be 9.1 or later.

NOTE: The Software RAID (SWRAID) is not supported by CEM and thus is not supported in the iDRAC GUI. SWRAID can be managed using either RACADM, WSMAN or Redfish.

Using iDRAC, you can perform most of the functions that are available in OpenManage Storage Management including real-time (no reboot) configuration commands (for example, create virtual disk). You can completely configure RAID before installing the operating system.

You can configure and manage the controller functions without accessing the BIOS. These functions include configuring virtual disks and applying RAID levels and hot spares for data protection. You can initiate many other controller functions such as rebuilds and troubleshooting. You can protect your data by configuring data-redundancy or assigning hot spares.

The storage devices are:

- Controllers — Most operating systems do not read and write data directly from the disks, but instead send read and write instructions to a controller. The controller is the hardware in your system that interacts directly with the disks to write and retrieve data. A controller has connectors (channels or ports) which are attached to one or more physical disks or an enclosure containing physical disks. RAID controllers can span the boundaries of the disks to create an extended amount of storage space— or a virtual disk — using the capacity of more than one disk. Controllers also perform other tasks, such as initiating rebuilds, initializing disks, and more. To complete their tasks, controllers require special software known as firmware and drivers. In order to function properly, the controller must have the minimum required version of the firmware and the drivers installed. Different controllers have different characteristics in the way they read and write data and execute tasks. It is helpful to understand these features to most efficiently manage the storage.
- Physical disks or physical devices — Reside within an enclosure or are attached to the controller. On a RAID controller, physical disks or devices are used to create virtual disks.
- Virtual disk — It is storage created by a RAID controller from one or more physical disks. Although a virtual disk may be created from several physical disks, it is viewed by the operating system as a single disk. Depending on the RAID level used, the virtual disk may retain redundant data if there is a disk failure or have particular performance attributes. Virtual disks can only be created on a RAID controller.
- Enclosure — It is attached to the system externally while the backplane and its physical disks are internal.
- Backplane — It is similar to an enclosure. In a Backplane, the controller connector and physical disks are attached to the enclosure, but it does not have the management features (temperature probes, alarms, and so on) associated with external enclosures. Physical disks can be contained in an enclosure or attached to the backplane of a system.

NOTE: In any MX chassis which contains storage sleds and compute sleds, iDRAC pertaining to any of the compute sleds in that chassis will report all storage sleds (both assigned and unassigned). If any one of the assigned or unassigned blades are in Warning or Critical heath state, the blade controller also reports the same status.

In addition to managing the physical disks contained in the enclosure, you can monitor the status of the fans, power supply, and temperature probes in an enclosure. You can hot-plug enclosures. Hot-plugging is defined as adding of a component to a system while the operating system is still running.

The physical devices connected to the controller must have the latest firmware. For the latest supported firmware, contact your service provider.

Storage events from PERC are mapped to SNMP traps and WSMan events as applicable. Any changes to the storage configurations are logged in the Lifecycle Log.

Table 49. PERC capability

PERC Capability	CEM configuration Capable Controller (PERC 9.1 or later)	CEM configuration Non-capable Controller (PERC 9.0 and lower)
Real-time	**NOTE:** For PowerEdge Rx5xx/ Cx5xx servers, PERC 9, PERC 10, and PERC 11 controllers are supported. If there is no existing pending or scheduled jobs for the controller, then configuration is applied. If there are pending or scheduled jobs for that controller, then the jobs have to be cleared or you must wait for the jobs to be completed before applying the configuration at run-time. Run-time or real-time means, a reboot is not required.	Configuration is applied. An error message is displayed. Job creation is not successful and you cannot create real-time jobs using Web interface.
Staged	If all the set operations are staged, the configuration is staged and applied after reboot or it is applied at real-time.	Configuration is applied after reboot

Topics:

Comprensión de los conceptos de RAID

Storage Management utiliza la tecnología de arreglos redundantes de discos independientes (RAID) para proporcionar capacidad de administración del almacenamiento. Para entender Storage Management, es necesario conocer los conceptos de RAID y saber cómo las controladoras RAID y el sistema operativo perciben el espacio en disco en el sistema.

¿Qué es RAID?

RAID es una tecnología para administrar el almacenamiento de datos en discos físicos que residen en el sistema o están conectados a él. Un aspecto clave de RAID es la capacidad de distribuir los discos físicos de modo que la capacidad de almacenamiento combinada de varios discos físicos pueda ser tratada como un solo espacio de disco ampliado. Otro aspecto clave de RAID es la capacidad para mantener datos redundantes que pueden usarse para restaurar datos en caso de que un disco falle. RAID usa técnicas diferentes, como el seccionamiento, el duplicado 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 y escritura, protección de datos y capacidad de almacenamiento. No todos los niveles de RAID mantienen datos redundantes, es decir que, para algunos niveles de RAID, los datos perdidos no se pueden restaurar. La elección de un nivel de RAID depende de si la prioridad es el rendimiento, la protección o la capacidad de almacenamiento.

NOTA: El Consejo de asesoramiento sobre RAID (RAB) define las especificaciones que se utilizan para implementar la tecnología RAID. Aunque el RAB define los niveles de RAID, la implementación comercial de distintos proveedores puede variar con respecto a las especificaciones de RAID reales. La implementación de 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

El RAID puede implementarse mediante hardware o software. Un sistema que usa RAID de 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 de software que proporciona el sistema operativo, el sistema operativo es el que implementa los niveles RAID. Por esta razón, usar RAID de software por sí mismo puede reducir el rendimiento del sistema. Sin embargo, puede usar RAID de software junto con volúmenes RAID de hardware para proporcionar mejor rendimiento y variedad en la configuración de volúmenes RAID. Por ejemplo, puede duplicar un par de volúmenes RAID 5 de hardware entre dos controladoras RAID a fin de proporcionar redundancia de la controladora RAID.

Conceptos de RAID

RAID usa técnicas específicas para escribir datos en los discos. Estas técnicas permiten que RAID proporcione redundancia de datos o mejore el rendimiento. Estas técnicas incluyen las siguientes:

- Duplicado: Duplicación de datos de un disco físico a otro disco físico. El duplicado proporciona redundancia de datos al mantener dos copias de los mismos datos en discos físicos distintos. Si ocurre un error en uno de los discos del duplicado, el sistema puede continuar funcionando con el disco que no se ve afectado. Ambos lados del duplicado contienen siempre los mismos datos. Cualquier lado del duplicado puede actuar como el lado operativo. Un grupo de discos RAID duplicado es comparable en rendimiento con un grupo de discos RAID 5 respecto de las operaciones de lectura, pero es más rápido en las operaciones de escritura.
- Seccionamiento: El seccionamiento de discos escribe datos en todos los discos físicos en un disco virtual. Cada sección consta de direcciones de datos de disco virtual consecutivas que se asignan en unidades de tamaño fijo a cada disco físico en el 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 la 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: Espacio total en el disco consumido por una sección, sin incluir un disco de paridad. Por ejemplo, imagine una sección que contiene 64 KB de espacio en el disco y que tiene 16 KB de datos que residen en cada disco en la sección. En este caso, el tamaño de la sección es de 64 KB y el tamaño del elemento de la sección es de 16 KB.
- Elemento de la sección: un elemento de la sección es la porción de una sección que reside en un solo disco físico.
- Tamaño del elemento de la sección: Cantidad de espacio en el disco consumida por un elemento de la sección. Por ejemplo, imagine una sección que contiene 64 KB de espacio en el disco y que tiene 16 KB de datos que residen en cada disco en la sección. En este caso, el tamaño del elemento de la sección es de 16 KB y el tamaño de la sección es de 64 KB.
- Paridad: La paridad hace referencia a los datos redundantes que se mantienen utilizando un algoritmo en combinación con el seccionamiento. Cuando ocurre un error en uno de los discos seccionados, los datos se pueden reconstruir a partir de la información de paridad usando 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 duplicado, 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 de RAID para organizar el almacenamiento en disco. Algunos niveles de RAID mantienen datos redundantes para que usted pueda restaurar los datos después de una falla del disco. Los distintos niveles de 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. Mientras más discos se usen, mayor es la probabilidad de una falla de disco. A causa de las diferencias en la redundancia y el rendimiento de E/S, un nivel de RAID puede ser más adecuado 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 errores: La disponibilidad o tolerancia a errores se refiere a la capacidad de un sistema para mantener el funcionamiento y proporcionar acceso a los datos aun cuando uno de sus componentes falle. En los volúmenes de RAID, la disponibilidad o tolerancia a errores se logra manteniendo datos redundantes. Los datos redundantes incluyen 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 de RAID que elija. Algunos niveles de RAID pueden ser más adecuados para determinadas aplicaciones.
- Rentabilidad: El mantenimiento de datos redundantes o de información sobre paridad en relación con volúmenes de RAID exige espacio adicional en el disco. 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 errores (MTBF): El uso de discos adicionales para mantener la redundancia de los datos también aumenta la probabilidad de sufrir errores de disco en un cualquier momento. Aunque esto no se puede evitar en situaciones en las que los datos redundantes son una necesidad, realmente puede repercutir en la carga de trabajo del personal de asistencia de sistemas de la organización.
- Volumen: El volumen se refiere a un solo disco virtual que no es RAID. Puede crear volúmenes mediante utilidades externas, como 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 tenga espacio libre disponible.

Elección de niveles RAID

Es posible usar RAID para controlar el almacenamiento de datos en varios discos. Cada nivel o concatenación de RAID presenta características diferentes de rendimiento y protección de datos.

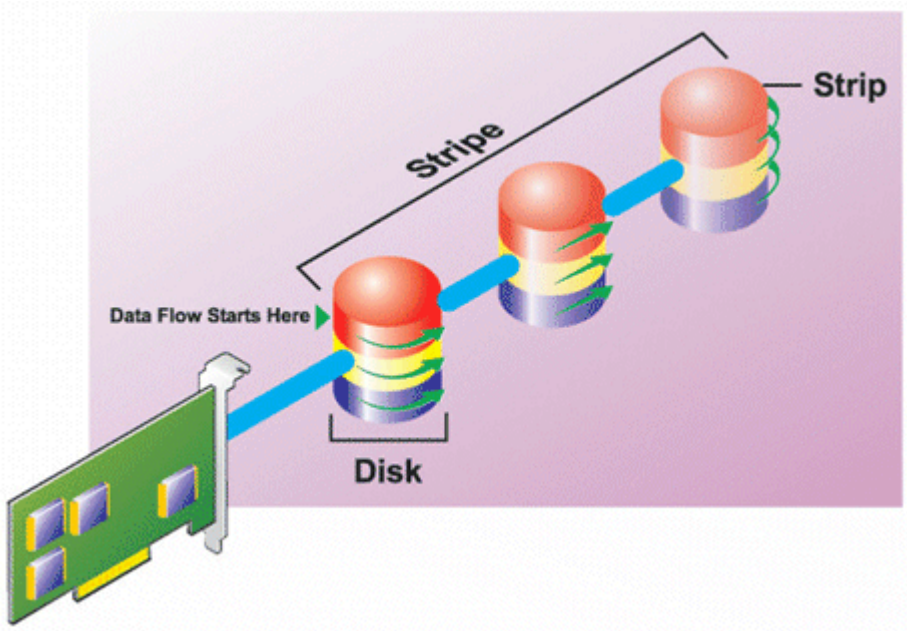
NOTA: Las controladoras PERC H3xx no admiten los niveles de RAID 6 y 60.

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)

RAID nivel 0: seccionamiento

RAID 0 utiliza el seccionamiento de datos, que consisten en escribir los datos en segmentos del mismo tamaño entre los discos físicos. RAID 0 no proporciona redundancia de datos.

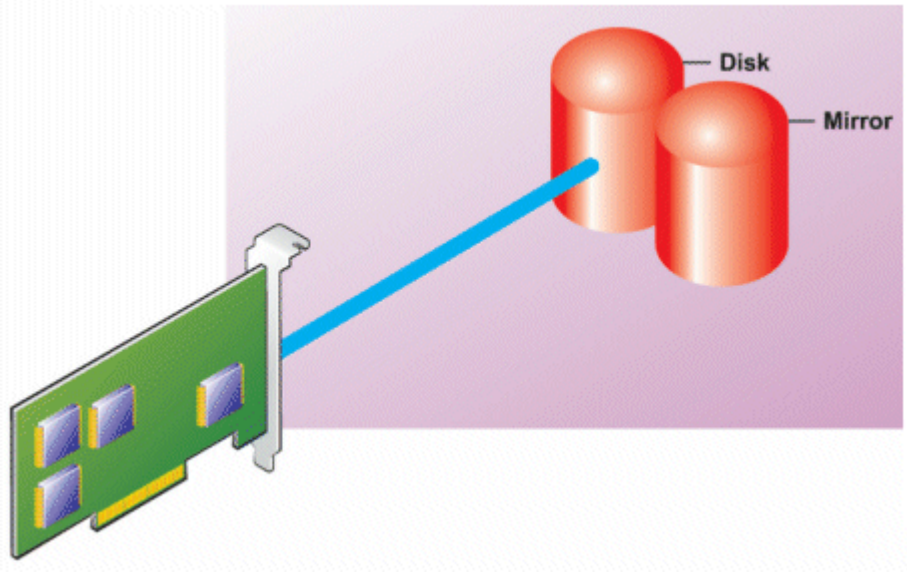


Características de RAID 0:

- Agrupa *n* discos en un disco virtual grande con una capacidad total de (tamaño de disco más pequeño)**n* discos.
- Los datos se guardan en los discos alternadamente.
- No se guardan datos redundantes. 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 1 de RAID (duplicado)

RAID 1 es la forma más sencilla de mantener datos redundantes. En RAID 1, los datos se duplican en uno o más discos físicos. Si un disco físico genera errores, los datos se pueden recrear utilizando los datos del otro lado del duplicado.



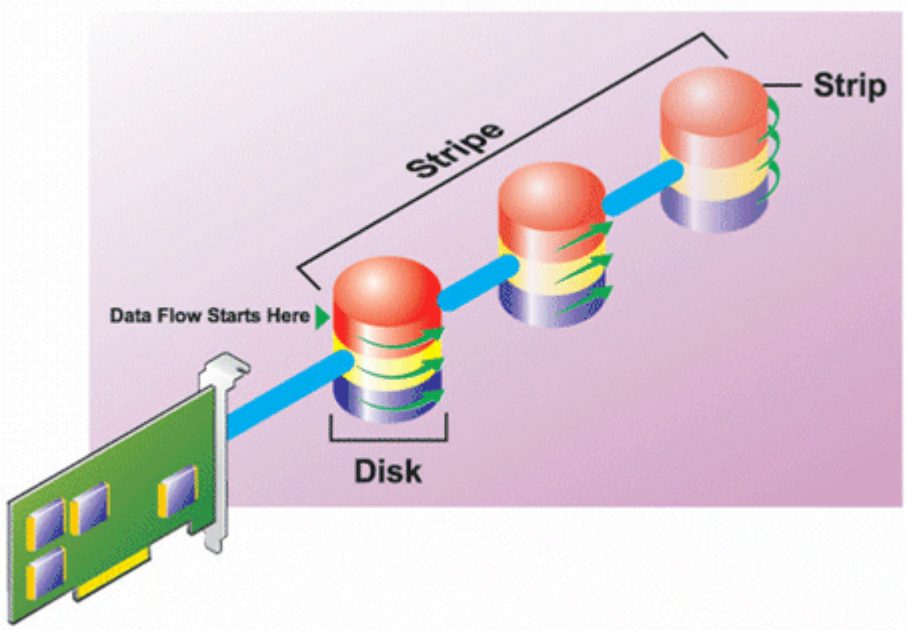
Características de RAID 1:

- Agrupa *n* + *n* discos en un disco virtual con capacidad de *n* discos. Las controladoras que actualmente admite Storage Management permiten seleccionar dos discos cuando se crea un RAID 1. Como estos discos se duplican, 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 duplicado del disco que falló.
- 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.

RAID de nivel 5 o seccionamiento con paridad distribuida

RAID 5 proporciona redundancia de datos al utilizar el seccionamiento de datos combinado con la información de paridad. Sin embargo, en vez de dedicar un disco físico a la paridad, la información de paridad está seccionada entre todos los discos físicos en el grupo de discos.

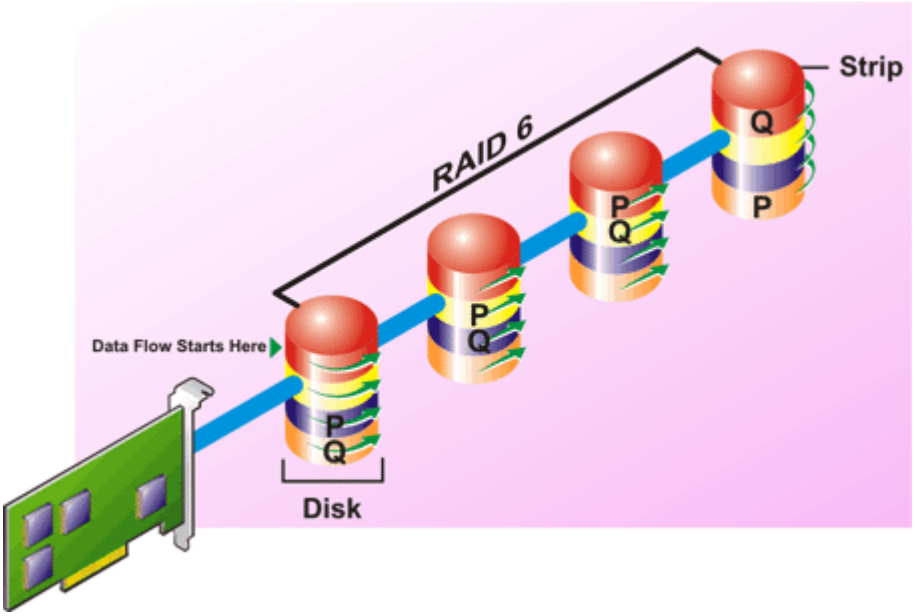


Características de RAID 5:

- Agrupa *n* discos en un disco virtual grande con capacidad de (*n*-1) discos.
- La información redundante (paridad) se almacena alternadamente entre todos los discos.
- Cuando un disco falla, el disco virtual seguirá funcionando, pero en estado degradado. Los datos se reconstruirán a partir de los discos que continúen funcionando.
- Mejor rendimiento de lectura, pero un rendimiento de escritura más lento.
- Hay redundancia para la protección de datos.

Nivel 6 de RAID (seccionamiento con paridad distribuida adicional)

RAID 6 proporciona redundancia de datos al utilizar el seccionamiento de datos combinado con la información de paridad. Al igual que en RAID 5, la paridad se distribuye en 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**.



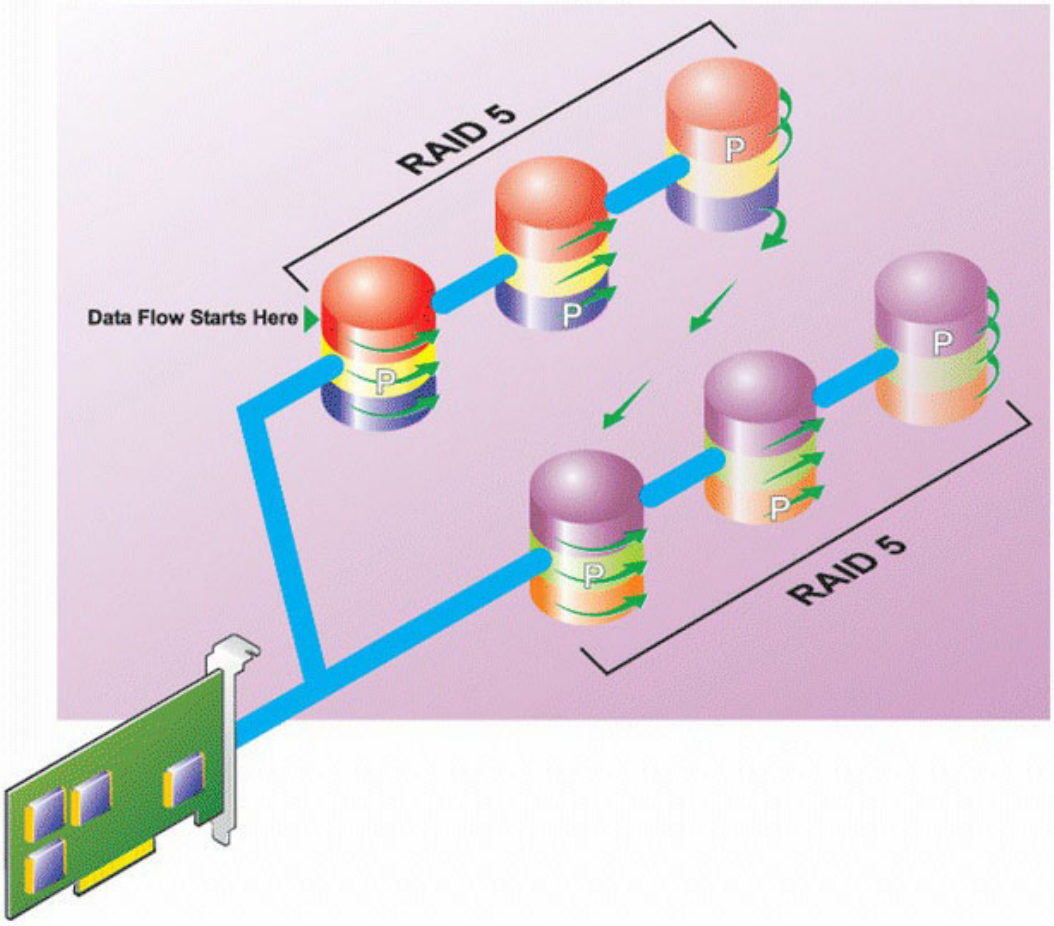
Características de RAID 6:

- 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 reconstruirán a partir de los discos que continúen funcionando.
- Mejor rendimiento de lectura, pero un rendimiento de escritura más lento.
- Mayor redundancia para la protección de datos.
- Se requieren dos discos por intervalo para la paridad. RAID 6 es más costoso en términos de espacio de disco.

RAID de nivel 50 (seccionamiento en conjuntos de RAID 5)

RAID 50 se utiliza para seccionar en más de un intervalo de discos físicos. Por ejemplo, un grupo de discos RAID 5 que se implementa 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 es directamente compatible. En este caso, puede implementar varios discos virtuales de RAID 5 y, luego, convertir los discos de RAID 5 en discos dinámicos. Después, puede crear un volumen dinámico que se extienda a todos los discos virtuales de RAID 5.

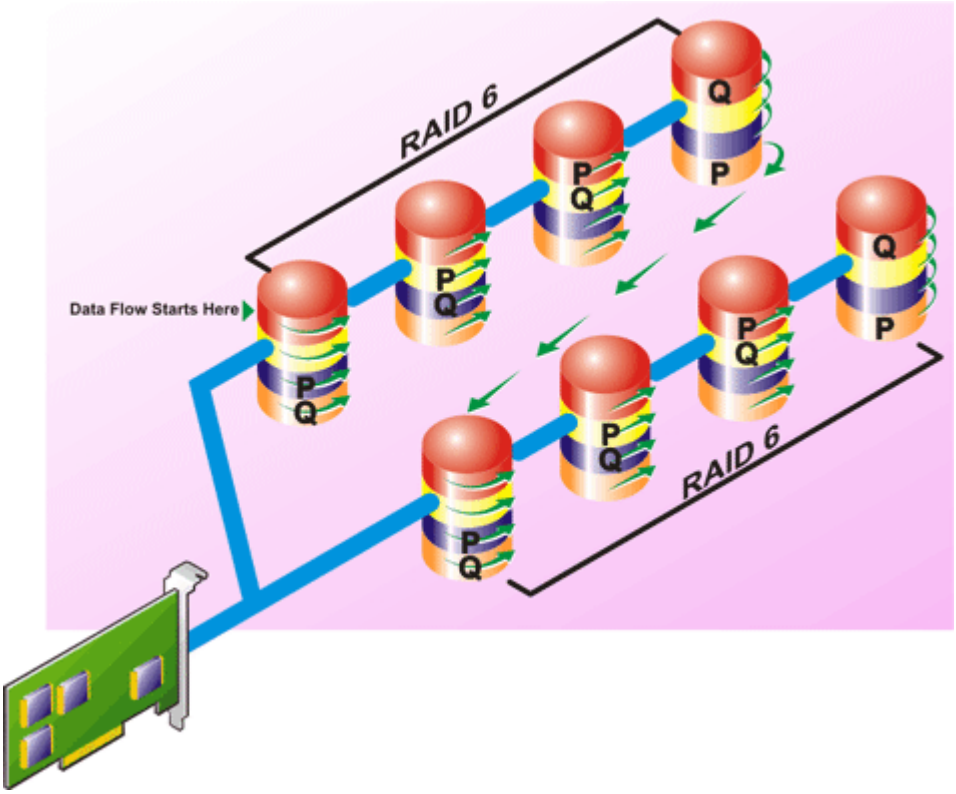


Características de RAID 50:

- Agrupa *n***s* discos para formar un disco virtual grande con capacidad de *s**(*n*-1) discos, en donde *s* representa el número de tramos y *n* es el número de discos dentro de cada tramo.
- La información redundante (paridad) se almacena alternadamente en todos los discos de cada tramo de RAID 5.
- Mejor rendimiento de lectura, pero un rendimiento de escritura más lento.
- Se requiere tanta información de paridad como en RAID 5 convencional.
- Los datos se seccionan en todos los intervalos. RAID 50 es más costoso en términos de espacio de disco.

RAID de nivel 60 (seccionamiento en conjuntos de RAID 6)

RAID 60 se utiliza para seccionar en más de un intervalo de discos físicos que están configurados como RAID 6. Por ejemplo, un grupo de discos RAID 6 que se implementa con cuatro discos físicos y, luego, continúa con un grupo de cuatro discos físicos adicionales sería un RAID 60.

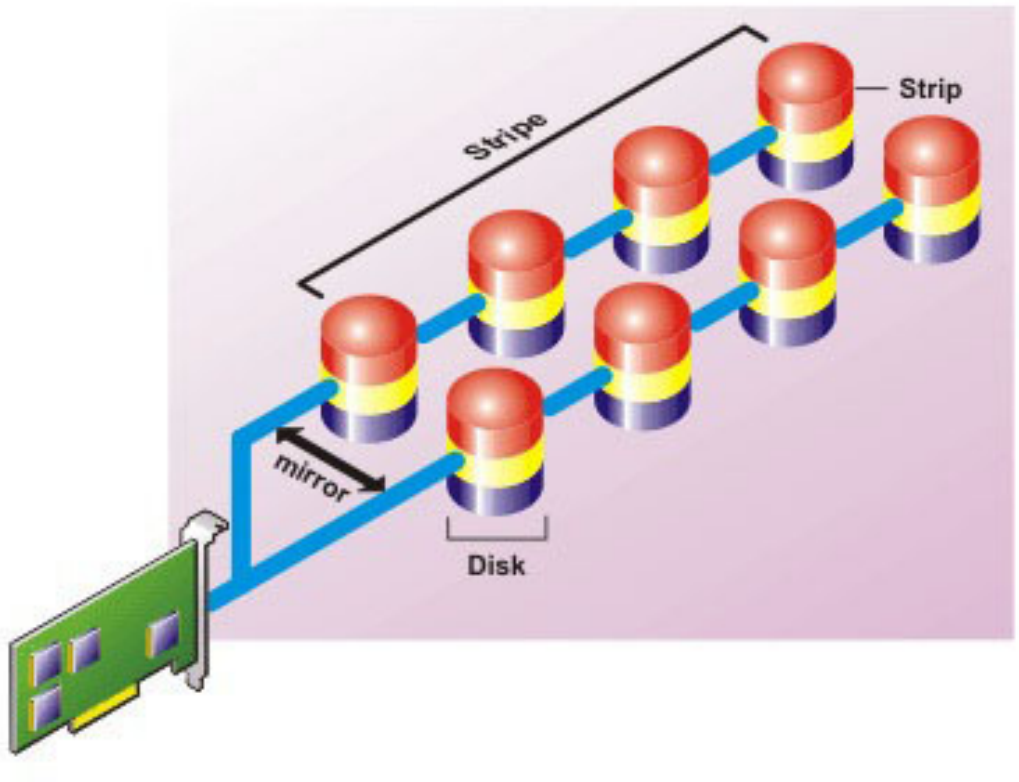


Características de RAID 60:

- 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 intervalo para la paridad. RAID 60 es más costoso en términos de espacio de disco.

RAID de nivel 10 (seccionamiento con duplicados)

RAB considera que RAID de nivel 10 es una implementación de RAID nivel 1. RAID 10 combina los discos físicos duplicados (RAID 1) con el seccionamiento de datos (RAID 0). Con RAID 10, los datos se seccionan entre varios discos físicos. Después, el grupo de discos seccionados se duplica en otro conjunto de discos físicos. RAID 10 se puede considerar un *duplicado 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 duplicadas de los datos son seccionadas entre conjuntos de discos físicos. Este nivel proporciona redundancia por medio del duplicado.
- Cuando un disco falla, el disco virtual continúa funcionando. Los datos se leen del disco duplicado 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 con los niveles RAID más comunes. Esta tabla proporciona pautas generales para seleccionar un nivel RAID. Evalúe los requisitos específicos de su entorno antes de seleccionar un nivel RAID.

Tabla 50. Comparación de rendimiento de niveles RAID

Nivel RAID	Redundancia 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.
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.

Tabla 50. Comparación de rendimiento de niveles RAID (continuación)

Nivel RAID	Redundancia de datos	Rendimiento de lectura	Rendimiento de escritura	Rendimiento de recreación	Discos mínimos requeridos	Usos sugeridos
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 fundamental. 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 fundamental. 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 BOSS:

- Adaptador BOSS-S1
- Modular BOSS-S1 (para servidores blade)
- Adaptador BOSS-S2

Las interfaces de iDRAC son compatibles con las siguientes controladoras PERC11:

- Adaptador PERC H755
- PERC H755 Front
- PERC H755N Front

Las interfaces de iDRAC son compatibles con las siguientes controladoras PERC10:

- Mini PERC H740P
- Adaptador PERC H740P
- PERC H840 adaptadora
- PERC H745P MX

Las interfaces de iDRAC son compatibles con las siguientes controladoras PERC9:

- Mini PERC H330
- Adaptador PERC H330
- Mini PERC H730P
- Adaptador PERC H730P

- PERC H730P MX

Controladoras no RAID admitidas

La interfaz de iDRAC es compatible con la controladora externa HBA SAS de 12 Gbps y las controladoras Mini o Adaptador HBA330.

iDRAC admite adaptadores HBA330 MMZ, HBA330 MX.

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: PERC H480 con versión 10.1 o posterior, el firmware admite hasta cuatro gabinetes por puerto.

Resumen de funciones admitidas para dispositivos de almacenamiento

En las siguientes tablas, se proporcionan las funciones admitidas por los dispositivos de almacenamiento a través de iDRAC.

Tabla 51. Funciones admitidas para las controladoras de almacenamiento

Función	PERC 11			PERC 10			PERC 9				
	H755 frontal	H755N frontal	Adaptador H755	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	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real
Convertir en RAID	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica
Convertir en RAID/no RAID,	En tiempo real (convierte la unidad en un volumen ePD-PT no RAID)	En tiempo real (convierte la unidad en un volumen ePD-PT no RAID)	En tiempo real (convierte la unidad en un volumen ePD-PT no RAID)	En tiempo real (solo se admite en el modo de controladora eHBA, convierte la unidad en un volumen	En tiempo real (solo se admite en el modo de controladora eHBA, convierte la unidad en un volumen	En tiempo real (solo se admite en el modo de controladora eHBA, convierte la unidad en un volumen	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real

Tabla 51. Funciones admitidas para las controladoras de almacenamiento (continuación)

Función	PERC 11			PERC 10			PERC 9				
	H755 frontal	H755N frontal	Adaptador H755	Mini H740P	Adaptador H740P	Adaptador H840	Mini H330	Adaptador H330	Mini H730P	Adaptador H730P	FD33xS
				no RAID ePD-PT)	no RAID ePD-PT)	no RAID ePD-PT)					
Recreación	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real
Cancelar recreación	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real
Crear discos virtuales	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real
Cambiar el nombre de los discos virtuales	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real
Editar las políticas de la caché de los discos virtuales	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real
Ejecutar una revisión de coherencia en el disco virtual	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real
Cancelar revisión de congruencia	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real
Inicializar discos virtuales	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real
Cancelar inicialización	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real
Cifrar discos virtuales	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	No aplica	No aplica	Tiempo real	Tiempo real	Tiempo real
Asignar o desasignar repuesto	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real

Tabla 51. Funciones admitidas para las controladoras de almacenamiento (continuación)

Función	PERC 11			PERC 10			PERC 9				
	H755 frontal	H755N frontal	Adaptador H755	Mini H740P	Adaptador H740P	Adaptador H840	Mini H330	Adaptador H330	Mini H730P	Adaptador H730P	FD33xS
s dinámicos dedicados											
Eliminar discos virtuales	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real
Cancelar la inicialización en segundo plano	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real
Expansión de la capacidad en línea	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real
Migración de nivel de RAID	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real
Descarte de caché preservada	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	No aplica	No aplica	Tiempo real	Tiempo real	Tiempo real
Establecer modo de lectura de patrullaje	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real
Modo de lectura de patrullaje manual	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real
Áreas de lectura de patrullaje no configuradas	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	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)
Modo de revisión de coherencia	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real

Tabla 51. Funciones admitidas para las controladoras de almacenamiento (continuación)

Función	PERC 11			PERC 10			PERC 9				
	H755 frontal	H755N frontal	Adaptador H755	Mini H740P	Adaptador H740P	Adaptador H840	Mini H330	Adaptador H330	Mini H730P	Adaptador H730P	FD33xS
Modo de escritura diferida	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real
Modo de equilibrio de carga	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real
Porcentaje de revisión de congruencia	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real
Porcentaje de recreación	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real
Porcentaje de inicialización de segundo plano	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real
Porcentaje de reconstrucción	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real
Importar configuración ajena	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real
Importar configuración ajena automáticamente	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real
Borrar configuración ajena	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real
Restablecer configuración de la controladora	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real
Crear o cambiar claves de	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	No aplica	No aplica	Tiempo real	Tiempo real	Tiempo real

Tabla 51. Funciones admitidas para las controladoras de almacenamiento (continuación)

Función	PERC 11			PERC 10			PERC 9				
	H755 frontal	H755N frontal	Adaptador H755	Mini H740P	Adaptador H740P	Adaptador H840	Mini H330	Adaptador H330	Mini H730P	Adaptador H730P	FD33xS
seguridad											
Administrador de clave empresarial segura	Organizado en etapas	Organizado en etapas	Organizado en etapas	Organizado en etapas	Organizado en etapas	Organizado en etapas	No aplica	No aplica	No aplica	No aplica	No aplica
Inventario y supervisar de forma remota la condición de los dispositivos SSD PCIe	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica
Preparar para quitar SSD PCIe	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica
Borrar los datos de manera segura para SSD PCIe	No aplica	Tiempo real	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica
Configurar el modo backplane (dividido / unificado)	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real
Hacer parpadear o dejar de hacer parpadear LED de componentes	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real	Tiempo real

Tabla 51. Funciones admitidas para las controladoras de almacenamiento (continuación)

Función	PERC 11			PERC 10			PERC 9				
	H755 frontal	H755N frontal	Adaptador H755	Mini H740P	Adaptador H740P	Adaptador H840	Mini H330	Adaptador H330	Mini H730P	Adaptador H730P	FD33xS
Cambiar modo de la controladora	No aplica	No aplica	No aplica	Organizado en etapas	Organizado en etapas	Organizado en etapas	Organizado en etapas	Organizado en etapas	Organizado en etapas	Organizado en etapas	Organizado en etapas
Compatibilidad de T10PI para discos virtuales	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica

NOTA: Se agregó compatibilidad con lo siguiente:

- modo eHBA para PERC versión de firmware 10.2 o posterior, el cual admite la conversión a discos no RAID
- conversión de controladora al modo HBA
- tramo desigual en RAID 10

Tabla 52. Funciones admitidas de las controladoras de almacenamiento para plataformas MX

Características	PERC 11	PERC 10	PERC 9
	H755 MX	H745P MX	H730P MX
Inicializar discos virtuales	Tiempo real	Tiempo real	Tiempo real
Cancelar inicialización	Tiempo real	Tiempo real	Tiempo real
Cifrar discos virtuales	Tiempo real	Tiempo real	Tiempo real
Asignar o desasignar repuestos dinámicos dedicados	Tiempo real	Tiempo real	Tiempo real
Eliminar discos virtuales	Tiempo real	Tiempo real	Tiempo real
Cancelar la inicialización en segundo plano	Tiempo real	Tiempo real	Tiempo real
Expansión de la capacidad en línea	Tiempo real	Tiempo real	Tiempo real
Migración de nivel de RAID	Tiempo real	Tiempo real	Tiempo real
Descarte de caché preservada	Tiempo real	Tiempo real	Tiempo real
Establecer modo de lectura de patrullaje	Tiempo real	Tiempo real	Tiempo real
Modo de lectura de patrullaje manual	Tiempo real	Tiempo real	Tiempo real
Áreas de lectura de patrullaje no configuradas	Tiempo real	Tiempo real	Tiempo real (solo en la interfaz de web)
Modo de revisión de coherencia	Tiempo real	Tiempo real	Tiempo real
Modo de escritura diferida	Tiempo real	Tiempo real	Tiempo real
Modo de equilibrio de carga	Tiempo real	Tiempo real	Tiempo real

Tabla 52. Funciones admitidas de las controladoras de almacenamiento para plataformas MX (continuación)

Características	PERC 11	PERC 10	PERC 9
	H755 MX	H745P MX	H730P MX
Porcentaje de revisión de congruencia	Tiempo real	Tiempo real	Tiempo real
Porcentaje de recreación	Tiempo real	Tiempo real	Tiempo real
Porcentaje de inicialización de segundo plano	Tiempo real	Tiempo real	Tiempo real
Porcentaje de reconstrucción	Tiempo real	Tiempo real	Tiempo real
Importar configuración ajena	Tiempo real	Tiempo real	Tiempo real
Importar configuración ajena automáticamente	Tiempo real	Tiempo real	Tiempo real
Borrar configuración ajena	Tiempo real	Tiempo real	Tiempo real
Restablecer configuración de la controladora	Tiempo real	Tiempo real	Tiempo real
Crear o cambiar claves de seguridad	Tiempo real	Tiempo real	Tiempo real
Inventario y supervisar de forma remota la condición de los dispositivos SSD PCIe	Tiempo real	No aplica	No aplica
Preparar para quitar SSD PCIe	No aplica	No aplica	No aplica
Borrar los datos de manera segura para SSD PCIe	Tiempo real	No aplica	No aplica
Configurar el modo backplane (dividido/unificado)	Tiempo real	No aplica	No aplica
Hacer parpadear o dejar de hacer parpadear LED de componentes	Tiempo real	Tiempo real	Tiempo real
Cambiar modo de la controladora	No aplica	No aplica	Organizado en etapas
Compatibilidad de T10PI para discos virtuales	No aplica	No aplica	No aplica

NOTA: H745P MX admite el modo eHBA con PERC 10.2 y superior.

Tabla 53. Funciones admitidas para los dispositivos de almacenamiento

Función	SSD PCIe	BOSS S1	BOSS S2
Crear discos virtuales	No aplica	Organizado en etapas	Organizado en etapas
Restablecer configuración de la controladora	No aplica	Organizado en etapas	Organizado en etapas
Inicialización rápida	No aplica	Organizado en etapas	Organizado en etapas
Eliminar discos virtuales	No aplica	Organizado en etapas	Organizado en etapas
Full Initialization (Inicialización completa)	No aplica	No aplica	No aplica
Inventario y supervisar de forma remota la condición	Tiempo real	No aplica	No aplica

Tabla 53. Funciones admitidas para los dispositivos de almacenamiento (continuación)

Función	SSD PCIe	BOSS S1	BOSS S2
de los dispositivos SSD PCIe			
Preparar para quitar SSD PCIe	Tiempo real	No aplica	No aplica
Borrar los datos de manera segura para SSD PCIe	Organizado en etapas	No aplica	No aplica
Hacer parpadear o dejar de hacer parpadear LED de componentes	Tiempo real	No aplica	Tiempo real
Conexión directa de unidades	Tiempo real	No aplica	Tiempo real

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, controladoras BOSS 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 excepciones de SNMP para los sucesos de almacenamiento. Los errores se registran en el registro de Lifecycle.

NOTA:

- Si enumera la vista del gabinete del comando WSMan 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**.
- Para obtener un inventario exacto de las controladoras BOSS, asegúrese de haber finalizado Recopilar inventario del sistema al reiniciar la operación (CSIOR). CSIOR se activa de manera predeterminada.
- La recopilación de la condición de almacenamiento sigue la misma convención del producto Dell EMC OpenManage. Para obtener más información, consulte *Guía del usuario de OpenManage Server Administrator* disponible en https://www.dell.com/openmanagemanuals.
- Los discos físicos en el sistema con varios planos posteriores se pueden incluir con otro plano posterior. Utilice la función parpadear para identificar los discos.
- Es posible que el valor de FQDD de determinados backplanes no sea el mismo en el inventario de software y el de hardware.
- El registro del ciclo de vida útil de la controladora PERC no está disponible cuando se procesan los eventos de la controladora de PERC anterior y esto no afecta la funcionalidad. El procesamiento de eventos pasados puede variar según la configuración

Supervisión de dispositivos de red mediante la interfaz web

Para ver la información del dispositivo de almacenamiento utilizando la interfaz web, realice lo siguiente:

- Vaya a **Almacenamiento** > **Descripción general** > **Resumen** para ver el resumen de los componentes de almacenamiento y los eventos registrados recientemente. Esta página se actualiza automáticamente cada 30 segundos.

- Vaya a **Almacenamiento** > **Descripción general** > **Controladoras** para ver la información de la controladora RAID. Aparecerá la página **Controladoras**.
- Vaya a **Almacenamiento** > **Descripción general** > **Discos físicos** para ver la información del disco físico. Aparecerá la página **Discos físicos**.
- Vaya a **Almacenamiento** > **Descripción general** > **Discos virtuales** para ver la información del disco virtual. Aparecerá la página **Discos virtuales**.
- Vaya a **Almacenamiento** > **Descripción general** > **Gabinetes** para ver la información sobre el gabinete. Aparecerá la página **Gabinetes**.

También puede utilizar filtros para ver información de un dispositivo específico.

NOTA:

- La lista de hardware de almacenamiento no se visualiza si el sistema no tiene dispositivos de almacenamiento compatibles con CEM.
- El comportamiento de los dispositivos NVMe no certificados por Dell o de terceros puede no ser coherente en iDRAC.
- Si las SSD NVMe de la ranura de plano posterior admiten los comandos NVMe-MI y la conexión I2C está en buen estado, iDRAC detectará estas SSD NVMe y las registrarás en las interfaces, independientemente de las conexiones PCI de las ranuras de plano posterior respectivas.

NOTA:

Tipo	Compatibilidad con la GUI web	Compatibilidad con otras interfaces
SATA	No disponible	Inventario y configuración de RAID
NVMe	Solo inventario de discos físicos	Inventario y configuración de RAID

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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

Supervisión de plano posterior mediante la utilidad de configuración de iDRAC

En la utilidad de configuración de la iDRAC, vaya a **System Summary (Resumen del sistema)**. Aparecerá la página **iDRAC Settings System Summary (Resumen del sistema de configuración de la iDRAC)**. La sección **Backplane Inventory (Inventario de plano posterior)** incluye información sobre el 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 chasis conectados a la controladora y un vínculo al disco físico que contiene cada chasis. También se muestran los discos físicos conectados directamente a la controladora.

Para ver la topología de los dispositivos de almacenamiento, vaya a **Storage (Almacenamiento)** > **Overview (Descripción general)**. En la página **Overview (Descripción general)**, aparece la representación jerárquica de los componentes de almacenamiento en el sistema. Las opciones disponibles 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 criptográfico

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 v3.00.00.00 o posterior, puede agregar repuestos dinámicos globales cuando los discos virtuales no se crean.

Puede cambiar la asignación del repuesto dinámico cuando se desasigna 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, presione F2 para entrar a la configuración del sistema o la configuración del dispositivo. La opción CTRL+R ya no es compatible en PERC 10. CTRL+R solo funciona con PERC 9 mientras el modo de arranque está establecido en BIOS.

Si ha asignado un disco físico como repuesto dinámico global en el modo de funcionamiento Add to Pending Operation (Agregar a operación pendiente), 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 para asignar el repuesto dinámico global se borra.

Si ha desasignado un disco físico como repuesto dinámico global en el modo de funcionamiento Add to Pending Operation (Agregar a operación pendiente), 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 para desasignar el repuesto dinámico global se borra.

Si se elimina el último disco virtual, los repuestos dinámicos globales también vuelven al estado listo.

Si un PD ya es un repuesto dinámico global, el usuario puede seguir asignándolo 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 **Configuración** > **Configuración de almacenamiento**.
   Aparecerá la página **Configuración de almacenamiento**.
2. En el menú desplegable **Controladora**, seleccione la controladora para ver los discos físicos asociados.
3. Haga clic en **Configuración de disco físico**.
   Se muestran todos los discos físicos asociados a la controladora.
4. Para asignar un repuesto dinámico global, en los menús desplegables de la columna **Acción**, seleccione **Repuesto dinámico global** para uno o varios discos físicos.
5. Para desasignar un repuesto dinámico, en los menús desplegables de la columna **Acción**, seleccione **Desasignar repuesto dinámico** para uno o varios discos físicos.
6. Haga clic en **Apply Now** (Aplicar ahora).
   Según sus necesidades, también puede elegir aplicar **En el siguiente reinicio** o **A la hora programada**. 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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

Conversión de un disco físico en modo RAID a modo no RAID

La conversión de un disco físico a modo RAID habilita el disco para todas las operaciones de RAID. Cuando un disco se encuentra en modo no RAID, dicho disco está expuesto al sistema operativo (a diferencia de los discos no configurados y en buen estado) y se utiliza en un modo de paso directo.

PERC 10 no es compatible para convertir unidades en no RAID. Sin embargo, es compatible con PERC 10.2 y versiones posteriores.

Puede convertir las unidades de discos físicos en 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 conectados en caliente en PERC H330 siempre están en modo no RAID. En otras controladoras RAID, están siempre en modo RAID.
- Los discos conectados directamente en PERC 11 están listos o EPD-PT según el ajuste actual de comportamiento de configuración automática.

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 **Opciones de filtro**. Se muestran dos opciones: **Borrar todos los filtros** y **Filtro avanzado**. Haga clic en la opción **Filtro avanzado**.

Se muestra una lista elaborada que permite configurar diferentes parámetros.

3. En el menú desplegable **Agrupar por**, seleccione un gabinete o discos virtuales.
   Se muestran los parámetros asociados con el gabinete o el DV.
4. Haga clic en **Aplicar** cuando seleccione todos los parámetros deseados. 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 la controladora S140, solo puede utilizar la interfaz de RACADM para convertir las unidades que no son RAID a modo RAID. Los modos RAID del software compatible son Windows o Linux.

Para obtener más información acerca de los comandos, consulte *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

Borrado de discos físicos

La función borrado del sistema permite borrar el contenido de las unidades físicas. Esta función es accesible mediante RACADM o la interfaz gráfica de usuario de LC. Las unidades físicas en el servidor se agrupan en dos categorías.

- Unidades de borrado seguro: incluyen unidades que proporcionan borrado criptográfico como unidades ISE y SED SAS y SATA, además de las SSD de PCIe.
- Unidades de borrado con sobrescritura: incluyen todas las unidades que no admiten borrado criptográfico.

NOTA: Antes de borrar vFlash y ejecutar la operación, debe desasociar todas las particiones mediante interfaces de iDRAC.

NOTA: El borrado del sistema solo se aplica a las unidades dentro del servidor. iDRAC no puede borrar unidades en un gabinete externo, por ejemplo un JBOD.

El subcomando RACADM SystemErase incluye opciones para las siguientes categorías:

- La opción **SecureErasePD** borra criptográficamente todas los unidades de borrado seguro.
- La opción **OverwritePD** sobrescribe los datos en todas las unidades.

NOTA: El borrado criptográfico del disco físico BOSS se puede realizar mediante el método `SystemErase` que es compatible con LC-UI, Wsman y Racadm

Antes de ejecutar SystemErase, utilice el siguiente comando para comprobar la capacidad de borrado de todos los discos físicos de un servidor:

```
# racadm storage get pdisks -o -p SystemEraseCapability
```

NOTA: Si SEKM está habilitado en el servidor, desactive SEKM mediante el comando `racadm sekm disable` antes de utilizar este comando. Esto puede evitar que se bloqueen los dispositivos de almacenamiento protegidos por iDRAC, en caso de que la configuración de SEKM se borre de iDRAC mediante la ejecución de este comando.

Para borrar las unidades ISE y SED, utilice este comando:

```
# racadm systemerase -secureerasepd
```

Para borrar las unidades de borrado con sobrescritura, utilice el comando siguiente:

```
# racadm systemerase -overwritepd
```

NOTA: RACADM SystemErase elimina todos los discos virtuales de los discos físicos que se borran mediante los comandos anteriores.

NOTA: RACADM SystemErase hace que el servidor se reinicie para poder realizar las operaciones de borrado.

NOTA: Los dispositivos SSD de PCIe o SED individuales se pueden borrar usando RACADM o la interfaz gráfica de usuario del iDRAC. Para obtener más información, consulte la sección *Borrado de datos de un dispositivo SSD de PCIe* y la sección *Borrado de datos de un dispositivo SED*.

Para obtener información sobre la función de borrado del sistema dentro de la GUI de Lifecycle Controller, consulte *Guía del usuario de Lifecycle Controller* disponible en https://www.dell.com/idracmanuals.

Borrado de datos de un dispositivo SED/ISE

NOTA: Esta operación no se admite cuando el dispositivo compatible forma parte de un disco virtual. El dispositivo compatible con el destino se debe eliminar del disco virtual antes de realizar el borrado del dispositivo.

El borrado criptográfico borra permanentemente todos los datos presentes en el disco. La realización de un borrado criptográfico en una SED/ISE sobrescribe todos los bloques y provoca la pérdida permanente de todos los datos en los dispositivos compatibles. Durante el borrado criptográfico, el host no puede acceder al dispositivo compatible. El borrado del dispositivo SED/ISE se puede realizar en tiempo real o después de reiniciar 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 los datos del dispositivo SED/ISE, asegúrese de cumplir con las siguientes condiciones:

- Lifecycle Controller está activado.
- Cuenta con privilegios de inicio de sesión y control del servidor.
- La unidad admitida seleccionada no forma parte de un disco virtual.

NOTA:

- El borrado de SED/ISE se puede realizar como una operación en tiempo real o como una operación en etapas.
- Una vez que se borra la unidad, es posible que aún se muestre como activa dentro del sistema operativo debido al almacenamiento de datos en caché. Si esto ocurre, reinicie el sistema operativo y la unidad borrada ya no se mostrará ni informará ningún dato.
- La operación de borrado criptográfico no es compatible con los discos NVMe conectados en caliente. Reinicie el servidor de antes de iniciar la operación. Si la operación continúa fallando, asegúrese de que CSIOR esté habilitado y que los discos NVMe sean compatibles con Dell Technologies.

Borrado de datos de un dispositivo ISE/SED mediante la interfaz web

Para borrar los datos en el dispositivo compatible:

1. En la interfaz web de iDRAC, vaya a **Almacenamiento** > **Descripción general** > **Discos físicos**. Aparecerá la página **Discos físicos**.
2. Desde el menú desplegable **Controladora**, seleccione la controladora para ver los dispositivos asociados.
3. En los menús desplegables, seleccione **Borrado criptográfico** para una o varias unidades SED/ISE.
   Si ha seleccionado **Borrado criptográfico** 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:
   - **Aplicar ahora:** seleccione esta opción para aplicar las acciones inmediatamente sin reiniciar el sistema.
   - **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 las acciones en un día y hora programados:
     - **Hora de inicio** y **Hora de finalización**: haga clic en los íconos 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 no se ha creado correctamente, aparecerá un mensaje indicando que no se creó el ID del 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.

Borrado de datos de un dispositivo SED mediante RACADM

Para borrar de forma segura un dispositivo SED:

```
racadm storage cryptographicerase:<SED FQDD>
```

Para crear el trabajo de destino después de ejecutar el comando `cryptographicerase`:

```
racadm jobqueue create <SED FQDD> -s TIME_NOW -realtime
```

Para crear el trabajo de destino por etapas después de ejecutar el comando cryptographicerase:

```
racadm jobqueue create <SED 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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

Recreación de un disco físico

La recreación de un disco físico es la capacidad para reconstruir el contenido de un disco que ha fallado. Esto solo funciona cuando la opción de recreación automática se configura en false (falso). Si hay un disco virtual redundante, la operación de recreación puede reconstruir el contenido de un disco físico que ha fallado. Una recreación se puede realizar durante el funcionamiento normal, pero reduce el rendimiento.

Es posible usar la opción de cancelar la recreación para cancelar una recreación que está en curso. Si cancela una recreación, el disco virtual permanece en estado degradado. La falla de un disco físico adicional puede causar la falla del disco virtual y ocasionar la pérdida de datos. Se recomienda llevar a cabo una recreación en el disco físico que ha fallado lo antes posible.

En caso de que cancele la recreación de un disco físico que está asignado como repuesto dinámico, debe volver a iniciar la recreación en el mismo disco físico para poder restaurar los datos. Aunque cancele la recreación de un disco físico y asigne después otro disco físico como repuesto dinámico, no se recrearán los datos en el repuesto dinámico recién asignado.

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 un disco virtual
- Cancelar la inicialización en segundo plano
- Expansión de la capacidad en línea
- Migración de nivel RAID

NOTA: Puede administrar y supervisar 240 discos virtuales mediante interfaces de iDRAC. Para crear discos virtuales, utilice la configuración del dispositivo (F2), la herramienta de línea de comandos PERCCLI o el Dell OpenManage Server Administrator (OMSA).

NOTA: El conteo de PERC 10 es menor, ya que no admite arreglos de cadena margarita.

Creación de discos virtuales

Para implementar las funciones de RAID, se debe crear un disco virtual. Un disco virtual hace referencia al almacenamiento creado mediante una controladora RAID a partir de 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 usando los discos físicos conectados a la controladora PERC. Para crear un disco virtual, es necesario tener el 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 la cantidad máxima de discos virtuales admitida 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 en la controladora seleccionada. Debe esperar que finalice este trabajo o puede eliminarlo antes de intentar una operación nueva. Puede ver y administrar el estado del trabajo programado en la página Job Queue (Cola de trabajo).
- El disco físico está en modo no RAID. Debe convertirlo en modo RAID mediante las interfaces de la iDRAC, como la interfaz web de la 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: PERC H330 no es compatible con RAID 6 ni RAID 60.

NOTA: La controladora BOSS le permite crear solo discos virtuales que sean del mismo tamaño que el tamaño completo del medio de almacenamiento físico M.2. Asegúrese de establecer en cero el tamaño del disco virtual cuando utilice el perfil de configuración del servidor para crear un disco virtual BOSS. En el caso de otras interfaces como RACADM, WSMan y Redfish, no se debe especificar el tamaño del disco virtual.

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 se crean no se almacenan en la controladora. Esto significa que, si se produce un reinicio con otro sistema operativo, es posible que el nuevo sistema operativo cambie el nombre del disco virtual utilizando sus propias convenciones de nomenclatura.
- La agrupación de discos es una agrupación lógica de discos conectados a una controladora RAID en la cual se crean uno o más discos virtuales, de manera que todos los discos virtuales del grupo de discos usen todos los discos físicos del grupo. La implementación actual admite la formación de bloques con grupos de discos mixtos durante la creación de dispositivos lógicos.
- Los discos físicos están vinculados a grupos de discos. Por lo tanto, no hay una combinación de nivel RAID en un grupo de discos.
- Existen limitaciones con respecto al número de discos físicos que pueden incluirse en el disco virtual. Estas limitaciones dependen de la controladora. Cuando se crea un disco virtual, las controladoras admiten una cierta cantidad de secciones y tramos (métodos para combinar el almacenamiento en los discos físicos). Dado que la cantidad total de secciones y tramos es limitada, la cantidad de discos físicos que pueden utilizarse también es limitada. Las limitaciones de secciones y tramos afectan las posibilidades de niveles RAID como se indica a continuación:
  - Número máximo de tramos afecta a los niveles RAID 10, RAID 50 y RAID 60.
  - Número máximo de secciones afecta a los niveles RAID 0, RAID 5, RAID 50, RAID 6 y RAID 60.

- Número de discos físicos en un duplicado es siempre 2. Esto afecta a RAID 1 y RAID 10.

NOTA:
- RAID 1 solo se admite para las controladoras de BOSS.
- La controladora SWRAID solo admite RAID 0, 1, 5 y 10.

- No se pueden crear discos virtuales en SSD PCIe. Pero PERC 11 y las controladoras posteriores admiten la creación de discos virtuales mediante 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** > **Visión general** > **Discos virtualesFiltro avanzado**.
2. En la sección **Disco virtual**, haga 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 medio**, **Tamaño de sección**, **Política de lectura**, **Política de escritura**, **Política de caché del 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 puede ajustar este valor. Se calcula automáticamente después de seleccionar los discos para el nivel de RAID múltiple. El campo **Recuento de tramos** se aplica a RAID 10, RAID 50 y RAID 60. Si seleccionó RAID 10 y si la controladora admite RAID 10 desigual, no se muestra el valor del recuento de tramos. La controladora ajusta automáticamente el valor adecuado. Para RAID 50 y RAID 60, este campo no se muestra cuando utiliza la cantidad mínima de discos para crear RAID. Se puede cambiar si utiliza más discos.
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 carácter especial que ingrese se elimina y se reemplaza por un espacio durante la creación del disco virtual.

Creación de discos virtuales mediante RACADM

Utilice el comando `racadm storage createvd`.

Para obtener más información, consulte *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

NOTA: La división de discos o la configuración parcial de discos virtuales no se admite usando RACADM en las unidades administradas por la controladora S140.

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:

- **Adaptive 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 tienen acceso a sectores aleatorios del disco, la controladora usa la política sin lectura anticipada. La controladora continuará evaluando si las solicitudes de lectura están accediendo a sectores secuenciales del disco y, si es necesario, iniciará una lectura anticipada.
- **Lectura anticipada**: La controladora lee los sectores secuenciales del disco virtual cuando busca datos. La política de lectura anticipada puede mejorar el rendimiento del sistema si los datos se escriben en sectores secuenciales del disco virtual.
- **Sin lectura anticipada**: si 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 política de actualización tanto de la memoria principal como de la memoria caché proporciona una mayor seguridad de datos que la política de actualización exclusiva de la memoria caché, ya que el sistema da por sentado que los datos solo estarán disponibles después de que se hayan escrito en el disco.
- **Write Back (Exclusividad para escritura en caché)**: La controladora envía una señal de finalización de la solicitud de escritura apenas los datos están en la memoria caché de la controladora, aunque todavía no se hayan escrito en la unidad de disco. La exclusividad para escritura en caché puede mejorar el rendimiento, ya que las solicitudes de lectura posteriores pueden recuperar datos de la caché más rápidamente que del disco. Sin embargo, la pérdida de datos se puede producir en caso de una falla del sistema que impida que los datos se escriban en un disco. Otras aplicaciones también podrían experimentar problemas cuando las acciones dan por sentado que los datos están disponibles en el disco.
- **Force Write Back (Forzar exclusividad para escritura en caché)**: 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 cambian automáticamente a repuestos dinámicos globales.

Si elimina todos los discos virtuales de un repuesto dinámico global, dicho repuesto dinámico se eliminará 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 arranque. Esto se realiza desde la banda lateral sin importar qué sistema operativo sea. 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. Cuando sea necesario, la tarea revisar 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 revisión de congruencia mediante la interfaz web o RACADM.

También puede cancelar la operación de revisión de congruencia. La opción Cancelar revisión de congruencia es una operación en tiempo real.

Es necesario tener el privilegio de inicio de sesión y control del servidor para realizar una revisión de congruencia en los discos virtuales.

NOTA: La revisión de congruencia no se admite cuando las unidades están establecidas en modo RAID0.

NOTA: Si realiza una operación de cancelación de congruencia cuando no hay operaciones de comprobación de congruencia en curso, la operación pendiente en la GUI aparece como Cancelar BGI en lugar de Cancelar comprobación de congruencia.

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 cancelación de la inicialización es una operación en tiempo real. Es posible cancelar la inicialización utilizando solamente la interfaz web de la 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 operaciones de escritura futuras. La tarea de inicialización se puede completar rápidamente, ya que la información existente en los discos físicos no se borra, a pesar de que las operaciones de escritura futuras sobrescribirán toda la información que permanezca en los discos físicos.

La inicialización rápida solo elimina la información en las secciones y en el sector de arranque. Realice una inicialización rápida solo si existen limitaciones de tiempo o las unidades de disco duro son nuevas o se encuentran en desuso. La inicialización rápida se completa en menos tiempo (generalmente, entre 30 y 60 segundos).

PRECAUCIÓN: Después de ejecutar una inicialización rápida, no se puede obtener acceso a los datos existentes.

La tarea de inicialización rápida no escribe ceros en los bloques de discos de los discos físicos. Debido a que la tarea de inicialización rápida no realiza una operación de escritura, se produce menos degradación en el disco.

Si se realiza una inicialización rápida en un disco virtual, se sobrescriben los primeros y 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 de inicialización lenta) inicia todos los discos físicos incluidos en el disco virtual. Esta tarea actualiza los metadatos en los discos físicos y borra todos los datos y los sistemas de archivos existentes. Es posible realizar una inicialización completa después de crear el disco virtual. En comparación con la operación de inicialización rápida, es recomendable utilizar la inicialización completa si existe algún problema con un disco físico o se sospecha que el disco contiene bloques de disco dañados. La operación de inicialización completa reasigna los bloques dañados y escribe ceros en todos los bloques de disco.

Si se lleva a cabo la inicialización completa de un disco virtual, no se necesita una inicialización en 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 finaliza y se inicia un proceso de inicialización en segundo plano en el disco virtual.

Siempre se recomienda ejecutar una inicialización completa en las unidades donde se hayan almacenado datos anteriormente. La inicialización completa puede tardar entre 1 y 2 minutos por GB. La velocidad de inicialización varía según el modelo de la controladora, la velocidad de las unidades de disco duro y la versión de firmware.

La tarea de inicialización completa inicializa un disco físico a la vez.

NOTA: La inicialización completa solo se admite en tiempo real. Solamente unas pocas controladoras admiten la inicialización completa.

Cifrado de discos virtuales

Cuando se deshabilita el cifrado en una controladora (es decir, se elimina la clave de seguridad), es necesario habilitar manualmente el cifrado para los discos virtuales creados con unidades SED. Si el disco virtual se crea después de haber habilitado el cifrado en una controladora, el disco virtual se cifra automáticamente. Sin embargo, se configurará automáticamente como un disco virtual cifrado, a menos que se deshabilite la opción de cifrado habilitada 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 el cifrado esté habilitado en las controladoras, el usuario debe habilitar manualmente el cifrado en el disco virtual si dicho disco se crea a partir de la iDRAC. El disco virtual se cifra automáticamente solo si se crea a partir de OMSA.

Asignación o desasignación de repuestos dinámicos dedicados

Un repuesto dinámico dedicado es un disco de copia de seguridad no utilizado que se asigna a un disco virtual. Cuando falla un disco físico utilizado en un disco virtual, el repuesto dinámico se activa para reemplazar el disco físico que no funciona sin interrumpir el sistema ni requerir intervenciones.

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 de funcionamiento Add to Pending Operation (Agregar a operación pendiente), se crea la operación pendiente, pero no se crea un trabajo. Por lo tanto, si intenta desasignar el repuesto dinámico dedicado, la operación pendiente para asignar el repuesto dinámico dedicado se borra.

Si ha desasignado un disco físico como repuesto dinámico dedicado en el modo de funcionamiento Add to Pending Operation (Agregar a operación pendiente), se crea la operación pendiente, pero no se crea un trabajo. Por lo tanto, si intenta asignar el repuesto dinámico dedicado, la operación pendiente para desasignar el repuesto dinámico dedicado se borra.

NOTA: Mientras la operación de exportación de registros esté en curso, no podrá ver información sobre repuestos dinámicos dedicados en la página **Manage Virtual Disks (Administrar discos virtuales)**. Después de que la operación de exportación del registro se haya completado, vuelva a cargar o actualice la página **Manage Virtual Disks (Administrar discos virtuales)** para ver la información.

Cambiar el nombre del VD

Para cambiar el nombre de un disco virtual, el usuario debe contar con privilegios de control del sistema. El nombre del disco virtual puede contener solamente caracteres alfanuméricos, espacios, guiones y guiones bajos. La longitud máxima del nombre depende de cada controladora. En la mayoría de los casos, la longitud máxima es de 15 caracteres. El nombre no puede comenzar ni finalizar con un espacio, ni se puede dejar en blanco. Cada vez que se le cambia el nombre a un disco virtual, se crea un registro de LC.

Editar capacidad de disco

La expansión de la 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) y libera un nuevo espacio disponible al final de cada arreglo RAID.

La expansión de la capacidad en línea (OCE) se puede llevar a cabo de dos maneras:

- Si hay espacio libre disponible en la unidad física más pequeña en el grupo de discos virtuales después de iniciar el LBA de discos virtuales, la capacidad del disco virtual se podrá ampliar dentro de dicho espacio libre. Esta opción le permite

introducir el nuevo tamaño aumentado del disco virtual. Si el grupo de discos en un disco virtual tiene espacio disponible solamente antes de iniciar el LBA, la edición de capacidad de disco en el mismo grupo de discos no está permitida a pesar de que hay espacio disponible en una unidad física.

- También es posible ampliar la capacidad de un disco virtual agregando discos físicos compatibles al grupo de discos virtuales existente. 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 usado del grupo de discos físicos existente en un disco virtual específico, el nivel 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 final del disco virtual. De manera interna, el tamaño final del disco virtual se transmite a la controladora PERC como un porcentaje (este porcentaje es el espacio que el usuario desea utilizar del espacio vacío que queda en el arreglo para que el disco local se amplíe). Debido a esto, es posible que el porcentaje del tamaño final del disco virtual después de completar la reconfiguración sea diferente si el usuario no definió el tamaño máximo posible del disco virtual como tamaño final del disco virtual (el porcentaje resulta ser inferior al 100 %). Si el usuario introduce el tamaño máximo posible de disco virtual, no verá esta diferencia entre el tamaño de disco virtual introducido y el tamaño final del disco virtual.

Migración de nivel de RAID

La migración de nivel de RAID (RLM) hace referencia al cambio del nivel de RAID de un disco virtual. iDRAC9 ofrece una opción para aumentar el tamaño del DV mediante RLM. De cierto modo, RLM permite migrar el nivel de RAID de un disco virtual, que, a su vez, puede aumentar el tamaño del disco virtual.

La migración de nivel de RAID es el proceso de conversión de un DV con un nivel de RAID a otro. Cuando realiza la migración de un DV a un nivel de RAID diferente, los datos de usuario de este se redistribuyen en el formato de la nueva configuración.

Esta configuración es compatible en etapas y en tiempo real.

En la siguiente tabla, se describen diseños posibles de DV reconfigurables y la reconfiguración (RLM) de un DV con adición de discos y sin adición de discos.

Tabla 54. Diseño posible de DV

Diseño de DV de origen	Diseño posible de DV de destino con adición de disco	Diseño posible de DV de destino sin adición de disco
R0 (disco único)	R1	ND
R0	R5/R6	ND
R1	R0/R5/R6	R0
R5	R0/R6	R0
R6	R0/R5	R0/R5

Operaciones permitidas cuando OCE o RLM está en curso

Las siguientes operaciones se pueden realizar cuando OCE o RLM está en curso:

Tabla 55. Operaciones permitidas

Desde un extremo de la controladora, en el que un DV procesa OCE/RLM	Desde un extremo de DV (que procesa OCE/RLM)	Desde cualquier otro disco físico de estado preparado en la misma controladora	Desde cualquier otro extremo de DV (que no procesa OCE/RLM) en la misma controladora
Restablecer configuración	Eliminar	Hacer parpadear	Eliminar
Exportar registro	Hacer parpadear	Dejar de parpadear	Hacer parpadear
Establecer modo de lectura de patrullaje	Dejar de parpadear	Asignar un repuesto dinámico global	Dejar de parpadear
Comenzar lectura de patrullaje		Convertir en discos no RAID	Cambiar nombre

Tabla 55. Operaciones permitidas (continuación)

Desde un extremo de la controladora, en el que un DV procesa OCE/RLM	Desde un extremo de DV (que procesa OCE/RLM)	Desde cualquier otro disco físico de estado preparado en la misma controladora	Desde cualquier otro extremo de DV (que no procesa OCE/RLM) en la misma controladora
Cambiar propiedades de la controladora			Cambiar política
Administrar las propiedades de alimentación de discos físicos			Inicialización lenta
Convertir en discos con capacidad de RAID			Inicialización rápida
Convertir en discos no RAID			Reemplazar un disco miembro
Cambiar modo de controladora			

Restricciones o limitaciones de OCE y RLM

A continuación, se indican las limitaciones comunes para OCE y RLM:

- La OCE y la RLM se limitan a la situación en que el grupo de discos contiene solamente un disco virtual.
- La OCE no es compatible con RAID50 ni RAID60. La RLM no es compatible con RAID10 , RAID50 ni 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 u OCE a “escritura simultánea” hasta que finaliza la RLM u OCE.
- Generalmente, la reconfiguración de los Virtual Disks (Discos virtuales) afecta al rendimiento del disco hasta que la operación de reconfiguración concluya.
- La cantidad total de discos físicos en un grupo de discos no puede ser superior a 32.
- Si ya hay alguna operación ejecutándose en segundo plano (como inicialización en segundo plano/reinstalación/escritura diferida/lectura de patrullaje) en el disco virtual o disco físico correspondiente, no se permitirá la reconfiguración (OCE/RLM) en ese momento.
- Cualquier tipo de migración de discos que se realice mientras la reconfiguración (OCE/RLM) esté en curso en las unidades asociadas con el disco virtual hará que ocurra un error en la reconfiguración.
- Toda unidad nueva que se agregue para la OCE o RLM se convierte en parte del disco virtual una vez finalizada la reconstrucción. Sin embargo, el estado de esas unidades nuevas cambia a “en línea” justo después de que se inicia la reconstrucción.

Cancelar inicialización

Esta función permite cancelar la inicialización en segundo plano en un disco virtual. En las controladoras PERC, la inicialización en segundo plano de un disco virtual redundante se inicia automáticamente después de crear un disco virtual. La inicialización en segundo plano de un disco virtual redundante prepara el disco virtual para la información de paridad y mejora el rendimiento de escritura. Sin embargo, no es posible ejecutar algunos procesos (como la creación de un disco virtual) mientras la inicialización en segundo plano está en curso. Cancelar la inicialización permite cancelar manualmente la inicialización en segundo plano. Si se cancela, la inicialización en segundo plano se reinicia automáticamente entre 0 y 5 minutos después.

NOTA: La inicialización en segundo plano no se aplica a discos virtuales RAID 0.

Administración de discos virtuales mediante la interfaz web

1. En la interfaz web de iDRAC, haga clic en **Configuración** > **Configuración de almacenamiento** > **Configuración de disco virtual**.
2. En el menú **Discos virtuales**, seleccione la controladora en la que desea administrar los discos virtuales.

3. En el menú desplegable **Acción**, seleccione una de las acciones.

   Cuando se selecciona una, se muestra una ventana **Acción** adicional. Seleccione o ingrese el valor deseado.

   - **Cambiar nombre**
   - **Eliminar**
   - **Editar política de caché**: puede cambiar la política de caché para las siguientes opciones:
     - **Política de lectura**: los siguientes valores están disponibles para seleccionarse:
       - **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.
       - **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.
     - **Política de escritura**: permite cambiar 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.
     - **Política de caché de disco**: permite cambiar 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.
   - **Editar capacidad del disco**: puede agregar los discos físicos al disco virtual seleccionado en esta ventana. En esta ventana también se muestra tanto la capacidad actual como la nueva capacidad del disco virtual después de agregar los discos físicos.
   - **Migración de nivel RAID**: muestra el nombre del disco, el nivel RAID actual y el tamaño del disco virtual. Permite seleccionar un nuevo nivel RAID. Es posible que el usuario deba agregar 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.
   - **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 debido a que la información existente en los discos físicos no se borra, a pesar de que las operaciones de escritura futuras permiten sobrescribir 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.

   Para obtener más información sobre estas opciones, consulte la *Ayuda en línea de iDRAC*.
4. Haga clic en **Aplicar ahora** para aplicar los cambios de inmediato, en **En el siguiente reinicio** para aplicar los cambios en el próximo reinicio, en **En el período programado** para aplicar los cambios en un momento específico y en **Descartar todos los pendientes** para descartar los cambios.

   Según el modo de operación seleccionado, se aplicará la configuración.

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>=yes

Asignar repuesto dinámico

<Option>=no

Desasignar repuesto dinámico

Función de la configuración de RAID

En la siguiente tabla se muestran algunas de las funciones de la configuración de RAID que están disponibles en RACADM y WSMan:

PRECAUCIÓN: Si se fuerza a un disco físico para conectarse en línea u offline puede ocasionar la pérdida de datos.

Tabla 56. Función de la configuración de RAID

Función	Comando de RACADM	Descripción
Forzar en línea	`racadm storage forceonline:<PD FQDD>`	Una falla de alimentación, datos dañados o alguna otra razón pueden causar que un disco físico esté offline. Puede utilizar esta función para forzar a un disco físico a fin de conectarlo nuevamente en línea cuando ya se hayan probado todas las demás opciones. Una vez que el comando se ejecute, la controladora coloca la unidad en estado en línea y restablece su membresía dentro del disco virtual. Esto sucede solo si la controladora puede leer la unidad y escribir en sus metadatos.
NOTA: La recuperación de datos solo es posible cuando está dañada una parte limitada del disco. Forzar la función en línea no puede solucionar un disco que ya presentó fallas.		
Forzar fuera de línea	`racadm storage forceoffline:<PD FQDD>`	Esta función permite elimina una unidad de una configuración de disco virtual para que quede offline, lo que tendría como resultado una configuración degradada de VD. Es útil si una unidad

Tabla 56. Función de la configuración de RAID (continuación)

Función	Comando de RACADM	Descripción
		tiene más probabilidad de fallar en un futuro cercano o si informa de una falla SMART, pero aún está en línea. También puede utilizarse si desea emplear una unidad que forma parte de una configuración RAID existente.
Reemplazar el disco físico	`racadm storage replacephysicaldisk:<Source PD FQDD > -dstpd <Destination PD FQDD>`	Permite copiar los datos de un disco físico que es miembro de un VD en otro disco físico. El disco de origen debería estar en estado en línea, mientras el disco de destino debería estar en estado listo y ser de tamaño y tipo similar para remplazar el origen.
Disco virtual como dispositivo de arranque	`racadm storage setbootvd:<controller FQDD> -vd <VirtualDisk FQDD>`	Un disco virtual puede configurarse como un dispositivo de arranque con esta función. Esto permite una tolerancia a errores cuando se selecciona un VD con redundancia como dispositivo de arranque. Además, tiene el sistema operativo instalado en él.
Desbloquear la configuración ajena	`racadm storage unlock:<Controller FQDD> -key <Key id> -passwd <passphrase>`	Esta función se utiliza para autenticar unidades bloqueadas que tengan un cifrado de la controladora de origen diferente que la del destino. Una vez desbloqueada, la unidad puede migrarse correctamente de una controladora a otra.

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
- Descartar 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
- Modo de cifrado (Administrador de clave empresarial segura y administración de claves local)

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. Se ejecuta automáticamente una vez a la semana en unidades de disco duro SAS y SATA.

La lectura de patrullaje no se ejecuta en un disco físico en las siguientes circunstancias:

- El disco físico es una SSD.
- 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: Las 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 mediante las interfaces de la 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

NOTA: Tanto H330 como H345 requieren que se cargue el controlador para que se ejecuten las operaciones de inicialización en 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.

Aunque puede invocar las operaciones correctamente mediante las interfaces de la iDRAC, las operaciones fallan cuando se inicie el trabajo asociado. 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 prioridad más alta de la controladora. Se minimiza el tiempo de la inicialización en segundo plano y es la configuración con el mayor impacto en el rendimiento del sistema.

Revisión de congruencia

La revisión de congruencia verifica la precisión de la información redundante (de paridad). Esta tarea solo se aplica a los discos virtuales redundantes. De ser necesario, la tarea de revisión de congruencia regenera los datos redundantes. Cuando el estado de un disco virtual es de error en la redundancia, realizar una revisión de congruencia puede regresar el disco virtual al 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 prioridad más alta de la controladora. Se minimiza el tiempo de la revisión de congruencia 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 a través de las siguientes funciones:

1. **Sistema de administración de claves local (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.
2. **Administrador de clave empresarial segura (SEKM)**: esta función se utiliza para generar la clave mediante el servidor de administración de claves (KMS). Si utiliza la SEKM, debe configurar iDRAC con la información de KMS y se debe aplicar la configuración de SSL.

NOTA:

- Esta tarea no se admite en las controladoras de hardware PERC que se ejecutan en modo eHBA.
- 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.

NOTA:

- Para activar la SEKM, asegúrese de que esté instalado el firmware compatible de PERC.
- No es posible volver a una versión anterior del firmware de PERC si SEKM está instalado. Si intenta instalar una versión anterior de otro firmware de la controladora PERC en el mismo sistema, que no esté en el modo SEKM, también podría producir errores. Para instalar una versión anterior del firmware de las controladoras PERC que no estén en el modo SEKM, puede utilizar el método de actualización DUP de SO, o bien desactivar SEKM en las controladoras. Luego, puede volver a intentar hacer el cambio a la versión anterior desde iDRAC.

NOTA: Cuando se importa un volumen bloqueado que se puede conectar en caliente de un servidor a otro, podrá ver entradas CTL para los atributos de la controladora que se aplicarán en el registro de LC.

Configuración de las propiedades de la controladora mediante la interfaz web

1. En la interfaz web de la iDRAC, vaya a **Storage (Almacenamiento)** > **Overview (Descripción general)** > **Controllers (Controladoras)**.
   Se mostrará la página **Configuración de controladoras**.
2. En el menú desplegable **Controller (Controladora)**, seleccione la controladora que desea configurar.
3. Especifique la información necesaria para las distintas propiedades.
   En la columna **Current Value (Valor actual)**, figuran 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 **Apply Operation Mode (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 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 mediante las interfaces de la iDRAC, las operaciones fallarán cuando se inicie 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.

Puede importar configuraciones externas de manera que las unidades de disco virtual no se pierdan si mueve los discos físicos. Es posible importar una configuración externa 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 externa contiene solo un lado de un duplicado en un disco virtual RAID 1, el disco virtual se encuentra en estado degradado y se puede importar. Si la configuración externa 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 Import Foreign Configuration (Importar configuración externa) 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 externa bloqueada con el administrador de claves locales (LKM), no se podrá ejecutar la operación de importación de configuración externa en la iDRAC en esta versión. Es necesario desbloquear las unidades con CTRL-R y continuar con la importación de la configuración externa desde la iDRAC.

La tarea Import Foreign Configuration (Importar configuración externa) solo aparece cuando la controladora detecta una configuración externa. 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 una configuración externa 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 es compatible con la importación automática de configuraciones ajenas sin la interacción de los usuarios. La importación automática puede habilitarse o deshabilitarse. Si está habilitada, la controladora PERC puede importar automáticamente cualquier configuración externa detectada sin intervención manual. Si está deshabilitada, la controladora PERC no importa automáticamente ninguna configuración externa.

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 chasis externo cuando el sistema operativo se está ejecutando en el sistema. Quitar el cable puede provocar una configuración externa 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 externa hasta el momento en que se ejecuta la importación real. La importación de configuraciones externas solo se realiza en discos que se encuentran en el estado no configurado y bueno.
- 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

NOTA: Si hay una configuración incompleta de disco externo en el sistema, también se mostrará como externo el estado de uno o más discos virtuales en línea existentes.

NOTA: La importación de la configuración externa para la controladora BOSS no es compatible.

Para importar la configuración ajena:

1. En la interfaz web de iDRAC, vaya a **Configuración** > **Configuración de almacenamiento**.
2. En el menú desplegable **Controladora**, seleccione la controladora a la que desea importar la configuración externa.
3. Haga clic en **Importar** en **Configuración externa** y, a continuación, haga clic en **Aplicar**.

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 Clear Foreign Configuration (Borrar configuración externa) 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, haga clic en **Configuración** > **Configuración de almacenamiento** > **Configuración de la controladora**.
   Se muestra la página **Configuración de la controladora**.
2. En el menú desplegable **Controladora**, seleccione la controladora para la que desea borrar la configuración externa.

   NOTA: Para borrar la configuración externa en las controladoras BOSS, haga clic en "Restablecer configuración".

3. Haga clic en **Borrar configuración**.
4. Haga clic en **Aplicar**.
   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 anula la asignación de los repuestos dinámicos en la controladora. Esto solamente elimina los discos de la configuración, no borra ningún otro dato. Restablecer la configuración tampoco elimina configuraciones externas. La compatibilidad en tiempo real de esta función solo está disponible 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 tener privilegios de control del servidor.

NOTA: Restablecer la configuración de la controladora no elimina una configuración externa. Para eliminar una configuración externa, 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 la iDRAC, vaya a **Storage (Almacenamiento)** > **Overview (Descripción general)** > **Controllers (Controladoras)**.
2. En el menú desplegable **Actions (Acciones)**, seleccione la opción **Reset Configuration (Restablecer configuración)** para una o más 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

En las controladoras PERC 9.1, puede cambiar la personalidad de la controladora mediante el cambio de modo de RAID a HBA. La controladora funciona de manera similar a una controladora HBA, en las que las controladoras se pasan a través del sistema operativo. El cambio de modo de la controladora es una operación por etapas y no se produce en tiempo real.

Las controladoras PERC 10 y versiones posteriores son compatibles con el modo HBA mejorado, ya que sustituyen HBA en las opciones del modo actual de la controladora. Sin embargo, PERC 9 continúa siendo compatible con el modo HBA.

NOTA:
- El HBA mejorado es compatible con el PD no RAID y todos los VD de nivel RAID.
- Solo es compatible con la creación de los VD RAID0, RAID1 y RAID10.
- HBA no es compatible con PERC 11.

El modo HBA mejorado proporciona las siguientes funciones:
- Crear discos virtuales con nivel RAID 0, 1 o 10.
- Presentar discos que no son RAID al host.
- Configurar una política de caché predeterminada para los discos virtuales, como escritura no simultánea con lectura anticipada.
- Configurar discos virtuales y discos que no son RAID como dispositivos de arranque válidos.
- Convierta automáticamente todos los discos no configurados en no RAID:
  - En el arranque del sistema
  - En el restablecimiento de la controladora
  - Cuando los discos sin configurar se insertan sobre la marcha

NOTA: La creación o importación de discos virtuales RAID 5, 6, 50 o 60 no es compatible. Además, en el modo HBA mejorado, los discos no RAID se enumeran primero en orden ascendente, mientras los volúmenes de RAID se enumeran en orden descendente.

Antes de cambiar el modo de la controladora de RAID a HBA, asegúrese de que:
- La controladora RAID admite el cambio de modo de la controladora. La opción para cambiar el modo de la controladora no está disponible en las controladoras en las que 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 un estado de error se deben ser eliminar o hay que limpiar la caché fijada.

- Se debe eliminar cualquier clave de seguridad local asociada con las SED.
- 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 que exista una licencia disponible de CMC (no aplica para las plataformas MX) para los sleds de almacenamiento PERC FD33xS y FD33xD antes de cambiar el modo de la controladora. Para obtener más información sobre la licencia de CMC para los sleds de almacenamiento, consulte la *Guía del usuario de Dell Chassis Management Controller versión 1.2 para PowerEdge FX2/FX2s* disponible en dell.com/cmcmanuals.

Excepciones al cambiar el modo de la controladora

En la siguiente lista, se enumeran las excepciones al configurar el modo de la controladora mediante las interfaces de la iDRAC, como la interfaz web, RACADM o 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 es posible 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 inicia.
- Cuando cambia la controladora PERC del modo HBA a RAID, las unidades permanecen en estado Non-RAID (Sin RAID) y no se establecen automáticamente en el estado Ready (Listo). Además, el atributo **RAIDEnhancedAutoImportForeignConfig** se configura automáticamente en **Enabled (Activado)**.

En la siguiente lista, se enumeran las excepciones al configurar el modo de la controladora mediante la función de perfil de configuración del servidor mediante la interfaz de RACADM o WSMan:

- La función Server Configuration Profile (Perfil de configuración del servidor) le permite configurar varias operaciones de RAID y también el modo de la controladora. Por ejemplo, si la controladora PERC está en modo HBA, puede editar el perfil de configuración del servidor (SCP) 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 no funciona. Sin embargo, el modo de la controladora se cambia y el trabajo se completa con errores. Para evitar este problema, debe insertar un comentario para anular los atributos RAIDaction en el archivo SCP.
- Cuando la controladora PERC está en modo HBA, si ejecuta la importación de vista previa en el SCP de exportación (que está editado para cambiar el modo de la controladora a RAID) e intenta crear un VD, ocurrirá un error durante la creación del disco virtual. La vista previa de importación 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 **Acción** > **Editar**.
   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 **En el siguiente reinicio**.
   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>]
```

- Realice los siguientes pasos para crear un trabajo y aplicar cambios:

```
$ racadm jobqueue create <Controller Instance ID> -s TIME_NOW -r pwrcycle
```

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

Los servidores Dell PowerEdge deben tener instalado un sistema operativo y el controlador de dispositivo correspondiente debe estar cargado para que los HBA Dell funcionen. Después de la prueba POST, se deshabilitarán los puertos HBA. El controlador de dispositivo de HBA se encarga de restablecer el HBA y habilitar sus puertos conectados a dispositivos de almacenamiento. Sin un sistema operativo, el controlador no se cargará y no se garantiza que iDRAC pueda ver los dispositivos de almacenamiento conectados a los HBA Dell.

Las controladoras no RAID son los HBA que no disponen de algunas capacidades de RAID. Estas controladoras no admiten discos virtuales.

La interfaz de iDRAC 14G es compatible con la controladora HBA SAS de 12 Gbps y las controladoras HBA330 (integrada y de adaptador), HBA330 MMZ, y los adaptadores HBA330 MX.

Las plataformas AMD son compatibles con las controladoras del adaptador HBA355i frontal y HBA355i.

Es posible realizar las siguientes tareas para controladoras no RAID:

- Ver las propiedades de la controladora, los discos físicos y el gabinete, según corresponda para la controladora no RAID. Además, ver las propiedades del EMM, el ventilador, la unidad de suministro de energía y la sonda de temperatura asociadas con el gabinete. Las propiedades se muestran en función del tipo de controladora.
- Ver información sobre el inventario de software y hardware.
- Actualizar el firmware para gabinetes detrás de la controladora HBA SAS de 12 Gbps (organizados en etapas).
- Supervisar el sondeo o la frecuencia de sondeo para el estado de intervalo SMART en el disco físico cuando se detecta un cambio de estado.
- Supervisar el estado de acoplamiento activo o extracción directa en los discos físicos.
- Hacer parpadear o dejar de hacer parpadear los LED.

NOTA:

- La compatibilidad es limitado para las unidades de cinta cuando se conectan en HBA355e o SAS de 12 gbps.
- Aunque el LED no está disponible para la unidad de cinta, la opción de parpadeo/cancelar parpadeo puede funcionar.

NOTA:

- Habilitar la operación Recopilar inventario del sistema en el reinicio (CSIOR) antes de hacer un inventario o supervisar las controladoras no RAID.
- 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.

NOTA: No se admite la detección de unidades fallidas detrás de las controladoras HBA SAS.

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 errores en cada disco y envía alertas si se predice un error en el disco. Las controladoras revisan los discos físicos en busca de predicciones de errores y, si encuentran alguna, pasan esta información a la iDRAC. La iDRAC registra una alerta de inmediato.

Operaciones de la controladora en modo no RAID o 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

Esta función es una opción de la controladora que le permite al usuario descartar 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 el caso de que se desconecte la alimentación o un cable, hasta que usted recupere el disco virtual o 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 siguientes condiciones:

- La controladora no tiene ninguna configuración externa.
- La controladora no tiene ningún disco virtual perdido ni fuera de línea.
- Ningún disco virtual tiene los cables desconectados.

Managing PCIe SSDs

Peripheral Component Interconnect Express (PCIe) solid-state device (SSD) is a high-performance storage device designed for solutions requiring low latency, high Input Output Operations per Second (IOPS), and enterprise class storage reliability and serviceability. The PCIe SSD is designed based on Single Level Cell (SLC) and Multi-Level Cell (MLC) NAND flash technology with a high-speed PCIe 2.0, PCIe 3.0, or PCIe 4.0 compliant interface. In 14th generation of PowerEdge servers, we have three different ways to connect SSDs. You can use an extender to connect the SSDs via backplane, directly connect the SSDs from backplane to mother board using slimline cable without extender, and use HHHL (Add-In) card which sits on the motherboard.

NOTE:
- 14th generation of PowerEdge servers are supporting Industry standard NVMe-MI specification based NVMe SSDs
- PERC 11 supports PCIe SSD/NVMe devices behind PERC inventory monitoring and configuration.

Using iDRAC interfaces, you can view and configure NVMe PCIe SSDs.

The key features of PCIe SSD are:
- Hot plug capability
- High-performance device

In few of the 14th generation of PowerEdge servers, up to 32 NVMe SSDs are supported.

You can perform the following operations for PCIe SSDs:
- Inventory and remotely monitor the health of PCIe SSDs in the server
- Prepare to remove the PCIe SSD
- Securely erase the data
- Blink or unblink the device LED (Identify the device)

You can perform the following operations for HHHL SSDs:
- Inventory and real-time monitoring of the HHHL SSD in the server
- Failed card reporting and logging in iDRAC and OMSS
- Securely erasing the data and removing the card
- TTY logs reporting

You can perform the following operations for SSDs:
- Drive status reporting such as Online, Failed, and Offline

NOTE: Hot plug capability, prepare to remove, and blink or unblink the device LED is not applicable for HHHL PCIe SSD devices.

NOTE: When NVMe devices are controlled behind SW RAID, prepare to remove and cryptographic erase operations are not supported, blink and unblink are supported.

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 backplane PCIe dedicado, se muestran dos FQDD. Un FQDD es para las unidades comunes y el otro es para las SSD. Si el backplane se comparte (universal), se muestra solo un FQDD. En caso de que las SSD estén conectadas directamente, el FQDD de la controladora se reporta como CPU.1, lo que indica que la SSD está directamente conectada 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 de PCIe, en la interfaz web de la iDRAC, vaya a **Storage (Almacenamiento)** > **Overview (Descripción general)** > **Physical Disks (Discos físicos)**. Aparecerá la página

Propiedades. Para la SSD de PCIe, en la columna **Name (Nombre)**, aparece **PCIe SSD (SSD de PCIe)**. Amplíe 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 de 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

NOTA: Esta operación no se admite cuando:

- La SSD PCIe se configura mediante la controladora S140.
- El dispositivo NVMe está detrás de PERC 11.

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 extraer físicamente un dispositivo.

El intercambio directo ordenado solo se admite cuando las unidades SSD PCIe se encuentran instaladas en un sistema compatible en el cual se ejecuta un sistema operativo admitido. Para asegurarse de tener la configuración correcta para la 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 (ámbar intermitente).
- 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 la iDRAC, vaya a **Storage (Almacenamiento)** > **Overview (Descripción general)** > **Physical Disks (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 de PCIe, solo la opción **Apply Now (Aplicar ahora)** está disponible. Esta operación no se admite en el modo por etapas.
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 crea 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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

Borrado de datos de un dispositivo SSD PCIe

NOTA: Esta operación no es compatible con la configuración de SSD PCIe mediante la controladora SWRAID.

El borrado criptográfico borra permanentemente todos los datos presentes en el disco. La realización de un borrado criptográfico en una SSD PCIe sobrescribe todos los bloques y provoca la pérdida permanente de todos los datos en la SSD PCIe. Durante el borrado criptográfico, el host no puede acceder a la SSD 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 la unidad se borra, se muestra en el sistema operativo como en línea, pero no se inicializa. Debes inicializar y formatear la unidad antes de usarla de nuevo.
- Después de realizar el acoplamiento activo de una unidad SSD de PCIe, es posible que demore varios segundos para aparecer en la interfaz web.

Borrado de datos de un dispositivo SSD PCIe mediante la interfaz web

Para borrar los datos en el dispositivo SSD PCIe:

1. En la interfaz web de la iDRAC, vaya a **Overview (Descripción general)** > **Storage (Almacenamiento)** > **Physical Disks (Discos físicos)**.
   Aparecerá la página **Physical Disk (Disco físico)**.
2. En el menú desplegable **Controladora**, seleccione la controladora para ver las unidades SSD PCIe asociadas.
3. En los menús desplegables, seleccione **Cryptographic Erase (Borrado criptográfico)** para una o varias unidades SSD PCIe.
   Si ha seleccionado **Cryptographic Erase (Borrado criptográfico)** y desea ver las otras opciones en el menú desplegable, seleccione **Action (Acción)** y haga clic en el menú desplegable para ver las demás 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 crea 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 Dell PowerEdge de la 14.ª generación admiten una nueva topología de almacenamiento interno, en la que se pueden conectar dos controladoras de almacenamiento (PERC) a un conjunto de unidades internas a través de un solo expansor. Esta configuración se utiliza para el modo de alto rendimiento sin protección contra fallas o la funcionalidad de alta disponibilidad (HA). El expansor divide arreglo de unidades interno entre las dos controladoras de almacenamiento. En este modo, la creación de discos virtuales solo muestra las unidades conectadas a una controladora en particular. No existen requisitos de licencia para esta función. Esta característica solo es compatible con 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 tiene acceso a las primeras 12 unidades y la segunda controladora tiene acceso a las últimas 12 unidades. Las unidades conectadas a la primera controladora tienen el número 0-11, mientras que las unidades conectadas a la segunda controladora tienen el número 12-23.
- Modo dividido 4:20: una controladora tiene acceso a las primeras 4 unidades y la segunda controladora tiene acceso a las últimas 20 unidades. Las unidades conectadas a la primera controladora tienen el número 0-3, mientras que las unidades conectadas a la segunda controladora tienen el número 4-23.
- Modo dividido 8:16: una controladora tiene acceso a las primeras 8 unidades y la segunda controladora tiene acceso a las últimas 16 unidades. Las unidades conectadas a la primera controladora tienen el número 0-7, mientras que las unidades conectadas a la segunda controladora tienen el número 8-23.
- Modo dividido 16:8: una controladora tiene acceso a las primeras 16 unidades y la segunda controladora tiene acceso a las últimas 8 unidades. Las unidades conectadas a la primera controladora tienen el número 0-15, mientras que las unidades conectadas a la segunda controladora tienen el número 16-23.
- Modo dividido 20:4: una controladora tiene acceso a las primeras 20 unidades y la segunda controladora tiene acceso a las últimas 4 unidades. Las unidades conectadas a la primera controladora tienen el número 0-19, mientras que las unidades conectadas a la segunda controladora tienen el número 20-23.
- Modo dividido 6:6:6:6: 4 blades instalados en un chasis y cada blade tiene 6 unidades asignadas. Este modo solo se admite en blades de la serie C de PowerEdge.
- Información no disponible: la información de la controladora no está disponible.

iDRAC permite la configuración del modo dividido si el expansor tiene la capacidad de admitir la configuración. Asegúrese de habilitar este modo antes de instalar la segunda controladora. iDRAC realiza una verificación de la capacidad de expansión antes de permitir que este modo se configure y no verifica si la segunda controladora PERC está presente.

NOTA: Pueden aparecer errores en el cable (u otros errores) si pone el plano posterior en modo dividido con solo un PERC conectado, o si coloca el plano posterior en el modo unificado con dos PERC conectados.

Para modificar la configuración, es necesario tener el privilegio de control del servidor.

Si cualquier otra operación de RAID está en estado pendiente o cualquier trabajo de RAID está programado, no puede cambiar el modo de plano posterior. De forma similar, si esta configuración está pendiente, no puede 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 solo será efectivo después de un reinicio de la alimentación del sistema. Si cambia del modo dividido a unificado, se muestra un mensaje de error en el siguiente arranque, ya que la segunda controladora no ve ninguna unidad. Además, la primera controladora verá una configuración extraña. 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, haga clic en **Configuración** > **Configuración de almacenamiento** > **Configuración de gabinetes**.
2. En el menú **Controladora**, seleccione la controladora para configurar sus gabinetes asociados.
3. En el menú desplegable **Acción**, seleccione **Editar modo de gabinete**.
   Se mostrará la página **Editar modo de gabinete**.
4. En la columna **Valor actual**, seleccione el modo requerido de gabinete para el backplane o gabinete. Las opciones son:
   - Modo unificado
   - Modo dividido
   - Modo dividido 4:20
   - Modo dividido 8:16
   - Modo dividido 16:8
   - Modo dividido 20:4

   NOTA: En el caso de C6420, los modos disponibles son los siguientes: modo dividido y modo dividido-6:6:6:6. Es posible que algunos valores solo sean compatibles con ciertas plataformas.

   En el caso de R740xd y R940, el ciclo de apagado y encendido del servidor se requiere para emplear la nueva zona de backplane, y, en el caso de C6420, el ciclo de C/A (del servidor blade) se requiere para emplear la nueva zona de backplane.
5. Haga clic en **Agregar a operaciones pendientes**.
   Se creará una identificación de trabajo.
6. Haga clic en **Apply Now** (Aplicar ahora).
7. Vaya a la página **Cola de trabajos** y compruebe que se muestre el estado Completado para el trabajo.
8. Realice un ciclo de encendido del sistema para que se aplique la configuración.

Configuración de un gabinete mediante RACADM

Para configurar el chasis 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 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 identificación del 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 `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 backplanes de servidor PowerEdge de 14.ª generación admiten unidades SSD SAS/SATA y PCIe en la misma ranura. Estas ranuras se denominan ranuras universales y se conectan a la controladora de almacenamiento principal (PERC) y la tarjeta de extensión PCIe o Direct Connect Manager mediante backplanes de CPU admiten unidades SSD SAS/SATA y PCIe en la misma ranura. El firmware del backplane proporciona información sobre las ranuras que admiten esta función. El backplane es compatible con discos SAS/SATA o SSD PCIe. Por lo general, las cuatro ranuras con números más altos son universales. Por ejemplo, en un backplane universal que admite 24 slots, las ranuras 0-19 solo admiten discos SAS/SATA, mientras que las ranuras 20-23 admiten SSD SAS/SATA o PCIe.

El estado de recopilación del gabinete proporciona el estado combinado para todas las unidades en el gabinete. El enlace del gabinete en la página **Topología** muestra toda la información del gabinete, sin importar a qué controladora está asociada. Dado que se pueden conectar dos controladoras de almacenamiento (PERC y extensión PCIe) al mismo backplane, solo el backplane asociado con la controladora PERC se muestra en la página **Inventario del sistema**.

En la página **Almacenamiento** > **Gabinetes** > **Propiedades**, la sección **Descripción general de los 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: Las ranuras universales admiten intercambio en caliente. Si desea extraer 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 ejecuta esta tarea, el sistema operativo del host puede tener problemas como una pantalla azul, una alarma del kernel, etc.

Configuración de modo de SGPIO

La controladora de almacenamiento puede conectarse al backplane en modo I2C (configuración predeterminada para backplanes de Dell) o modo de entrada/salida de propósito general (SGPIO). Esta conexión se requiere para los LED parpadeantes en las unidades. Las controladoras Dell PERC y el backplane son compatibles con estos modos. Para admitir determinados adaptadores de canal, el modo de backplane debe cambiarse al modo SGPIO.

El modo SGPIO solo es compatible con los backplanes pasivos. No se admite en los backplanes basados en el expansor o en los backplanes pasivos en el modo descendente. En el firmware del backplane, se proporciona información sobre la funcionalidad, el estado actual y el estado solicitado.

Después de la operación de borrado LC o restablecimiento del iDRAC al valor predeterminado, el modo SGPIO se restablece al estado desactivado. Compara la configuración de iDRAC con la configuración del backplane. Si el backplane está establecido en modo SGPIO, iDRAC cambia la configuración para que coincida con la configuración del backplane.

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 recurso de un chasis

Esta opción le permite configurar la etiqueta de recurso de un chasis de almacenamiento.

El usuario puede cambiar la propiedad de la etiqueta de recurso del chasis para identificar los gabinetes. Estos campos se analizan en busca de valores no válidos y aparece un error si se introduce un valor no válido. Estos campos forman parte del firmware del chasis; los datos que se muestran inicialmente son los valores guardados en el firmware.

NOTA: La etiqueta de recurso tiene un límite de 10 caracteres que incluye el carácter nulo.

NOTA: Estas operaciones no se admiten en chasis internos.

Establecer el nombre de recurso del chasis

Esta opción le permite al usuario configurar el nombre de recurso de un chasis de almacenamiento.

El usuario puede cambiar la propiedad de nombre de recurso del chasis para identificar fácilmente los chasis. Estos campos se analizan en busca de valores no válidos y aparece un error si se introduce un valor no válido. Estos campos forman parte del firmware del chasis; los datos que se muestran inicialmente son los valores guardados en el firmware.

NOTA: El nombre de recurso tiene un límite de 32 caracteres que incluye el carácter nulo.

NOTA: Estas operaciones no se admiten en chasis internos.

Elección de modo de operación para aplicar configuración

Durante la creación y la administración de discos virtuales, si se desea configurar discos físicos, controladoras y chasis o restablecer controladoras, se debe seleccionar el modo de funcionamiento antes de aplicar los distintos valores. 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:
   - **Storage (Almacenamiento)** > **Physical Disks (Discos físicos)**
   - **Storage (Almacenamiento)** > **Virtual Disks (Discos virtuales)**
   - **Storage (Almacenamiento)** > **Controllers (Controladoras)**
   - **Storage (Almacenamiento)** > **Enclosures (Chasis)**
2. Seleccione una de las siguientes opciones en el menú desplegable **Aplicar modo de operación**:
   - **Apply Now (Aplicar ahora)**. Seleccione esta opción para aplicar la configuración inmediatamente. Esta opción está disponible solo para las controladoras PERC 9. Si hay trabajos pendientes de finalización, esta opción aparece atenuada. Este trabajo demorará, al menos, 2 minutos en completarse.
   - **At Next Reboot (Al siguiente reinicio)**. Seleccione esta opción para aplicar la configuración 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)

- **Add to Pending Operations (Agregar a operaciones pendientes)**. Seleccione esta opción a fin de crear una operación pendiente para aplicar la configuración. Puede ver todas las operaciones pendientes de una controladora en la página **Storage (Almacenamiento)** > **Overview (Descripción general)** > **Pending Operations (Operaciones pendientes)**.

NOTA:

- La opción **Add to Pending Operations (Agregar a operaciones pendientes)** no es aplicable para la página **Pending Operations (Operaciones pendientes)** ni para los dispositivos SSD PCIe en la página **Physical Disks (Discos físicos)** > **Setup (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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

Visualización y aplicación de operaciones pendientes

Aquí puede ver y confirmar todas las operaciones pendientes de la controladora de almacenamiento. Todos los valores se aplicarán a la vez, durante el siguiente reinicio o a una hora programada en función de las opciones seleccionadas. 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 de PCIe, el trabajo se crea en el disco SSD de PCIe y no en la extensión de PCIe.

Visualización, aplicación o eliminación de operaciones pendientes mediante la interfaz web

1. En la interfaz web de la iDRAC, vaya a **Storage (Almacenamiento)** > **Overview (Descripción general)** > **Pending Operations (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.
   - **At Next Reboot (Al siguiente reinicio)**. Seleccione esta opción para confirmar todas las operaciones durante el siguiente reinicio del sistema.

- **At Scheduled Time (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 **Job Queue (Cola de trabajos)** para ver el progreso del trabajo en la página **Job Queue (Cola de trabajos)**.

   Si están pendientes el borrado de configuración externa, la importación de configuración externa, operaciones de clave de seguridad u operaciones de cifrado de disco virtual (y si estas son las únicas operaciones pendientes), no se podrá crear un trabajo desde la página **Pending Operations (Operaciones pendientes)**. Es necesario realizar otra operación de configuración de almacenamiento o usar RACADM o WSMan para crear el trabajo de configuración necesario en la controladora requerida.

   No es posible ver ni borrar operaciones pendientes para los dispositivos de SSD de PCIe en la página **Pending Operations (Operaciones pendientes)**. Utilice el comando racadm para borrar las operaciones pendientes en los dispositivos SSD de 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 todas las operaciones pendientes para las SSD de 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. La compatibilidad en tiempo real de esta función solo está disponible en el firmware PERC 9.1 y en 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:
   - **Storage (Almacenamiento)** > **Overview (Descripción general)** > **Physical Disks (Discos físicos)** > **Status (Estado)**: Se muestra la página de discos físicos identificados, donde es posible hacer parpadear o dejar de hacer parpadear los discos físicos y las SSD de PCIe.
   - **Storage (Almacenamiento)** > **Overview (Descripción general)** > **Virtual Disks (Discos virtuales)** > **Status (Estado)**: Se muestra la página de discos virtuales identificados, donde es posible 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 deseleccione todas las unidades de disco físico o SSD de PCIe. Seleccione la opción **Select/Deselect All (Seleccionar/Deseleccionar todo)** y haga clic en **Blink (Hacer parpadear)** para iniciar el parpadeo de todas las unidades de disco físico y los SSD de 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.

Cómo hacer parpadear o dejar de hacer parpadear los LED de componentes mediante RACADM

Para hacer parpadear o dejar de hacer parpadear los 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**.

Reinicio en caliente

Cuando se realiza un reinicio en caliente, se observan los siguientes comportamientos:

- Las controladoras PERC en la interfaz de usuario de iDRAC aparecen en gris inmediatamente después del reinicio en caliente. Están disponibles una vez que se vuelve a realizar el inventario después del reinicio en caliente. Esto solo se aplica a las controladoras PERC y no a NVME/HBA/BOSS.

- Los archivos de almacenamiento en SupportAssist están vacíos cuando las controladoras PERC aparecen en gris en la GUI.
- El registro de LC para eventos PASADOS y críticos se realiza para PERC durante el proceso de `perc reinventory`. La opción Restablecer todo el LCL para los componentes de PERC se suprime. LCL se reanuda después de que se vuelve a realizar el inventario de PERC.
- No puede iniciar ningún trabajo en tiempo real hasta que se vuelva a realizar el inventario de PERC.
- Los datos de telemetría no se recopilan hasta que se vuelve a realizar el inventario de PERC.
- Una vez finalizado el inventario de PERC, se observa un comportamiento es normal.

19

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 de estos ajustes de configuración del BIOS. Cuando seleccione un atributo, se muestran diferentes parámetros que se relacionan con dicho atributo específico. Puede modificar varios parámetros de un atributo y aplicar los cambios antes de modificar otro atributo. 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.
- El puerto USB directo de iDRAC está disponible sin reinicio del host, incluso cuando todos los puertos USB están desactivados.

Aplicar

El botón **Aplicar** permanece atenuado hasta que se haya modificado alguno de los atributos. Una vez que hayan realizado los cambios en un atributo y se haya hecho clic en **Aplicar,** se puede modificar el atributo con los cambios necesarios. En caso de que la solicitud no establezca el atributo del BIOS, se produce un error con código de estado correspondiente de la respuesta HTTP asignado al error de API SMIL o el error de creación de trabajos. En ese momento, se genera y se muestra un mensaje. Para obtener más información, consulte *Guía de referencia de mensajes de error y eventos para servidores Dell EMC PowerEdge de 14.ª generación* disponible en https://www.dell.com/idracmanuals.

Descartar cambios

El botón **Descartar cambios** permanece atenuado hasta que se haya modificado alguno de los atributos. Si hace clic en el botón **Descartar cambios,** todos los cambios recientes se descartan y se restauran a los valores iniciales o anteriores.

Aplicar y reiniciar

Cuando un usuario modifica el valor de un atributo o secuencia de arranque, aparecen dos opciones para que el usuario aplique 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 Cola de trabajo para supervisar el progreso de ese trabajo específico.

El usuario puede ver información de auditoría relacionada con la configuración del BIOS en los registros LC.

Si hace clic en **Aplicar y reiniciar**, se reinicia el servidor inmediatamente para configurar todos los cambios necesarios. En caso de que la solicitud no establezca los atributos del BIOS, se produce un error con código de estado correspondiente de la respuesta HTTP asignado al error de API SMIL o al error de creación de trabajos. En ese momento, se genera y se muestra un mensaje EEMI.

Aplicar en el siguiente reinicio

Cuando un usuario modifica el valor de un atributo o secuencia de arranque, aparecen dos opciones para que el usuario aplique 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 Cola de trabajo para supervisar el progreso de ese trabajo específico.

El 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 modificaciones inmediatas según los últimos cambios de configuración hasta que se lleve a cabo correctamente la siguiente sesión de reinicio. En caso de que la solicitud no establezca los atributos del BIOS, se produce un error con código de estado correspondiente de la respuesta HTTP asignado al error de API SMIL o al error de creación de trabajos. En ese momento, se genera y se muestra un mensaje EEMI.

Eliminar todos los valores pendientes

El botón **Eliminar todos los valores pendientes** se activa solo cuando no hay valores pendientes según los últimos cambios de configuración. En caso de que el usuario decidiera no aplicar los cambios de configuración, el usuario puede hacer clic en el botón **Eliminar todos los valores pendientes** para finalizar todas las modificaciones. En caso de que la solicitud no elimine los atributos del BIOS, se produce un error con código de estado correspondiente de la respuesta HTTP asignado al error de API SMIL o al error de creación de trabajos. En ese momento, se genera y se muestra un mensaje EEMI.

Valor pendiente

La configuración de un atributo del BIOS a través de la iDRAC no se aplica de inmediato en el BIOS. Es necesario reiniciar el servidor para que los cambios surtan efecto. Cuando se modifica un atributo del BIOS, entonces se actualiza el **valor pendiente**. Si un atributo ya tiene un valor pendiente (que ya se ha configurado) se muestra en la interfaz gráfica de usuario.

Modificación de la configuración del BIOS

La modificación de la configuración del BIOS produce entradas en el registro de auditoría, que se introduce en los registros LC.

Escaneo activo del BIOS

El escaneo activo del BIOS verifica la integridad y autenticidad de la imagen de la ROM principal del BIOS cuando el host está encendido, pero no en POST.

NOTA:
- Para esta función, se requiere la licencia iDRAC Datacenter.
- Debe tener el privilegio de depuración para poder utilizar esta función.

iDRAC realiza la verificación de secciones inmutables de la imagen del BIOS automáticamente en los siguientes escenarios:
- En el ciclo de CA/arranque en frío
- Según un calendario determinado por el usuario
- A demanda (iniciado por el usuario)

El resultado correcto del escaneo activo se registra en el registro de LC. El resultado de la falla se registra en LCL y SEL.

Temas:

Escaneo activo del BIOS

El escaneo activo del BIOS verifica la integridad y autenticidad de la imagen de la ROM principal del BIOS cuando el host está encendido, pero no en POST.

NOTA:
- Para esta función, se requiere la licencia iDRAC Datacenter.
- Debe tener el privilegio de depuración para poder utilizar esta función.

iDRAC realiza la verificación de secciones inmutables de la imagen del BIOS automáticamente en los siguientes escenarios:
- En el ciclo de CA/arranque en frío
- Según un calendario determinado por el usuario
- A demanda (iniciado por el usuario)

El resultado correcto del escaneo activo se registra en el registro de LC. El resultado de la falla se registra en LCL y SEL.

Recuperación del BIOS y raíz de hardware de confianza (RoT)

Para el servidor PowerEdge, es obligatorio recuperarse de una imagen de BIOS dañada, ya sea debido a ataques maliciosos o a sobrecargas de alimentación, o bien a otros eventos imprevisibles. Una reserva alternativa de la imagen del BIOS sería necesaria para recuperar el BIOS a fin de que el servidor PowerEdge regrese al modo funcional desde el modo sin arranque. Este BIOS alternativo o de recuperación se almacena en un segundo SPI (combinado con el SPI del BIOS principal).

La secuencia de recuperación se puede iniciar a través de cualquiera de los siguientes enfoques con iDRAC como el orquestador principal de la tarea de recuperación del BIOS:

1. **Recuperación automática de la imagen principal o la imagen de recuperación del BIOS**: la imagen del BIOS se recupera automáticamente durante el proceso de arranque del host después de que el mismo BIOS detecte los daños en el BIOS.
2. **Recuperación forzada de la imagen principal o la imagen de recuperación del BIOS**: el usuario inicia una solicitud de OOB para actualizar el BIOS, ya sea porque tenga un BIOS nuevo actualizado o que el BIOS se acaba de bloquear mediante un error al iniciarse.
3. **Actualización de ROM de BIOS principal**: la única ROM principal se divide en la ROM de datos y la ROM de código. iDRAC tiene acceso o control completo sobre la ROM del código. Cambia el MUX para acceder a la ROM de código siempre que sea necesario.
4. **Raíz de confianza (RoT) del hardware del BIOS**: esta función está disponible en los servidores con el número de modelo RX5X, CX5XX y TX5X. Durante cada arranque del host (solo para el arranque en frío o el ciclo de CA, no durante el reinicio en caliente), iDRAC garantiza que se realice la RoT. La RoT se ejecuta automáticamente y el usuario no puede iniciarla mediante ninguna interfaz. Esta política de primer arranque del iDRAC verifica los contenidos de la ROM del BIOS en cada ciclo de CA y ciclo de CC del host. Este proceso garantiza el arranque seguro del BIOS y protege aún más el proceso de arranque del host.

NOTA: Para obtener más información sobre la RoT de hardware, consulte este enlace: https://downloads.dell.com/Manuals/Common/dell-emc-idrac9-security-root-of-trust-bios-live-scanning.pdf

20

Configuración y uso de la consola virtual

iDRAC agregó una opción de HTML5 mejorada en vConsole que permite el vKVM (teclado virtual, video y mouse) en un cliente VNC estándar. Puede utilizar la consola virtual para administrar un sistema remoto mediante el teclado, video y mouse de la estación de trabajo, a fin de controlar los dispositivos correspondientes en un servidor administrado. Esta es una función con licencia para los servidores de estante y torre. Está disponible de manera predeterminada para los servidores blade. Necesita el privilegio de configuración de iDRAC para acceder a todas las configuraciones de la consola virtual.

A continuación, se presenta la lista de atributos configurables en la consola virtual:

- vConsole habilitado: habilitado/deshabilitado
- Máx. de sesiones: 1-6
- Sesiones activas: 0-6
- Puerto de presencia remota
- Cifrado de video: activado / desactivado
- Video del servidor local: activado / desactivado
- Tipo de plug-in: eHTML5 (de manera predeterminada), ActiveX, Java, HTML5
- Acción dinámica al expirar el tiempo de espera de la solicitud de uso compartido: acceso completo, acceso de solo lectura y denegación de acceso
- Bloqueo automático del sistema: habilitado / deshabilitado
- Estado de conexión de teclado/mouse: conexión automática, conectado y desconectado

Las características claves son las siguientes:

- Se admite un máximo de seis sesiones de consola virtual simultáneas. Todas las sesiones visualizan la misma consola de servidor administrado a la vez.
- Puede iniciar la consola virtual en un navegador web compatible mediante el plug-in Java, ActiveX, HTML5 o eHTML5.

  NOTA:
  - Cualquier cambio en la configuración del servidor Web provocará la finalización de la sesión de consola virtual existente.
  - De manera predeterminada, el tipo de consola virtual está establecido como eHTML5.
  - Incluso si la opción de cifrado de video está deshabilitada en la GUI, puede configurar la función mediante otras interfaces cuando el tipo de plug-in es eHTML5. El cifrado de medios está habilitado de manera predeterminada para el tipo de plug-in de eHTML5.
- 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 plug-in de HTML5.
- Si otro usuario solicita una sesión de consola virtual, el primer usuario recibe una notificación y tendrá la opción de denegar el acceso, permitir un acceso de solo lectura o permitir un acceso de uso compartido completo. El segundo usuario recibe la notificación de que el primer usuario tiene el control. El primer usuario debe responder en treinta segundos o, de lo contrario, el acceso se otorgará al segundo usuario en función de la configuración predeterminada. Si ninguno de los dos usuarios dispone de privilegios de administrador y el primer usuario finaliza la sesión, también finalizará automáticamente la sesión del segundo usuario.
- Los registros de arranque y los registros de bloqueo se capturan como registros de video y están en formato MPEG1.
- La pantalla de bloqueo se captura como archivo JPEG.
- Los macros de teclado son compatibles con todos los complementos.
- Los macros de teclado son compatibles con todos los complementos. A continuación, se presenta la lista de macros que son compatibles con los complementos ActiveX y Java:

Tabla 57. Macros de teclado compatibles con los complementos ActiveX y Java

Cliente MAC	Cliente Win	Cliente Linux
Ctrl + Alt + Supr	Ctrl-Alt-Supr	Ctrl-Alt-Supr

Tabla 57. Macros de teclado compatibles con los complementos ActiveX y Java (continuación)

Cliente MAC	Cliente Win	Cliente Linux
Alt-Pet Sis-B	Alt-Pet Sis-B	Alt-Pet Sis-B
-	Win + P	-
-	-	Ctrl + Alt + F<1-12>
Alt-PetSis	-	-
PetSis	-	-
Impr Pant	-	-
Alt + Impr Pant	-	-
Pausa	-	-

NOTA: Para los macros de teclado compatibles con el complemento de HTML, consulte la sección Consola virtual basada en HTML5.

NOTA: El número de sesiones activas de la consola virtual que se muestran en la interfaz web corresponde solo a sesiones activas de la interfaz web. Este número no incluye sesiones desde otras interfaces, como SSH y RACADM.

NOTA: Para obtener información sobre cómo configurar el navegador para tener acceso a la consola virtual, consulte Configuración de exploradores web para usar la consola virtual en la página 75.

NOTA: Para desactivar el acceso de KVM, use la opción **Desactivar** en la configuración de chasis en la interfaz web de OME Modular.

Temas:

- Resoluciones de pantalla y velocidades de actualización admitidas
- Configuración de la consola virtual
- Vista previa de la consola virtual
- Inicio de la consola virtual
- Uso del visor de la consola virtual

Resoluciones de pantalla y velocidades de actualización admitidas

En la tabla siguiente se indican las resoluciones de pantalla admitidas y las velocidades de actualización para una sesión de consola virtual que se ejecuta en el servidor administrado.

Tabla 58. 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 que configure la resolución de pantalla del monitor a 1920 x 1200 píxeles.

La consola virtual es compatible con una resolución de video máxima de 1920 x 1200 a 60 Hz de velocidad de actualización. A fin de lograr esta resolución, se requieren las siguientes condiciones:

- KVM/monitor conectado a VGA compatible con la resolución 1920 x 1200
- Controlador de video Matrox más reciente (para Windows)

Cuando un KVM/monitor local con una resolución máxima inferior a 1920 x 1200 está conectado a un conector VGA, se reducirá la resolución máxima admitida en la consola virtual.

La consola virtual de iDRAC aprovecha la controladora de gráficos Matrox G200 incorporada para determinar la resolución máxima del monitor conectado cuando existe una pantalla física. Cuando el monitor es compatible con una resolución de 1920 x 1200 o superior, la consola virtual es compatible con la resolución 1920 x 1200. Si el monitor conectado es compatible con una resolución máxima inferior (como muchas KVM), la resolución máxima de la consola virtual es limitada.

Resolución máxima de la consola virtual basada en la tasa de visualización del monitor:

- monitor 16:10: la resolución máxima es de 1920 x 1200
- monitor 16:9: la resolución máxima es de 1920 x 1080

Cuando un monitor físico no está conectado al puerto VGA del servidor, el sistema operativo instalado indicará las resoluciones disponibles para la consola virtual.

Resoluciones máximas de la consola virtual basadas en el sistema operativo host sin monitor físico:

- Windows: 1600 x 1200 (1600 x 1200, 1280 x 1024, 1152 x 864, 1024 x 768 y 800 x 600)
- Linux: 1024 x 768 (1024 x 768, 800 x 600, 848 x 480, 640 x 480)

NOTA: Si se requiere una resolución más alta a través de la consola virtual cuando el KVM físico o el monitor no está presente, se puede aprovechar una llave del emulador de la pantalla VGA para imitar una conexión de monitor externo con una resolución de hasta 1920 x 1080.

NOTA: Si tiene una sesión activa de la consola virtual y un monitor de menor resolución está conectado a la consola virtual, la resolución de la consola del servidor puede restablecerse si se selecciona el servidor en la consola local. Si el sistema ejecuta un sistema operativo Linux, es posible que una consola X11 no esté visible en el monitor local. Presione <Ctrl><Alt><F1> en la consola virtual del iDRAC para cambiar de 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 **Configuración** > **Consola virtual**. Haga clic en el enlace **Iniciar la consola virtual**; se muestra 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**. La consola virtual está configurada.

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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.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 **System (Sistema)** > **Properties (Propiedades)** > **System Summary (Resumen del sistema)**. La sección **Virtual Console Preview (Vista previa de la consola virtual)** muestra una imagen que ilustra 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 navegador web está configurado para utilizar los plug-ins HTML5, eHTML5, Java o ActiveX.
- Hay un ancho de banda de red mínimo de 1 Mb/seg disponible.

NOTA: Si la controladora de vídeo integrada se desactiva en el BIOS e inicia la consola virtual, el visor de la consola virtual aparece en blanco.

Cuando se inicia la consola virtual mediante navegadores IE de 32 o 64 bits, utilice HTML5/eHTML5 o el plug-in necesario (Java o ActiveX) disponible en el navegador correspondiente. Los valores de configuración de Opciones de Internet son comunes para todos los exploradores.

Cuando se inicia la consola virtual con el complemento Java, es posible que, de vez en cuando, se produzca un error de compilación de Java. Para resolver este problema, vaya al **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 no se inicie la primera vez. Esto se debe a una conexión de red lenta; el tiempo de espera de las credenciales temporales (que la consola virtual utiliza para conectarse) es de dos minutos. El tiempo de descarga del complemento cliente ActiveX puede superar este tiempo. Cuando el complemento se descargue correctamente, podrá iniciar la consola virtual con normalidad.

Para iniciar la consola virtual mediante el plug-in HTML5/eHTML5, debe desactivar el bloqueador de elementos emergentes.

La consola virtual tiene los siguientes controles de consola:

1. **General**: puede establecer macros de teclado, relación de aspecto y modo táctil.
2. **KVM**: mediante esta opción se muestra la velocidad de fotogramas, el ancho de banda, la compresión y la velocidad de paquetes.
3. **Rendimiento**: puede cambiar la calidad de video y la velocidad de video con esta opción.
4. **Lista de usuarios**: puede ver la lista de usuarios conectados a la consola.

Puede acceder a los medios virtuales haciendo clic en la opción **Conectar a medios virtuales** disponible en la consola virtual.

Inicio de la consola virtual mediante la interfaz web

Puede iniciar la consola virtual de las maneras siguientes:

- Vaya a **Configuración** > **Consola virtual**. Haga clic en el enlace **Iniciar la consola virtual**. Aparece la página Consola virtual.

El **Visor de la consola virtual** 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 su estación de administración.

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 Active Directory 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: Necesita Java 8 o una versión posterior para usar esta función y para iniciar la consola virtual de la iDRAC en una red IPv6.

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 sincronización del ratón, ajuste de escala de la consola virtual, opciones de chat, macros para el teclado, acciones relacionadas con la alimentación, dispositivos para el siguiente arranque y acceso a medios virtuales. Para obtener información sobre cómo usar estas funciones, consulte la *Ayuda en línea de la 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, aparece el nombre DNS o la dirección IP de la iDRAC a la que el usuario se encuentra conectado desde la estación de administración. Si la iDRAC no tiene 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>`

A veces, el visor de la consola virtual puede mostrar vídeo de baja calidad. Esto se debe a una conexión de red lenta que provoca la pérdida de uno o dos cuadros de video al iniciar la sesión de consola virtual. Para transmitir todos los cuadros de video y mejorar la calidad de video, realice cualquiera de las siguientes acciones:

- 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**.

eHTML5 based virtual console

NOTE: While using eHTML5 to access virtual console, the language must be consistent across client and target keyboard layout, OS, and browser. For example, all must be in English (US) or any of the supported languages.

To launch the eHTML5 virtual console, you must enable the virtual console feature from the iDRAC Virtual Console page and set the **Plug-in Type** option to eHTML5.

NOTE: By default the virtual console type is set to eHTML5.

You can launch virtual console as a pop-up window by using one of the following methods:

- From iDRAC Home page, click the **Start the Virtual Console** link available in the Console Preview session
- From iDRAC Virtual Console page, click **Start the Virtual Console** link.
- From iDRAC login page, type **https//<iDRAC IP>/console**. This method is called as Direct Launch.

In the eHTML5 virtual console, the following menu options are available:

- Power
- Boot
- Chat
- Keyboard
- Screen Capture
- Refresh
- Full Screen
- Disconnect Viewer
- Console Controls
- Virtual Media

The **Pass all keystrokes to server** option is not supported on eHTML5 virtual console. Use keyboard and keyboard macros for all the functional keys.

- **General** —
  - **Console control** — This has the following configuration options:
    - Keyboard Macros — This is supported in eHTML5 virtual console and are listed as the following drop-down options. Click **Apply** to apply the selected key combination on the server.
      - Ctrl+Alt+Del
      - Ctrl+Alt+F1
      - Ctrl+Alt+F2
      - Ctrl+Alt+F3
      - Ctrl+Alt+F4
      - Ctrl+Alt+F5
      - Ctrl+Alt+F6
      - Ctrl+Alt+F7
      - Ctrl+Alt+F8
      - Ctrl+Alt+F9
      - Ctrl+Alt+F10

- Ctrl+Alt+F11
- Ctrl+Alt+F12
- Alt+Tab
- Alt+ESC
- Ctrl+ESC
- Alt+Space
- Alt+Enter
- Alt+Hyphen
- Alt+F1
- Alt+F2
- Alt+F3
- Alt+F4
- Alt+F5
- Alt+F6
- Alt+F7
- Alt+F8
- Alt+F9
- Alt+F10
- Alt+F11
- Alt+F12
- PrntScrn
- Alt+PrntScrn
- F1
- Pause
- Tab
- Ctrl+Enter
- SysRq
- Alt+SysRq
- Win-P

▪ Aspect Ratio — The eHTML5 virtual console video image automatically adjusts the size to make the image visible. The following configuration options are displayed as a drop-down list:
- Maintain
- Don't Maintain

Click **Apply** to apply the selected settings on the server.

▪ Touch Mode — The eHTML5 virtual console supports the Touch Mode feature. The following configuration options are displayed as a drop-down list:
- Direct
- Relative

Click **Apply** to apply the selected settings on the server.

- **Virtual Clipboard** - Virtual clipboard enables you to cut / copy / paste text buffer from virtual console to iDRAC host server. Host server could be BIOS, UEFI or in OS prompt. This is a one-way action from client computer to iDRAC's host server only. Follow these steps to use the Virtual clipboard:
  - Place the mouse cursor or keyboard focus on the desired window in the host server desktop.
  - Select the **Console Controls** menu from vConsole.
  - Copy the OS clipboard buffer using keyboard hotkeys, mouse, or touch pad controls depending on the Client OS. Or, you can type the text manually in the text box.
  - Click **Send Clipboard to Host**.
  - Then, the text appears on the host server's active window.

NOTE:
- This feature is only available in Datacenter license.
- This feature only supports ASCII text.
- Control characters are not supported.
- Characters such as **New line** and **Tab** are allowed.
- Text buffer size is limited to 4000 characters.

    - If more than maximum buffer is pasted, then the edit box in iDRAC GUI will truncate it to maximum buffer size.
- **KVM** - This menu has list of the following read only components:
    - Frame Rate
    - Bandwidth
    - Compression
    - Packet Rate
- **Performance** - You can use the slider button to adjust **Maximum Video Quality** and **Maximum Video Speed**.
- **User List** - You can see the list of users that are logged in to the Virtual console.
- **Keyboard** — The difference between physical and virtual keyboard is that virtual keyboard changes its layout according to the browser language.
- **Virtual Media** — Click **Connect Virtual Media** option to start the virtual media session.
    - **Connect Virtual Media** - This menu contains the options for Map CD/DVD, Map Removable Disk, Map External Device, and Reset USB.
    - **Virtual Media Statistics** - This menu shows the Transfer Rate (Read-only). Also, it shows the details of CD/DVD and Removable Disks details such as Mapping details, status (read-only or not), duration, and Read/Write Bytes.
    - **Create Image** - This menu allows you to select a local folder and generate FolderName.img file with local folder contents.

NOTE: For security reasons read/write access is disabled while accessing virtual console in eHTML5. With Java or ActiveX plug-ins, you can accept security messaging before the plug-in is given the read/write authority.

Supported Browsers

The eHTML5 virtual console is supported on the following browsers:

- Internet Explorer 11
- Google Chrome 83/84
- Mozilla Firefox 80/81
- Safari 13.1.1

NOTE: It is recommended to have Mac OS version 10.10.2 (or onward) installed in the system.

For more details on supported browsers and versions, see the *Notas de la versión de iDRAC* disponibles en https://www.dell.com/idracmanuals.

HTML5 based virtual console

NOTE: While using HTML5 to access virtual console, the language must be consistent across client and target keyboard layout, OS, and browser. For example, all must be in English (US) or any of the supported languages.

To launch the HTML5 virtual console, you must enable the virtual console feature from the iDRAC Virtual Console page and set the **Plug-in Type** option to HTML5.

You can launch virtual console as a pop-up window by using one of the following methods:

- From iDRAC Home page, click the **Start the Virtual Console** link available in the Console Preview session
- From iDRAC Virtual Console page, click **Start the Virtual Console** link.
- From iDRAC login page, type **https//<iDRAC IP>/console**. This method is called as Direct Launch.

In the HTML5 virtual console, the following menu options are available:

- Power
- Boot
- Chat
- Keyboard
- Screen Capture
- Refresh
- Full Screen
- Disconnect Viewer
- Console Controls
- Virtual Media

The **Pass all keystrokes to server** option is not supported on HTML5 virtual console. Use keyboard and keyboard macros for all the functional keys.

- **Console control** — This has the following configuration options:
  - Keyboard Macros — This is supported in HTML5 virtual console and are listed as the following drop-down options. Click **Apply** to apply the selected key combination on the server.
    - Ctrl+Alt+Del
    - Ctrl+Alt+F1
    - Ctrl+Alt+F2
    - Ctrl+Alt+F3
    - Ctrl+Alt+F4
    - Ctrl+Alt+F5
    - Ctrl+Alt+F6
    - Ctrl+Alt+F7
    - Ctrl+Alt+F8
    - Ctrl+Alt+F9
    - Ctrl+Alt+F10
    - Ctrl+Alt+F11
    - Ctrl+Alt+F12
    - Alt+Tab
    - Alt+ESC
    - Ctrl+ESC
    - Alt+Space
    - Alt+Enter
    - Alt+Hyphen
    - Alt+F1
    - Alt+F2
    - Alt+F3
    - Alt+F4
    - Alt+F5
    - Alt+F6
    - Alt+F7
    - Alt+F8
    - Alt+F9
    - Alt+F10
    - Alt+F11
    - Alt+F12
    - PrntScrn
    - Alt+PrntScrn
    - F1
    - Pause
    - Tab
    - Ctrl+Enter
    - SysRq
    - Alt+SysRq
    - Win-P
  - Aspect Ratio — The HTML5 virtual console video image automatically adjusts the size to make the image visible. The following configuration options are displayed as a drop-down list:
    - Maintain
    - Don't Maintain

    Click **Apply** to apply the selected settings on the server.
  - Touch Mode — The HTML5 virtual console supports the Touch Mode feature. The following configuration options are displayed as a drop-down list:
    - Direct
    - Relative

    Click **Apply** to apply the selected settings on the server.

- **Virtual Clipboard** - Virtual clipboard enables you to cut / copy / paste text buffer from virtual console to iDRAC host server. Host server could be BIOS, UEFI or in OS prompt. This is a one-way action from client computer to iDRAC's host server only. Follow these steps to use the Virtual clipboard:
  - Place the mouse cursor or keyboard focus on the desired window in the host server desktop.
  - Select the **Console Controls** menu from vConsole.
  - Copy the OS clipboard buffer using keyboard hotkeys, mouse, or touch pad controls depending on the Client OS. Or, you can type the text manually in the text box.
  - Click **Send Clipboard to Host**.
  - Then, the text appears on the host server's active window.

  NOTE:
  - This feature is only available in Datacenter license.
  - This feature only supports ASCII text.
  - Control characters are not supported.
  - Characters such as **New line** and **Tab** are allowed.
  - Text buffer size is limited to 4000 characters.
  - If more than maximum buffer is pasted, then the edit box in iDRAC GUI will truncate it to maximum buffer size.
- **Keyboard** — The difference between physical and virtual keyboard is that virtual keyboard changes its layout according to the browser language.
- Touch Mode — The HTML5 virtual console supports the Touch Mode feature. The following configuration options are displayed as a drop-down list:
  - Direct
  - Relative

  Click **Apply** to apply the selected settings on the server.
- Mouse Acceleration — Select the mouse acceleration based on the operating system. The following configuration options are displayed as a drop-down list:
  - Absolute (Windows, latest versions of Linux, Mac OS-X)
  - Relative, no acceleration
  - Relative (RHEL, earlier versions of Linux)
  - Linux RHEL 6.x and SUSE Linux Enterprise Server 11 or later

  Click **Apply** to apply the selected settings on the server.
- **Virtual Media** — Click **Connect Virtual Media** option to start the virtual media session. when the virtual media is connected, you can see the options like Map CD/DVD, Map Removable Disk, and Reset USB.

NOTE: For security reasons read/write access is disabled while accessing virtual console in HTML5. With Java or ActiveX plug-ins, you can accept security messaging before the plug-in is given the read/write authority.

Supported Browsers

The HTML5 virtual console is supported on the following browsers:
- Internet Explorer 11
- Google Chrome 83/84
- Mozilla Firefox 80/81
- Safari 13.1.1

NOTE: It is recommended to have Mac OS version 10.10.2 (or onward) installed in the system.

For more details on supported browsers and versions, see the *Notas de la versión de iDRAC* disponibles en https://www.dell.com/idracmanuals.

Sincronización de los punteros del mouse

NOTA: Esta función no se aplica al tipo de plug-in de eHTML5.

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.

Cuando utilice Red Hat Enterprise Linux o Novell SUSE Linux, configure el modo de mouse para Linux antes de iniciar el visor de la consola virtual. Los ajustes predeterminados del mouse del sistema operativo se utilizan para controlar la flecha del mouse en el visor de la consola virtual.

Cuando se ven dos cursores del mouse en el visor de la consola virtual del cliente, esto indica que el sistema operativo del servidor es compatible con el posicionamiento relativo. Esto es común en los sistemas operativos Linux o Lifecycle Controller y ocasiona que aparezcan dos cursores del mouse si los ajustes de aceleración del mouse en el servidor son diferentes de los ajustes de aceleración del mouse en el cliente de la consola virtual. Para resolver esto, cambie a un cursor único o haga que la aceleración del mouse sea la misma en el sistema administrado y en la estación de administración:

- Para cambiar a un cursor único, en el menú **Herramientas**, seleccione **Cursor único**.
- Para establecer la aceleración del mouse, vaya a **Herramientas** > **Opciones de sesión** > **Mouse**. En la pestaña **Aceleración del mouse**, seleccione **Windows** o **Linux** según el sistema operativo que tenga.

Para salir del modo de cursor único, presione <Esc> o la tecla de terminación configurada.

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

Si se utiliza la consola virtual para conectarse a un sistema administrado con un sistema operativo de distribución Linux recientemente instalado, es posible que se produzcan problemas de sincronización con el mouse. Esto puede deberse a la función Aceleración previsible de puntero del escritorio GNOME. Para lograr una sincronización adecuada con el mouse en la consola virtual de iDRAC, se debe desactivar esta función. Para ello, en la sección de mouse en el archivo **/etc/X11/xorg.conf**, agregue lo siguiente:

```
Option "AccelerationScheme" "lightweight".
```

Si se siguen produciendo problemas de sincronización, realice el siguiente cambio adicional en el archivo **<inicio de usuario>/.gconf/desktop/gnome/peripherals/mouse/%gconf.xml**:

Cambie los valores de `motion_threshold` y `motion_acceleration` a `-1`.

Si desactiva la aceleración del mouse en el escritorio GNOME, en el visor de la consola virtual, vaya a **Herramientas** > **Opciones de sesión** > **Mouse**. En la 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 habilitar 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 desde la estación de administración al sistema administrado a través del visor de la consola virtual. Si está deshabilitada, todas las combinaciones de teclas se dirigen a la estación de administración 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)** > **, ficha General (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.

  En el cliente Java, se debe cargar la biblioteca nativa para que funcionen las opciones de pasar todas las pulsaciones de tecla al servidor y de modo de 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)** no estarán habilitadas. Si intenta seleccionar una de estas opciones, se mostrará un mensaje de error que indica que no se admiten las opciones seleccionadas.

  En el cliente ActiveX, se debe cargar la biblioteca nativa para que funcione la opción de 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)** no estará habilitada. Si intenta seleccionar esta opción, se mostrará un mensaje de error que indica que no se admite la característica 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 funcionan en el sistema operativo de la estación de administración no se pasan al sistema administrado.
- El modo del visor de la consola virtual (ventana o pantalla completa).

  En el modo de pantalla completa, la opción **Pasar todas las pulsaciones de tecla al servidor** está activada de manera predeterminada.

  En el modo de ventana, las pulsaciones de teclas solo se pasan cuando el visor de la consola virtual es visible y está activo.

  Cuando cambia del modo de pantalla completa al modo de ventana, se reanuda el estado anterior de la opción para pasar todas las pulsaciones de teclas.

Sesión de consola virtual basada en Java que se ejecuta en el sistema operativo Windows

- La combinación de teclas Ctrl+Alt+Supr no se envía al sistema administrado pero siempre es interpretada por la estación de administración.
- Cuando está activada la opción Pasar todas las pulsaciones de teclas al servidor, las pulsaciones de teclas siguientes no se envían al sistema administrado:
  - Tecla Atrás del explorador
  - Tecla Adelante del explorador
  - Tecla Actualizar del explorador
  - Tecla Detener del explorador
  - Tecla Buscar del explorador
  - Tecla Favoritos del explorador
  - Tecla Inicio y Página inicial del explorador
  - Tecla de silencio de volumen
  - Tecla de reducción de volumen
  - Tecla de aumento de volumen
  - Tecla de pista siguiente
  - Tecla de pista anterior
  - Tecla Detener medios
  - Tecla Reproducir/pausar medios
  - Tecla Iniciar correo
  - Tecla Seleccionar medios
  - Tecla Iniciar aplicación 1
  - Tecla Iniciar aplicación 2
- Todas las teclas individuales (no una combinación de diferentes teclas, sino una pulsación única de tecla) siempre se envían al sistema administrado. Esto incluye todas las teclas de función, las teclas Mayús, Alt y Ctrl, y las teclas de menú. Algunas de estas teclas afectan tanto la estación de administración como el sistema administrado.

  Por ejemplo, si la estación de administración y el sistema administrado ejecutan el sistema operativo Windows y la opción Pass All Keys (Pasar todas las teclas) está deshabilitada, al presionar la tecla Windows para abrir el menú **Inicio**, el menú **Inicio** se abre en la estación de administración y en el sistema administrado. Sin embargo, si la opción Pass All Keys (Pasar todas las teclas) está habilitada, 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 Pet Sis 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 Pet Sis 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 Pass all keystrokes to server (Pasar todas las pulsaciones de teclas al servidor) está activada, las teclas mágicas Pet Sis 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 Pet Sis están habilitadas o deshabilitadas 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 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 cuadro de diálogo de inicio de sesión `localhost.localdomain` Inicie sesión mediante el nombre de usuario y la contraseña del sistema operativo.
3. Si Pet Sis no está habilitado, actívelo mediante `echo 1 >/proc/sys/kernel/sysrq`.
4. Ejecute la secuencia de interrupción `~B`.
5. Use la tecla mágica Pet Sis para habilitar la función Pet Sis. Por ejemplo, con el siguiente comando es posible ver la información de memoria en la consola:

   ```
   echo m > /proc/sysrq-trigger displays
   ```

Uso de SSH o conector serie externo con conexión directa a través de un cable en serie

1. Para las sesiones de SSH, después de iniciar sesión con el nombre de usuario y la contraseña de iDRAC, en el símbolo del sistema `/admin>`, ejecute el comando `console com2`. Aparece el símbolo del sistema `localhost.localdomain`.
2. Para la redirección de consola mediante el conector serie externo conectado directamente al sistema mediante un cable en serie, la solicitud de inicio de sesión `localhost.localdomain` aparece después de que el servidor arranca 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 usando `echo 1 >/proc/sys/kernel/sysrq`.
5. Utilice la tecla mágica para activar la función SysRq. Por ejemplo, el siguiente comando reinicia el servidor:

   ```
   echo b > /proc/sysrq-trigger
   ```

   NOTA: No es necesario ejecutar la secuencia de interrupción antes de usar las teclas mágicas de SysRq.

Sesión de consola virtual basada en ActiveX que se ejecuta en el sistema operativo Windows

El comportamiento de la opción de pasar todas las pulsaciones de teclas al servidor en una sesión de consola virtual basada en ActiveX que se ejecuta en un sistema operativo de Windows es similar al comportamiento explicado para una sesión de consola virtual basada en Java que se ejecuta en la estación de administración de Windows con las excepciones siguientes:

- Cuando la opción Pasar todas las pulsaciones de teclas está desactivada, si presiona F1 se iniciará la ayuda de la aplicación tanto en la estación de administración como en el sistema administrado. También se mostrará el mensaje siguiente:

  ```
  Click Help on the Virtual Console page to view the online Help
  ```

- Es posible que las teclas multimedia no se bloqueen explícitamente.
- Las combinaciones <Alt + Espacio>, <Ctrl + Alt + +>, <Ctrl + Alt + -> no se envían al sistema administrado y son interpretadas por el sistema operativo en la estación de administración.

21

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 la iDRAC con información de supervisión del sistema operativo. Complementa la iDRAC mediante la entrega de datos adicionales para trabajar con las interfaces de la 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. Se agregó la interfaz de línea de comandos del sistema operativo host para habilitar o deshabilitar el estado del ciclo de encendido completo de todos los componentes del sistema, excepto la PSU.

NOTA: 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/Datacenter 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: Si realiza el borrado de LC `idrac.Servicemodule`, es posible que los valores sigan apareciendo como los valores antiguos.

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 privilegios de administrador en el sistema operativo del servidor para instalar iDRAC Service Module. Para obtener información acerca de la instalación, consulte iDRAC Service Module User's Guide (Guía del usuario del módulo de servicio de la iDRAC) disponible en www.dell.com/idracservicemodule.

NOTA: Esta función no es aplicable para los sistemas Dell Precision PR7910.

Instalación de iDRAC Service Module desde iDRAC Express e iDRAC Basic

En la página **iDRAC Service Module Setup (Configuración de iDRAC Service Module)**, haga clic en **Install Service Module (Instalar Service Module)**.

1. El instalador de Service Module está disponible para el sistema operativo host y se crea un trabajo en la iDRAC.

Para sistemas operativos Microsoft Windows o Linux, inicie sesión en el servidor de manera local o remota.

2. Busque 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 de procesamiento en lote **ISM-win.bat**.
   - En Linux, abra el símbolo del sistema del shell y ejecute el archivo de secuencia de comandos **ISM-Lx.sh**.
3. Una vez finalizada la instalación, la iDRAC mostrará Service Module como **Installed (Instalado)** y la fecha de instalación.

   NOTA: El instalador estará disponible para el sistema operativo host durante 30 minutos. Si no inicia la instalación dentro de los 30 minutos, deberá reiniciarla.

Instalación de iDRAC Service Module desde iDRAC Enterprise

1. En el asistente **SupportAssist Registration (Registro de SupportAssist)**, haga clic en **Next (Siguiente)**.
2. En la página **iDRAC Service Module Setup (Configuración iDRAC Service Module)**, haga clic en **Install Service Module** (**Instalar Módulo de servicio**).
3. Haga clic en **Launch Virtual Console (Iniciar consola virtual)** y en **Continue (Continuar)** en el cuadro de diálogo de advertencia de seguridad.
4. Para localizar el archivo del instalador de iSM, inicie sesión en el servidor de manera local o remota.

   NOTA: El instalador estará disponible para el sistema operativo host durante 30 minutos. Si no inicia la instalación dentro de los 30 minutos, deberá reiniciar la instalación.

5. Busque 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 de procesamiento en lote **ISM-win.bat**.
   - En Linux, abra el símbolo del sistema del shell y ejecute el archivo de secuencia de comandos **ISM-Lx.sh**.
6. Siga las instrucciones que aparecen en la pantalla para completar la instalación.
   En la página **iDRAC Service Module Setup (Configuración de iDRAC Service Module)**, se deshabilitará el botón **Install Service Module (Instalar Service Module)** después de finalizar la instalación, y el estado de Service Module figurará como **Running (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 User's Guide (Guía del usuario del módulo de servicio de iDRAC) disponible en www.dell.com/idracservicemodule.

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.

- Prepárese para quitar el SSD de PCIe de NVMe Para obtener más informaciónhttps://www.dell.com/support/article/sln310557 .
- Ciclo de apagado y encendido del servidor remoto

Compatibilidad de perfil de Redfish para atributos de red

iDRAC Service Module versión 2.3 o posterior proporciona atributos de red adicionales para la iDRAC, que pueden obtenerse mediante los clientes REST desde la iDRAC. Para obtener más detalles, consulte compatibilidad de perfil de Redfish de la 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 iSM versión 2.0 o posteriores, se modificó la función de información del sistema operativo con la supervisión de la interfaz de red del sistema operativo. Cuando iDRAC Service Module versión 2.0 se utiliza con la 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 **Registro del sistema operativo** seleccionada como destino (en la página **Alertas** o en las interfaces equivalentes de RACADM o WSMan) se replican en el registro del sistema operativo mediante el módulo de servicio del iDRAC. El conjunto predeterminado de registros que se va a incluir en los registros del sistema operativo es igual que el valor configurado para las alertas o capturas de SNMP.

El módulo de servicio del iDRAC también registra los sucesos ocurridos cuando el sistema operativo no funciona. Los registros del sistema operativo realizados por iDRAC Service Module siguen los estándares de registro del sistema IETF para los sistemas operativos basados en Linux.

NOTA: A partir de la versión 2.1 de iDRAC Service Module, la ubicación de la replicación de los registros de Lifecycle Controller en los registros del sistema operativo Windows puede configurarse mediante el instalador de iDRAC Service Module. Puede configurar la ubicación mientras instala iDRAC Service Module o modificar el instalador de iDRAC Service Module.

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 exista una notificación disponible, pero el servidor se restablece como si el interruptor de alimentación estuviera activado. ASR se implementa mediante un temporizador que cuenta regresivamente de forma continua. Health Monitor vuelve a cargar el contador de manera frecuente para evitar que la cuenta regresiva llegue a cero. Si ASR cuenta regresivamente hasta cero, se supone que el sistema operativo se ha bloqueado y que el sistema intenta reiniciarse automáticamente.

Puede realizar operaciones de recuperación automática del sistema, tales como reinicio, ciclo de encendido o apagado del servidor después de un intervalo de tiempo especificado. Esta función está activada solo si el temporizador de vigilancia del sistema operativo está desactivado. Si OpenManage Server Administrator está instalado, esta función de supervisión se desactiva para evitar la duplicación de los temporizadores de vigilancia.

Proveedores del Instrumental de administración de Windows

Windows Management Instrumentation (WMI) es un conjunto de extensiones para el Modelo de controlador de Windows que proporciona una interfaz de sistema operativo a través de la cual los componentes instrumentados proporcionan información y notificaciones. WMI es la implementación de Microsoft de los estándares de Web-Based Enterprise Management (WBEM) y el Modelo de información común (CIM) del grupo de trabajo de administración distribuida (DMTF) para administrar el hardware del servidor, los sistemas operativos y las aplicaciones. Los proveedores de WMI permiten la integración con las consolas de administración de sistemas (como Microsoft System Center) y permiten las secuencias de comandos para administrar servidores de Microsoft Windows.

Es posible activar o desactivar la opción de WMI en el iDRAC. El iDRAC expone las clases de WMI a través del módulo de servicio del iDRAC y proporciona la información sobre la condición del servidor. De manera predeterminada, se activa la función de información sobre WMI. El módulo de servicio de iDRAC expone las clases supervisadas de WSMan en 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.

Este contenido utiliza las clases **DCIM_iDRACCardString** y **DCIM_iDRACCardInteger** para ilustrar la funcionalidad que la función de información sobre WMI proporciona en el módulo de servicio iDRAC. Para conocer los detalles de las clases y los perfiles compatibles, consulte la documentación sobre perfiles WSMan disponible en https://www.dell.com/support.

Los atributos enumerados se utilizan para configurar las **Cuentas de usuario** junto con los privilegios necesarios:

AttributeName	Clase WSMAN	Privilegio	Licencia	Descripción	Operación compatible
UserName	DCIM_iDRACCardString	**Privilegios de escritura:** ConfigUsers, inicio de sesión **Privilegios de lectura:** inicio de sesión	Básico	16users: Users.1#UserName a Users.16#UserName	Enum, Get, Invoke
Contraseña	DCIM_iDRACCardString	**Privilegios de escritura:** ConfigUsers, inicio de sesión **Privilegios de lectura:** inicio de sesión	Básico	Users.1#Password a Users.16#Password	Enum, Get, Invoke
Privilegio	DCIM_iDRACCardInteger	**Privilegios de escritura:** ConfigUsers, inicio de sesión **Privilegios de lectura:** inicio de sesión	Básico	Users.1#Password a Users.16#Password	Enum, Get, Invoke

- `Enumerate` o la operación `Get` en las clases mencionadas proporcionará los datos relacionados con el atributo.
- El atributo se puede configurar invocando el comando `ApplyAttribute` o `SetAttribute` desde la clase **DCIM_iDRACCardService**.

NOTA: La clase **DCIM_Account** se elimina de WSMAN y se proporciona la función mediante el modelo de atributo. Las clases **DCIM_iDRACCardString** y **DCIM_iDRACCardInteger** proporcionan soporte similar para configurar cuentas de usuarios de iDRAC.

Restablecimiento forzado remoto del iDRAC

Mediante iDRAC, puede supervisar los servidores admitidos en busca de problemas críticos de hardware, firmware o software del sistema. A veces, es posible que la iDRAC deje de responder debido a diversas razones. En estos casos, debe apagar el servidor y restablecer la iDRAC. Para restablecer la CPU de la iDRAC, debe apagar y encender el servidor o realizar un ciclo de encendido de CA.

Mediante la función de restablecimiento forzado remoto de la iDRAC, cada vez que la iDRAC no responda, podrá realizar una operación de restablecimiento remoto de la iDRAC sin un ciclo de encendido de CA. Para restablecer la iDRAC de manera remota, asegúrese de que tiene privilegios de administrador en el sistema operativo host. De manera predeterminada, la función de restablecimiento forzado remoto de la iDRAC está habilitada. Puede realizar un restablecimiento forzado remoto de iDRAC 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?
    InstanceID="iSMExportedFunctions" -u:<admin-username> -p:<admin-password> -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 programas** del sistema operativo Windows. Cuando seleccione la opción **Restablecimiento forzado remoto de la iDRAC**, se le pedirá una confirmación para restablecer la iDRAC. Después de confirmar, la iDRAC se restablece y se muestra el resultado de la operación.

  NOTA: Aparecerá el siguiente mensaje de advertencia en la categoría **Registros de aplicación** en el **Visor de eventos**. Esta advertencia no requiere ninguna acción adicional.

  NOTA: `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**

  iSM proporciona un comando ejecutable en todos los sistemas operativos Linux compatibles con iSM. Puede ejecutar este comando iniciando sesión en el sistema operativo mediante SSH o 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 la iDRAC no se restaura completamente después del restablecimiento. Asegúrese de restablecer manualmente la iDRAC.

Tabla 59. 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 la iDRAC sin configurar la iDRAC, y administrar el servidor de manera remota configurando las excepciones y el destino de SNMP en el sistema operativo host. En iDRAC Service Module versión 2.3 o posterior, esta función convierte en excepciones de SNMP todos los registros de Lifecycle replicados en los registros del sistema operativo.

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 alerta de SNMP dentro de banda puede coexistir con el mecanismo de alertas de SNMP de la iDRAC, es posible que los registros guardados tengan alertas de SNMP redundantes de ambas fuentes. Se recomienda utilizar la opción dentro de banda o fuera de banda, en lugar de utilizar 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 iniciando sesión en el sistema operativo mediante SSH o 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 especificó, 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** permite configurar Net-SNMP para reenviar las excepciones. No obstante, debe configurar el destino de la excepción.

- **Sistema operativo ESXi VMware**

  En todos los sistemas operativos ESXo 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 la documentación técnica **In-BandSNMPAlerts** disponible en https://www.dell.com/support.

Acceso al iDRAC a través del sistema operativo del host

Cuando utiliza esta función, puede configurar y supervisar los parámetros de hardware a través de la interfaz web de iDRAC, WSMan y las interfaces de RedFish usando la dirección IP del host sin configurar la dirección IP de iDRAC. Puede utilizar las credenciales predeterminadas de la iDRAC si el servidor de la iDRAC no está configurado, o continuar usando las mismas credenciales de la iDRAC si el servidor de la iDRAC se configuró 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 el paquete web. Esta función está deshabilitada en una instalación de iSM típica. Si está habilitada, el número de puerto de escucha predeterminado es 1266. Puede modificar este número de puerto dentro del rango de 1024 a 65535. iSM redirige la conexión a la iDRAC. Luego, iSM crea una regla de servidor de seguridad de entrada (OS2iDRAC). El número de puerto de escucha se agrega a la regla de servidor de seguridad OS2iDRAC en el sistema operativo host, lo que permite las conexiones de entrada. La regla del servidor de seguridad se habilita automáticamente cuando esta función está habilitada.

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 habilitada o deshabilitada. Cuando la función se encuentra habilitada, aparece 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 la iDRAC, utilice el formato `https://<host-name>` o `OS-IP>:443/login.html` en el navegador, donde:

- `<host-name>` corresponde al nombre completo de host del servidor en el que iSM está instalado y configurado para el acceso a la iDRAC mediante la función del sistema operativo. Puede utilizar la dirección IP del sistema operativo si el nombre de host no está presente.
- `443` corresponde al número de puerto de la iDRAC predeterminado. Este es el número de puerto de conexión al que se redirigen todas las conexiones de entrada del número de puerto de escucha. Puede modificar el número de puerto mediante la interfaz web de iDRAC y las interfaces 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 deshabilitarla o modificarla con el comando PowerShell y las opciones correspondientes. Las opciones disponibles son las siguientes:

- **Estado**: Este parámetro es obligatorio. Los valores no distinguen entre mayúsculas y minúsculas y el valor puede ser **true**, **false** o **get**.
- **Puerto**: Este es número de puerto de escucha. Si no proporciona un número de puerto, se utiliza el número de puerto predeterminado (1266). Si el valor del parámetro **Estado** es FALSE, puede ignorar el resto de los parámetros. Debe introducir un nuevo número de puerto que no esté ya configurado para esta función. El nuevo número de puerto sobrescribe la regla de servidor de seguridad de entrada de OS2iDRAC existente y es posible usar el nuevo número de puerto para conectarse a la iDRAC. El rango de valores abarca de 1024 a 65535.
- **Rango de IP**: Este parámetro es opcional y proporciona una amplia gama de direcciones IP que se pueden conectar a la iDRAC mediante el sistema operativo host. El rango de direcciones IP está en formato de enrutamiento de interdominios sin clases (CIDR), que es una combinación de la dirección IP y la máscara de subred. Por ejemplo: 10.94.111.21/24. El acceso a la iDRAC está restringido para las direcciones IP que no estén dentro del 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 deshabilitada en una instalación típica o predeterminada de iSM. Para comprobar 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

Desactivar

`<source-port>` y `<source-IP-range/source-ip-range-mask>` no son necesarios.

<Enable-Flag>=1

Activar

`<source-port>` es necesario y `<source-ip-range-mask>` es opcional.

<source-IP-range>

El rango de IP debe estar en el formato *<dirección-IP/máscara-de-subred>*. 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 servicios de iDRAC** > **Configurar el módulo de servicios**.
   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.

   NOTA: Cuando un servidor tiene varios sistemas operativos y el módulo de servicios de iDRAC está instalado en todos los sistemas operativos, la iDRAC solo se conecta a la instancia más reciente de iSM entre todos los sistemas operativos. Se muestra un error para todas las instancias anteriores de iSM en otros sistemas operativos. Para conectar iSM con iDRAC en cualquier otro sistema operativo que ya tenga instalado iSM, desinstale y vuelva a instalar iSM en ese sistema operativo en particular.
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 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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

22

Uso de un puerto USB para la administración del servidor

En 14.ª generación de servidores, un puerto micro USB dedicado está disponible para configurar iDRAC. Puede realizar las siguientes funciones con el puerto micro USB:

- Conectarse al sistema mediante la interfaz de red USB para acceder a las herramientas de administración del sistema, como la interfaz web de iDRAC y RACADM.
- Configurar un servidor mediante el uso de archivos SCP almacenados en una unidad USB.

NOTA: Para administrar un puerto USB o configurar un servidor mediante la importación de archivos de perfil de configuración del sistema (SCP) en una unidad USB, debe tener el privilegio de Control del sistema.

NOTA: Se genera una alerta/informe cuando se inserta un dispositivo USB. Esta función solo está disponible en servidores basados en Intel.

Para ajustar la configuración de USB de administración, vaya a **Configuración de iDRAC** > **Configuración** > **Configuración de USB de administración**. Hay disponibles las dos opciones siguientes:

- **Puerto de administración USB**: seleccione **Activado** para habilitar el puerto a fin de importar el archivo SCP cuando una unidad USB está conectada o para acceder a iDRAC mediante el puerto micro USB.

  NOTA: Asegúrese de que la unidad USB contenga un archivo SCP válido.

  NOTA: Utilice un adaptador OTG para pasar de USB Tipo A a Micro-B. Las conexiones de hubs USB no son compatibles.
- **iDRAC administrada: SCP USB**: seleccione una de las opciones siguientes para configurar el sistema mediante la importación de SCP almacenados en una unidad USB:
  - **Desactivado**: desactiva las importaciones de SCP
  - **Activado solamente cuando el servidor tiene una configuración predeterminada de credenciales**: si esta opción está seleccionada, el SCP solo se puede importar cuando no se cambia la contraseña predeterminada para las siguientes opciones:
    - BIOS
    - Interfaz web del iDRAC
  - **Activado solo para archivos de configuración comprimidos**: seleccione esta opción para permitir la importación de archivos SCP solo si estos están en formato comprimido.

    NOTA: Si selecciona esta opción, puede proteger el archivo comprimido con una contraseña. Puede ingresar una contraseña para proteger el archivo mediante la opción **Contraseña para archivo Zip**.
  - **Activado**: seleccione esta opción para permitir la importación de archivos SCP sin la ejecución de una revisión durante el tiempo de ejecución.

Temas:

Acceso a la interfaz de iDRAC por medio de la conexión USB directa

La función iDRAC Direct permite conectar una laptop al puerto USB de iDRAC de manera directa. Esta función permite interactuar directamente con las interfaces de iDRAC, como la interfaz web, RACADM y WSMan, para lograr una administración y un mantenimiento avanzados de los servidores.

Para obtener una lista de los navegadores y los sistemas operativos compatibles, consulte *Notas de la versión de iDRAC* disponibles en https://www.dell.com/idracmanuals.

NOTA: Si utiliza el sistema operativo Windows, quizás deba instalar un controlador RNDIS para usar esta función.

Para acceder a la interfaz de iDRAC por medio del puerto USB:

1. Apague las redes inalámbricas y desconéctelas de cualquier otra red de conexión permanente.
2. Asegúrese de que el puerto USB esté activado. Para obtener más información, consulte Configuración de los valores de puerto de administración USB en la página 321.
3. Espere a que la laptop obtenga la dirección IP 169.254.0.4. Es posible que la obtención de las direcciones IP tarde varios segundos. iDRAC obtiene la dirección IP 169.254.0.3.
4. Empiece a utilizar las interfaces de red de iDRAC, como la interfaz web, RACADM, Redfish o WSMan.
   Por ejemplo, para acceder a la interfaz web de iDRAC, abra un navegador compatible y escriba la dirección *169.254.0.3* y presione Intro.
5. Cuando iDRAC utiliza el puerto USB, el indicador LED parpadea para indicar actividad. La frecuencia es de cuatro parpadeos por segundo.
6. Después de completar las acciones deseadas, desconecte el cable USB del sistema.
   El LED se apagará.

Configuración de iDRAC mediante el perfil de configuración del servidor en un dispositivo USB

Con el puerto de administración USB de iDRAC, se puede configurar iDRAC en el servidor. 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.

Configuración de los valores de puerto de administración USB

Puede habilitar o deshabilitar el puerto USB directo de iDRAC en el BIOS del sistema. Vaya a **BIOS del sistema** > **Dispositivos integrados**. Seleccione **Activar** para habilitar y **Desactivar** para deshabilitar el puerto USB directo de iDRAC.

En iDRAC, es necesario contar con el privilegio de control de servidor para configurar el puerto de administración USB. Cuando existe un dispositivo USB conectado, en la página **Inventario del sistema**, se 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 de iDRAC** > **Configuración** > **Configuración de USB de administración**.
2. El **Puerto de administración USB** se establece en Activado.
3. En el menú desplegable de Configuración **iDRAC administrada: SCP USB**, seleccione opciones para configurar un servidor mediante la importación de archivos de perfil de configuración del servidor almacenados en una unidad USB:
   - **Desactivado**
   - **Activado solamente cuando el servidor contiene configuraciones de credenciales predeterminadas.**
   - **Activado solo para archivos de configuración comprimidos**
   - **Activado**

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

   NOTA: iDRAC9 le permite proteger con contraseña el archivo comprimido después de seleccionar Activado solo para archivos de configuración comprimidos para comprimir el archivo antes de importarlo. Puede ingresar una contraseña para proteger el archivo mediante la opción Contraseña para archivo Zip.
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.PortStatus
```

- Para ver la configuración del puerto USB:

```
racadm get iDRAC.USB.ManagementPortMode
```

- Para ver el inventario del dispositivo USB:

```
racadm hwinventory
```

- Para configurar por medio de la configuración de alertas de exceso de corriente:

```
racadm eventfilters
```

Para obtener más información, consulte *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

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 **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 solo para archivos de configuración comprimidos**
   - **Activado**

   Para obtener información acerca de los campos, consulte la *Ayuda en línea de la utilidad de configuración de iDRAC*.
3. 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 root de un dispositivo USB denominado `System_Configuration_XML` en el que se encuentren los archivos config y control:

- El perfil de configuración del servidor (SCP) 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 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: Durante la importación del SCP, el cambio de los ajustes de administración de USB en el archivo de SCP tiene como resultado un trabajo con errores o un trabajo completado con errores. Puede comentar los atributos en el SCP para evitar 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.

   NOTA: En los archivos XML, se distinguen mayúsculas y minúsculas en el nombre y tipo de archivo. Asegúrese de que ambos estén en minúsculas.
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 inició 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 ajustes 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

Mediante el indicador LED de USB, se señala el estado de una operación de perfil de configuración de servidor que se está llevando a cabo con el puerto USB. Es posible que este LED no esté disponible en todos los sistemas.

- Luz verde fija: se está copiando el perfil de configuración del servidor desde el dispositivo USB.
- Luz verde parpadeante: el trabajo está en curso.
- Luz ámbar parpadeante: no se pudo realizar el trabajo o se completó con errores.
- Luz verde fija: el trabajo se ha completado correctamente.

NOTA: En PowerEdge R840 y R940xa, si hay una pantalla LCD, el indicador LED de USB no parpadea mientras se está realizando una operación de importación con el puerto USB. Compruebe el estado de la operación en la pantalla LCD.

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.

23

Uso de Quick Sync 2

Con Dell OpenManage Mobile en un dispositivo móvil Android o iOS, puede acceder fácilmente al servidor directamente o a través de OpenManage Essentials o la consola OpenManage Enterprise (OME). Le permite revisar detalles del servidor y el inventario, ver LC y los registros de eventos del sistema, obtener notificaciones automáticas en un dispositivo móvil desde una consola de OME, asignar direcciones IP y modificar la contraseña de iDRAC, configurar atributos clave del BIOS y tomar acciones correctivas, según sea necesario. También puede realizar un ciclo de apagado y encendido de un servidor, acceder a la consola del sistema o acceder a la GUI de iDRAC.

OMM se puede descargar de manera gratuita en Apple App Store o Google Play Store.

Debe instalar la aplicación OpenManage Mobile en el dispositivo móvil (compatible con dispositivos móviles Android 5.0+ y iOS 9.0+) para administrar el servidor mediante la interfaz Quick Sync 2 de iDRAC.

NOTA: Esta sección aparece solo en los servidores que tienen el módulo de Quick Sync 2 en la orejeta del rack izquierdo.

NOTA: Esta función es compatible actualmente con dispositivos móviles con sistema operativo Android y Apple iOS.

En la versión actual, esta función está disponible en toda la 14.ª generación de servidores PowerEdge. Es necesario tener dispositivos móviles habilitados para el panel de control izquierdo de Quick Sync 2 (integrado en la **orejeta del rack izquierda**) y Bluetooth de bajo consumo (y, opcionalmente, Wi-Fi). Por lo tanto, es una venta incremental de hardware y las funcionalidades no dependen de las licencias de software de iDRAC.

NOTA: Para obtener más información sobre cómo configurar Quick Sync 2 en sistemas de plataforma MX, consulte la *Guía del usuario de OpenManage Enterprise Modular* y la *Guía del usuario de OpenManage Mobile* disponibles en **dell.com/support/manuals**.

Los procedimientos de configuración de Quick Sync 2 de iDRAC son los siguientes:

NOTA: No corresponde a plataformas MX.

Una vez que se ha configurado Quick Sync 2, habilite el botón de Quick Sync 2 en el panel de control izquierdo. Asegúrese de que la luz de Quick Sync 2 se encienda. Acceda a la información de Quick Sync 2 mediante un dispositivo móvil (Android 5.0+ o IOS 9.0+, OMM 2.0 o superior).

Con OpenManage Mobile, es posible:

- Ver información de inventario
- Ver información de supervisión
- Configurar los valores de red básicos de iDRAC

Para obtener más información acerca de OpenManage Mobile, consulte *Guía del usuario de Dell EMC OpenManage Mobile* disponible en https://www.dell.com/openmanagemanuals.

Temas:

Configuración de Quick Sync 2 de iDRAC

Con la interfaz web de iDRAC, RACADM, WSMan e iDRAC HII, se puede configurar la función de Quick Sync 2 de iDRAC para permitir el acceso al dispositivo móvil:

- **Acceso**: configúrelo a De lectura y escritura, Solo lectura y Desactivado. La opción predeterminada es De lectura y escritura.
- **Tiempo de espera**: configúrelo en Activado o Desactivado. La opción predeterminada es Activado.
- **Límite de tiempo de espera**: 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 se encuentra entre 120 y 3600 segundos.

1. Si lo activa, puede especificar una hora después de la cual el modo de Quick Sync 2 se apaga. Para activarlo, pulse el botón de activación de nuevo.
2. Si está desactivado, el temporizador no le permite introducir un período de tiempo de espera.

- **Autenticación de lectura**: se configura en Activado. Esta es la opción predeterminada.
- **Wi-Fi**: se configura en Activado. 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 Quick Sync 2 en el panel de control izquierdo. Asegúrese de que la luz de Quick Sync se encienda. A continuación, acceda a la información de Quick Sync desde un dispositivo móvil.

Se registra una entrada en el registro de Lifecycle Controller cuando se modifica la configuración.

Configuración de los ajustes de la sincronización rápida 2 de la iDRAC mediante la interfaz web

Para configurar la sincronización rápida 2 de la iDRAC:

1. En la interfaz web de la iDRAC, vaya a **Configuration (Configuración)** > **Systems Settings (Configuración del sistema)** > **Hardware Settings (Configuración de hardware)** > **iDRAC Quick Sync (Sincronización rápida de la iDRAC)**.
2. En la sección **iDRAC Quick Sync (Sincronización rápida de la iDRAC)**, en el menú **Access (Acceso)**, seleccione una de las siguientes opciones para proporcionar acceso al dispositivo móvil Android o iOS:
   - Lectura/escritura
   - Solo lectura
   - Desactivado
3. Active el temporizador.
4. Especifique el valor de expiración de tiempo.

   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 ajustes de iDRAC Quick Sync 2 mediante RACADM

Para configurar la función iDRAC Quick Sync 2, utilice los objetos racadm del grupo **System.QuickSync**. Para obtener más información, consulte *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

Configuración de los valores de sincronización rápida 2 de la iDRAC mediante la utilidad de configuración de la iDRAC

Para configurar la sincronización rápida 2 de la iDRAC:

1. En la interfaz gráfica del usuario de la iDRAC, vaya a **Configuration (Configuración)** > **Systems Settings (Configuración del sistema)** > **Hardware Settings (Configuración de hardware)** > **iDRAC Quick Sync (Sincronización rápida de la iDRAC)**.
2. En la sección **Sincronización rápida del iDRAC**:
   - Especifique el nivel de acceso.
   - Active el tiempo de espera.
   - Especifique el límite de expiración de tiempo definido por el usuario (el rango es de 120 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 la iDRAC desde el dispositivo móvil, consulte *Guía del usuario de Dell EMC OpenManage Mobile* disponible en https://www.dell.com/openmanagemanuals para ver los pasos necesarios.

24

Administración de medios virtuales

iDRAC proporciona medios virtuales con un cliente basado en HTML5 con un archivo IMG e ISO local, compatibilidad con archivos ISO e IMG remotos. 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. Necesita el privilegio de Configuración de iDRAC para modificar la configuración.

A continuación, se presentan los atributos configurables:

- Medios conectados habilitados: habilitado/deshabilitado
- Modo de conexión: conexión automática, conectado y desconectado
- Máx. de sesiones: 1
- Sesiones activas: 1
- Cifrado de medios virtuales: habilitado (de manera predeterminada)
- Emulación de disco flexible: deshabilitado (de manera predeterminada)
- Inicio único: habilitado / deshabilitado
- Estado de conexión: conectado / desconectado

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 de estante y torre. Está disponible de manera predeterminada para los servidores blade.

Las características claves son las siguientes:

- Los medios virtuales son compatibles con unidades ópticas virtuales (CD/DVD) y unidades flash USB.
- Puede conectar a un sistema administrado una sola unidad flash USB, imagen o clave y una unidad óptica en la estación de administración. Entre las unidades ópticas compatibles, se incluyen 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.

- Todo medio virtual emula un dispositivo físico del sistema administrado.
- En sistemas administrados basados en Windows, las unidades de medios virtuales se montan automáticamente si están conectados y configurados con una letra de unidad.
- Con algunas configuraciones en los sistemas administrados basados en Linux, las unidades de medios virtuales no se montan automáticamente. Para montarlas manualmente, utilice el comando mount.
- Todas las solicitudes de acceso a la unidad virtual desde el sistema administrado se dirigen a la estación de administración a través de la red.
- Los dispositivos virtuales aparecen como dos unidades en el sistema administrado sin los medios que se están instalando en las unidades.
- Entre dos sistemas administrados se puede compartir la unidad CD/DVD (solo lectura) de la estación de administración, pero no un medio USB.
- Los medios virtuales requieren un ancho de banda de red mínimo disponible de 128 Kbps.
- Si se produce una conmutación por error LOM o NIC, es posible que se desconecte la sesión de medios virtuales.

Después de conectar una imagen de medios virtuales a través de la consola virtual, puede que la unidad no se muestre en el sistema operativo del host de Windows. Revise el administrador de dispositivos de Windows en búsqueda de cualquier dispositivo de almacenamiento masivo desconocido. Haga clic con el botón secundario en el dispositivo desconocido y actualice el controlador o seleccione la desinstalación del controlador. Windows reconoce el dispositivo después de desconectar y volver a conectar vMedia.

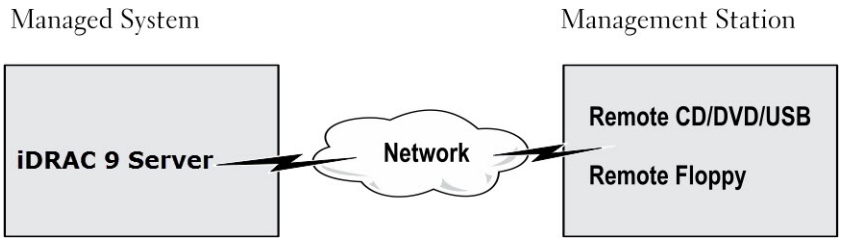


Ilustración 4. Configuración de medios virtuales

Temas:

Unidades y dispositivos compatibles

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

Tabla 60. Unidades y dispositivos compatibles

Unidad	Medios de almacenamiento compatibles
Unidades ópticas virtuales	• CD-ROM • DVD • CD-RW • Unidad combinada con medios CD-ROM
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 la iDRAC mientras ejecuta una sesión de medios virtuales. Si lo hace, es posible que se produzcan resultados no deseados, incluida la pérdida de datos.

1. En la interfaz web de la iDRAC, vaya a **Configuration (Configuración)** > **Virtual Media (Medios virtuales)** > **Attached Media (Medios conectados)**.
2. Especifique la configuración necesaria. 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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.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 la 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 **Virtual Media (Medios virtuales)**, seleccione **Detach (Desconectar)**, **Attach (Conectar)** o **Auto attach (Conectar automáticamente)** en función de lo que necesite. Para obtener más información acerca de las opciones, consulte la *Ayuda en línea de la utilidad de configuración de la 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 61. Estado de medios conectados y respuesta del sistema

Estado de los medios conectados	Respuesta del sistema
Desconectar	No se puede asignar una imagen al sistema.
Conectar	Los medios se asignan, incluso cuando se cierre la **Vista de cliente**.
Conexión automática	Los medios se asignan cuando se abre la **Vista de cliente** y su asignación se anula cuando se cierra la **Vista de cliente**.

Configuración del servidor para ver los dispositivos virtuales en los medios virtuales

Es necesario configurar los siguientes ajustes en la estación de administración para habilitar la visualización de unidades vacías. Para ello, en el explorador de Windows, en el menú **Organizar**, haga clic en **Opciones de carpeta y de búsqueda**. En la ficha **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, aparecerá el siguiente mensaje de error: *Virtual Media is currently unavailable (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 la iDRAC, vaya a **Configuration (Configuración)** > **Virtual Console (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 los medios virtuales cuando la **Consola virtual** está deshabilitada, asegúrese de que el sistema esté configurado para mostrar las unidades vacías. Para ello, en Explorador de Windows, vaya a **Opciones de carpeta**, desactive la opción **Ocultar las unidades vacías en la carpeta Mi PC** y haga clic en **Aceptar**.

Realice lo siguiente para acceder a los medios virtuales cuando la consola virtual está desactivada:

1. En la interfaz web de iDRAC, vaya a **Configuración** > **Medios virtuales**.
2. Haga clic en **Conectar medios virtuales**.

De manera alternativa, también puede iniciar los medios virtuales si realiza los siguientes pasos:

1. Vaya a **Configuración** > **Consola virtual**.
2. Haga clic en **Iniciar Consola virtual**. Aparece el mensaje siguiente:

```
Virtual Console has been disabled. Do you want to continue using Virtual Media
redirection?
```

3. Haga clic en **Aceptar**. Aparece la ventana **Medios virtuales**.
4. Desde el menú **Medios virtuales**, haga clic en **Asignar CD/DVD** o **Asignar disco extraíble**. Para obtener más información, consulte Asignación de unidad virtual.
5. **Estadísticas de medios virtuales** muestra la lista de unidades de destino, la asignación, el estado (solo lectura o no), la duración de la conexión, los bytes de lectura/escritura y la velocidad de transferencia.

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 sistemas que ejecutan el sistema operativo Windows configurados con la seguridad mejorada de Internet Explorer. Para resolver este problema, consulte la documentación del sistema operativo de Microsoft o comuníquese con el administrador del sistema.

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, haga clic en **Tools (Herramientas)** > **Stats (Estadísticas)** en el visor de la consola virtual. 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.

Cómo obtener acceso a los controladores

Los servidores Dell EMC PowerEdge tienen todos los controladores de sistema operativo compatibles incorporados en la memoria flash del sistema. Con iDRAC, puede montar o desmontar fácilmente los controladores para implementar el sistema operativo en el servidor.

Realice lo siguiente para montar los controladores:

1. En la interfaz web de iDRAC, vaya a **Configuración** > **Medios virtuales**.
2. Haga clic en **Montar controladores**.
3. Seleccione el sistema operativo en la ventana emergente y, a continuación, haga clic en **Montar controladores**.

   NOTA: La duración de exposición predeterminada es de 18 horas.

Realice lo siguiente para desmontar los controladores luego de finalizar el montaje:

1. Vaya a **Configuración** > **Medios virtuales**.
2. Haga clic en **Desmontar controladores**.
3. Haga clic en **Aceptar** en la ventana emergente.

NOTA: Es posible que no se muestre la opción **Montar controladores** si el paquete de controladores no está disponible en el sistema. Asegúrese de descargar e instalar el paquete de controladores más reciente desde https://www.dell.com/support.

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: Mientras utiliza medios virtuales basados en Java o ActiveX, debe disponer de privilegios de administración para asignar una unidad flash USB o un DVD de sistema operativo (que esté conectado a la estación de administración). Para asignar las unidades, inicie Internet Explorer como administrador o agregue la dirección IP de la 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

   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 las unidades USB, CD o DVD mediante la consola virtual basada en HTML5.
   - No es posible asignar las memorias USB como discos de medios virtuales mediante la consola virtual o los medios virtuales en una sesión de RDP.
   - No puede asignar medios físicos con formato NTFS en medios extraíbles ehtml; utilice dispositivos FAT o exFAT

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.

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 y disco extraíble) 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 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.

   NOTA:
   - La opción **Solo lectura** aparecerá en gris en medios extraíbles Java basados en ehtml5.
   - La emulación de disco flexible no se admite en el plug-in de ehtml5.

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 **Cliente** de medios virtuales puede mostrar discos extraíbles que no forman parte de la estación de administración. Para asegurarse de que las unidades virtuales correctas estén disponibles para la asignación, debe habilitar el ajuste de puerto para la unidad de disco duro SATA conectada. Para hacerlo:

1. Reinicie el sistema operativo en la estación de administración. Durante la POST, presione <F2> para entrar a **Configuración del sistema**.
2. Vaya a **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 **Cliente** de medios virtuales. Muestra 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 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 verlo.

NOTA: Para desasignar una unidad DVD virtual en el 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 habilitada y figure como el primer dispositivo con medios de inicio. Si es necesario, siga las instrucciones en pantalla para modificar el orden de arranque.
5. Haga clic en **Aceptar**, vuelva a **Configuración del BIOS del sistema** y haga clic en **Terminar**.
6. Haga clic en **Sí** para guardar los cambios y salir.

   El sistema administrado reinicia.

   El sistema administrado intenta iniciar desde un dispositivo de inicio según el orden de arranque establecido. Si el dispositivo virtual está conectado y hay un medio de inicio presente, el sistema se inicia con el dispositivo virtual. De lo contrario, el sistema omite el dispositivo, de manera similar a lo que ocurre con 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.

25

Administración de la tarjeta vFlash SD

NOTA: vFlash es compatible con los servidores de plataforma AMD.

La tarjeta vFlash SD es una tarjeta Secure Digital (SD) que se puede pedir e instalar de fábrica. Puede utilizar una tarjeta con un máximo de 16 GB de capacidad. Después de insertar la tarjeta, debe habilitar la funcionalidad vFlash para crear y administrar particiones. La función vFlash requiere licencia.

NOTA: No hay limitación del tamaño de la tarjeta SD, puede abrir y reemplazar la tarjeta SD instalada de fábrica por una tarjeta SD de mayor capacidad. Dado que vFlash utiliza el sistema de archivos FAT32, el tamaño del archivo se limita 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 **Descripción general** > **Servidor** > **vFlash**:

```
SD card not detected. Please insert an SD card of size 256MB or greater.
```

NOTA: Asegúrese de insertar una tarjeta SD vFlash compatible en la ranura para tarjetas vFlash iDRAC. Si inserta una tarjeta SD no compatible, se muestra el siguiente mensaje de error al inicializar la tarjeta: *se produjo 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. Estas particiones, cuando se conectan, se exponen al sistema como una unidad de disco flexible virtual, una unidad de disco duro o una unidad de CD/DVD según el modo de emulación seleccionado.
- Se pueden crear particiones a partir de 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 venza durante una operación de vFlash. Si sucede esto, las operaciones de vFlash en curso se completan normalmente.

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 *Manual de instalación y servicio* disponible en https://www.dell.com/poweredgemanuals.

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 SD vFlash, en la interfaz web de la iDRAC, vaya a **Configuration (Configuración)** > **System Settings (Configuración del sistema)** > **Hardware Settings (Configuración de hardware)** > **vFlash**. Aparecerá la página de 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 SD vFlash 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 acerca de estos objetos, consulte *Guía de la CLI de RACADM para iDRAC* disponible en https://www.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 SD vFlash, en **iDRAC Settings Utility (Utilidad de configuración de la iDRAC)**, vaya a **Media and USB Port Settings (Configuración de medios y puertos USB)**. Aparecerá la página **Media and USB Port Settings (Configuración de medios y puertos USB)** con las propiedades. Para obtener información sobre las propiedades que aparecen, consulte la *Ayuda en línea de la utilidad de configuración de la 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 la iDRAC, vaya a **Configuration (Configuración)** > **System Settings (Configuración del sistema)** > **Hardware Settings (Configuración de hardware)** > **vFlash**.
   Aparece la página **Propiedades de la tarjeta SD**.
2. Seleccione o deseleccione la opción **vFlash Enabled (vFlash habilitado)** 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 solo funcionará si hay una tarjeta SD vFlash presente. Si no hay una tarjeta presente, aparece el siguiente mensaje: *ERROR: SD Card not present (ERROR: Tarjeta SD ausente)*.

Activación o desactivación de la funcionalidad vFlash mediante la utilidad de configuración de iDRAC

Para activar o desactivar la funcionalidad vFlash:

1. En la utilidad de configuración de iDRAC, vaya a **Configuración de medios y puertos USB**.
   Aparecerá la página **iDRAC Settings (Configuración de la iDRAC) Media and USB Port Settings (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 la iDRAC, vaya a **Configuration (Configuración)** > **System Settings (Configuración del sistema)** > **Hardware Settings (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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.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**.
   Aparecerá la página **iDRAC Settings (Configuración de la iDRAC) Media and USB Port Settings (Configuración de medios y puertos USB)**.
2. Haga clic en **Inicializar vFlash**.
3. Haga clic en **Yes (Sí)**. Se iniciará la operación de inicialización.

4. Haga clic en **Back (Atrás)** y vaya a la misma página **iDRAC Settings (Configuración de la iDRAC) Media and USB Port Settings (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 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 de vFlash, utilice el comando: `racadm vflashpartition status -a`
4. Para obtener el último estado de una partición en particular, 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 otro modo, debe disponer del privilegio **Access Virtual Media (Acceder a los medios virtuales)** para crear, eliminar, formatear, conectar, desconectar o copiar el contenido de 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 (como WSMan, la utilidad de configuración de la iDRAC o RACADM), o si desea desplazarse a otra página de la interfaz gráfica del usuario, es posible que la iDRAC muestre el siguiente mensaje: `vFlash is currently in use by another process. Try again after some time` (Otro proceso está utilizando vFlash en este momento. Intente de nuevo más tarde).

La herramienta vFlash es capaz de crear particiones rápidamente cuando no hay otras operaciones de vFlash en curso, tal como el formateo, la conexión de particiones, etc. Por lo tanto, es recomendable 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 SD vFlash. Es posible crear particiones tipo *disquete* o *disco duro*. Las particiones tipo CD solo se admiten cuando se crean particiones mediante imágenes.

Antes de crear una partición vacía, asegúrese de lo siguiente:

- Dispone de privilegios **Acceder a los medios virtuales**.
- La tarjeta está inicializada.
- La tarjeta no está protegida contra escritura.
- No se está realizando una operación de inicialización en la tarjeta.

Creación de una partición vacía mediante la interfaz web

Para crear una partición vFlash vacía:

1. En la interfaz web de la iDRAC, vaya a **Configuration (Configuración)** > **Systems 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 creará una nueva partición vacía no formateada que, de manera predeterminada, es de solo lectura. Aparecerá 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 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]
   ```

   en el que `[n]` corresponde al tamaño de la partición.

   De manera predeterminada, se crea una partición vacía con derechos de lectura y escritura.

   Si el recurso compartido no se configura mediante el nombre de usuario o la contraseña, debe especificar los parámetros como

   ```
   -u anonymous -p anonymous
   ```

   .

Creación de una partición mediante un archivo de imagen

Puede crear una partición nueva en la tarjeta SD vFlash SD mediante un archivo de imagen (disponible en el formato **.img** o **.iso**). Las particiones son de tipos de emulación: disquete (**.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: La imagen cargada y el tipo de emulación deben coincidir. Existen problemas cuando la 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 podrá iniciarse 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 debe ser menor o igual que 4 GB, ya que el tamaño máximo admitido de la partición es 4 GB. No obstante, cuando cree una partición mediante un navegador web, el tamaño de archivo de imagen debe ser menor que 2 GB.

NOTA: La partición de vFlash es un archivo de imagen que se encuentra en un sistema de archivos FAT32. Por lo tanto, el archivo de imagen tiene la limitación de 4 GB.

NOTA: La instalación de un sistema operativo completo no es compatible.

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 la iDRAC, vaya a **Configuration (Configuración)** > **Systems Settings (Configuración del sistema)** > **Hardware Settings (Configuración de hardware)** > **vFlash** > **Create From Image (Crear a partir de imagen)**.
   Aparece la página **Crear partición a partir de archivo de imagen**.
2. Introduzca la información necesaria y haga clic en **Aplicar**. Para obtener más información acerca de estas opciones, consulte la *Ayuda en línea de iDRAC*.

   Se creará una nueva partición. Para el tipo de emulación de CD, se crea una partición de solo lectura. Para los tipos de emulación de disquete o disco duro, se crea una partición de lectura y 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 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 otorga acceso de solo lectura. Este comando distingue mayúsculas de minúsculas en la extensión del nombre del archivo de imagen. Si la extensión del nombre del archivo está en mayúscula, por ejemplo, FOO.ISO en lugar de FOO.iso, el comando arroja 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.

Si el recurso compartido no se configura mediante el nombre de usuario o la contraseña, debe especificar los parámetros como

```
-u anonymous -p anonymous
```

.

Formateo de una partición

Puede formatear una partición existente en la tarjeta SD vFlash 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 de tipo disco duro o disquete (no 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 la iDRAC, vaya a **Configuration (Configuración)** > **System Settings (Configuración del sistema)** > **Hardware Settings (Configuración de hardware)** > **vFlash** > **Format (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 según 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 la iDRAC, vaya a **Configuration (Configuración)** > **System Settings (Configuración del sistema)** > **Hardware Settings (Configuración de hardware)** > **vFlash** > **Manage (Administrar)**. Aparecerá la página **Manage Partitions (Administrar particiones)** con una lista de las particiones disponibles y la información relacionada para cada partición. Para obtener información sobre las particiones, consulte la *Ayuda en línea de la iDRAC*.

Visualización de las particiones disponibles mediante RACADM

Para ver las particiones disponibles y sus propiedades en mediante RACADM:

1. Abra una consola 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 una de 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 la 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. No es posible cambiarlo a lectura y escritura. Si la partición está conectada, la casilla aparece 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 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 escriba:

     ```
     racadm set iDRAC.vflashpartition.<index>.EmulationType <HDD, Floppy, or CD-DVD>
     ```

Conexión o desconexión de particiones

Cuando conecte una o más particiones, estarán visibles para el sistema operativo y el BIOS como dispositivos de almacenamiento masivo USB. Cuando conecte varias particiones, estas se enumeran en orden ascendente en el sistema operativo y en el menú del orden de arranque del BIOS en función del índice asignado.

Si desconecta una partición, esta dejará de ser visible en el sistema operativo y en el menú de orden de inicio del BIOS.

Al conectar o desconectar una partición, se restablece el bus USB del sistema administrado. Esto afecta las aplicaciones que utilizan vFlash y desconecta las sesiones de medios virtuales de la 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 la 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 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 ser compatible con el sistema de archivos de una partición conectada. De lo contrario, no podrá leer ni modificar el contenido de la partición desde el sistema operativo. Por ejemplo, en un entorno de Windows, el sistema operativo no puede leer una partición tipo EXT2, que es nativa de Linux. Del mismo modo, en un entorno de Linux, el sistema operativo no puede leer una partición tipo NTFS, que es nativa de Windows.
- La etiqueta de partición vFlash es diferente del nombre del volumen de sistema de archivos en el dispositivo USB emulado. Puede cambiar el nombre de volumen del dispositivo USB emulado desde el sistema operativo. Sin embargo, el nombre de la etiqueta de partición almacenado en la iDRAC no cambiará.

Eliminación de las particiones existentes

Antes de eliminar el contenido de una partición, asegúrese de lo siguiente:

- La funcionalidad vFlash está activada.
- La tarjeta no está protegida contra escritura.
- La partición no está conectada.
- No se está realizando una operación de inicialización en la tarjeta.

Eliminación de las particiones disponibles mediante la interfaz web

Para eliminar una partición existente:

1. En la interfaz web de la 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 **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 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 la iDRAC, vaya a **Configuration (Configuración)** > **System Settings (Configuración del sistema)** > **Hardware Settings (Configuración de hardware)** > **vFlash** > **Download (Descarga)**.
   Aparece la página **Descargar partición**.
2. Desde el menú desplegable **Etiqueta**, seleccione la partición que desee descargar y haga clic en **Descargar.**

   NOTA: En la lista, figuran todas las particiones existentes (salvo las conectadas). La primera partición está seleccionada de manera predeterminada.

3. Especifique la ubicación donde desea guardar el archivo.
   El contenido de la partición seleccionada se descarga en la ubicación especificada.

   NOTA: Si solo se especifica la ubicación de la carpeta, se utilizará la etiqueta de partición como nombre de archivo, junto con la extensión **.iso** para particiones de CD y disco duro e **.img** para particiones de disco flexible y disco duro.

Inicio de una partición

Se puede establecer una partición vFlash conectada como el dispositivo de inicio para la siguiente operación de inicio.

Antes de iniciar una partición, asegúrese de lo siguiente:

- La partición vFlash contiene una imagen de inicio (en formato **.img** o **.iso**) para realizar el inicio desde el dispositivo.
- La funcionalidad vFlash está activada.
- Dispone de privilegios Acceder a los medios virtuales.

Inicio de una partición mediante la interfaz web

Para establecer la partición vFlash como primer dispositivo de inicio, consulte Inicio de una partición mediante la interfaz web en la página 345.

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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.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 en `1`). La opción de inicio único inicia el dispositivo en la partición solo una vez y no lo mantiene como primero sistemáticamente en el orden de inicio.

26

Uso de SMCLP

NOTA: SMCLP solo se admite en las versiones de iDRAC anteriores a 4.00.00.00.

La especificación del protocolo de línea de comandos de administración de servidor (SMCLP) habilita la administración de sistemas basada en CLI. Define un protocolo para comandos de administración transmitidos a través de flujos orientados a caracteres estándar. Este protocolo accede a un administrador de objetos del modelo de información común (CIMOM) mediante un conjunto de comandos orientados al ser humano. El SMCLP es un subcomponente de la iniciativa SMASH del grupo de trabajo de administración distribuida (DMTF) para simplificar la administración de sistemas en varias plataformas. En la especificación de SMCLP, junto con la especificación de direccionamiento de elementos administrados y las especificaciones de varios perfiles en la asignación de SMCLP, se describen los verbos y destinos estándar para varias 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 de trabajo de administración distribuida (DMTF) para simplificar la administración de servidores en varias plataformas. En la especificación de SM-CLP, junto con la especificación de direccionamiento de elementos administrados y las especificaciones de varios perfiles en la asignación de SM-CLP, se describen los verbos y destinos estándar para varias ejecuciones de tareas de administración.

El SMCLP se aloja en el firmware de la controladora iDRAC y admite SSH e interfaces en serie. La interfaz SMCLP de iDRAC se basa en la especificación de SMCLP versión 1.0 proporcionada por la organización de DMTF.

NOTA: Se puede acceder a la información acerca de los perfiles, las extensiones y los MOF en https://www.dell.com/support y a toda la información sobre DMTF disponible en **dmtf.org/standards/profiles/**.

Los comandos de SM-CLP implementan un subconjunto de comandos de RACADM local. Los comandos son útiles para crear scripts, ya que puede ejecutar estos comandos desde una línea de comando de la estación de administración. Puede recuperar la salida de los comandos en formatos bien definidos, incluido XML, lo que facilita la creación de scripts y la integración en herramientas existentes de administración y creación de informes.

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
- Ver las cuentas de usuario de la iDRAC
- Ver las propiedades del sistema

Ejecución de los comandos SMCLP

Puede ejecutar los comandos de SMCLP mediante la interfaz SSH. Abra un SSH e inicie sesión en iDRAC como administrador. Se mostrará el símbolo del sistema de SMCLP (admin ->).

Símbolos del sistema de SMCLP:

- Los servidores Blade yx1x utilizan `-$`.
- Los servidores tipo rack y torre yx1x utilizan `admin->`.
- Los servidores Blade, rack y torre yx2x utilizan `admin->`.

donde, y es un carácter alfanumérico, tal como M (para servidores Blade), R (para servidores tipo rack) y T (para servidores tipo torre) y x es un número. Esto indica la generación de servidores Dell PowerEdge.

NOTA: Los scripts que utilizan `-$` puede utilizar estos para sistemas yx1x. Sin embargo, a partir de los sistemas yx2x se puede utilizar un script con `admin->` para los servidores tipo Blade, rack y torre.

Sintaxis SMCLP de iDRAC

SMCLP de iDRAC utiliza el concepto de verbos y destinos para proporcionar capacidades de administración de sistemas a través de la CLI. El verbo indica la operación que se debe realizar y el destino determina la entidad (o el objeto) que ejecutará 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 62. 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 63. Destinos de SMCLP

Destino	Definiciones
`admin1`	Dominio de admin
`admin1/profiles1`	Perfiles registrados en iDRAC
`admin1/hdwr1`	Hardware

Tabla 63. Destinos de SMCLP (continuación)

Destino	Definiciones
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

Tabla 63. Destinos de SMCLP (continuación)

Destino	Definiciones
admin1/system1/sp1/clpsvc1	Servicio de protocolo del servicio CLP
admin1/system1/sp1/clpsvc1/clpendpt*	Punto final del protocolo del servicio CLP
admin1/system1/sp1/clpsvc1/tcpendpt*	Punto final TCP del protocolo del servicio CLP
admin1/system1/sp1/jobq1	Cola de trabajo del protocolo del servicio CLP
admin1/system1/sp1/jobq1/job*	Trabajo del protocolo del servicio CLP
admin1/system1/sp1/pwrmgtsvc1	Servicio de administración del estado de la alimentación
admin1/system1/sp1/account1-16	Cuenta de usuario local
admin1/sysetm1/sp1/account1-16/identity1	Cuenta de identidad de usuario local
admin1/sysetm1/sp1/account1-16/identity2	Cuenta de identidad de IPMI (LAN)
admin1/sysetm1/sp1/account1-16/identity3	Cuenta de identidad de IPMI (conexión serie)
admin1/sysetm1/sp1/account1-16/identity4	Cuenta de identidad CLP
admin1/system1/sp1/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

Tabla 63. Destinos de SMCLP (continuación)

Destino	Definiciones
`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 de capacidad de administración (MAP). Una ruta de acceso de dirección especifica la ruta de acceso desde la raíz del espacio de direcciones a un objeto de dicho espacio.

El destino raíz se representa mediante una barra diagonal (/) o una barra diagonal invertida (\). Se trata del punto de inicio predeterminado al iniciar sesión en la iDRAC. Desplácese hasta la raíz mediante el verbo `cd`.

NOTA: La barra diagonal (/) y la barra diagonal invertida (\) son intercambiables en las rutas de acceso de dirección de SM-CLP. Sin embargo, una barra invertida al final de una línea de comandos hace que el comando continúe en la línea siguiente y se omita 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 la ubicación actual en el espacio de direcciones. Las abreviaturas `..` y `.` funcionan de la misma forma que en Windows y Linux: `..` se refiere al nivel superior 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` permite limitar la salida del comando de manera que muestre una o más propiedades, destinos, asociaciones y verbos. Por ejemplo, para mostrar solamente las propiedades y los destinos de la ubicación actual, utilice el siguiente comando:

```
show -display properties,targets
```

Para mostrar solo ciertas propiedades, indíquelas según se muestra en el siguiente comando:

```
show -d properties=(userid,name) /admin1/system1/sp1/account1
```

Si solo desea mostrar una propiedad, puede omitir los paréntesis.

Uso de la opción -level

La opción `show -level` ejecuta el comando `show` en 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 (texto)**, **clpcsv**, **keyword (palabra clave)** y **clpxml**.

El formato predeterminado es **text (texto)** y es la salida que se lee con mayor facilidad. El formato **clpcsv** es un formato de valores separados por coma adecuado para la carga en un programa de hoja de cálculo. El formato **keyword (palabra clave)** produce información como una lista de pares de palabras clave=valor, de a uno por línea. El formato **clpxml** es un documento XML que contiene un elemento XML **response (respuesta)**. DMTF tiene especificados los formatos **clpcsv** y **clpxml**, y dichas especificaciones se encuentran disponibles en el sitio web de DMTF, **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 en la página 351
- Administración de SEL en la página 351
- Navegación en MAP del destino en la página 353

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:

  Escriba `cd . .`

- Para subir un nivel:

  Escriba `cd .. .`

- Para salir:

  ```
  exit
  ```

27

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

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. Mediante el recurso compartido de archivos remotos (RFS), monte el archivo de imagen ISO o IMG en el sistema administrado a través de NFS, CIFS, HTTP o HTTPS.

   NOTA: RFS mediante autenticación HTTP, básica o implícita no es compatible, no se requiere autenticación. En el caso de HTTPS, la autenticación básica no es compatible, solo la autenticación implícita o sin autenticación es compatible.

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.

Managing remote file shares

Using Remote File Share (RFS) feature, you can set an ISO or IMG image file on a network share and make it available to the managed server's operating system as a virtual drive by mounting it as a CD or DVD using NFS, CIFS, HTTP or HTTPs. RFS is a licensed feature.

Remote file share supports only **.img** and **.iso** image file formats. A **.img** file is redirected as a virtual floppy and a **.iso** file is redirected as a virtual CDROM.

You must have Virtual Media privileges to perform an RFS mounting.

RFS and Virtual Media features are mutually exclusive.

- If the Virtual Media client is not active, and you attempt to establish an RFS connection, the connection is established and the remote image is available to the host operating system.
- If the Virtual Media client is active, and you attempt to establish an RFS connection, the following error message is displayed:

  Virtual Media is detached or redirected for the selected virtual drive.

The connection status for RFS is available in iDRAC log. Once connected, an RFS-mounted virtual drive does not disconnect even if you log out from iDRAC. The RFS connection is closed if iDRAC is reset or the network connection is dropped. The Web interface and command-line options are also available in CMCOME Modular and iDRAC to close the RFS connection. The RFS connection from CMC always overrides an existing RFS mount in iDRAC.

NOTE:

- CIFS and NFS supports both IPv4 and IPv6 addresses.
- When the iDRAC is configured with both IPv4 and IPv6, the DNS server can contain records associating the iDRAC hostname to both addresses. If IPv4 option is disabled in iDRAC, then iDRAC may not be able to access the external IPv6 share. This is because the DNS server may still contain IPv4 records, and DNS name resolution can return the IPv4 address. In such cases, it is recommended to delete the IPv4 DNS records from the DNS server, when disabling IPv4 option in iDRAC.
- If you are using CIFS and are part of an Active Directory domain, enter the domain name with the IP address in the image file path.
- If you want to access a file from an NFS share, configure the following share permissions. These permissions are required because iDRAC interfaces run in non-root mode.
  - Linux: Ensure that the share permissions are set to at least **Read** for the **Others** account.
  - Windows: Go to the **Security** tab of the share properties and add **Everyone** to **Groups or user names** field with **Read & execute** privilege.
- If ESXi is running on the managed system and if you mount a floppy image (**.img**) using RFS, the connected floppy image is not available to the ESXi operating system.
- iDRAC vFlash feature and RFS are not related.
- Only English ASCII characters are supported in network share file paths.
- The OS drive eject feature is not supported when virtual media is connected using RFS.
- RFS through HTTP or HTTPs feature is not available on CMC web interface.
- RFS may get disconnected when iDRAC IP is not reachable for more than 1 minute.

Configuración de recursos compartidos de archivos remotos mediante la interfaz web

Para activar el uso compartido de archivos remotos:

1. En la interfaz web de iDRAC, vaya a **Configuración** > **Medios virtuales** > **Medios adjuntos**.
   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 to connect for CIFS file system>/<file path>/<image name>`
   - NFS: `< IP to connect for NFS file system>:/<file path>/<image name>`
   - HTTP: `http://<URL>/<file path>/<image name>`
   - HTTPS: `https://<URL>/<file path>/<image name>`

   NOTA: Para evitar errores de E/S cuando se utilizan recursos compartidos CIFS alojados en sistemas Windows 7, modifique las siguientes claves de registro:
   - Configure HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\LargeSystemCache en `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 información sobre los caracteres recomendados para los nombres de usuario y las contraseñas, consulte Caracteres recomendados para nombres de usuario y contraseñas en la página 154.

NOTA: Los caracteres permitidos en los nombres de usuario y contraseñas para recursos compartidos de red están determinados por el tipo de recurso compartido de red. IDRAC admite caracteres válidos para credenciales de recursos compartidos de red, tal y como lo define el de recurso compartido, excepto <, >, y , (coma).

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.

   NOTA: Si se incluye la información del usuario en la ruta de imagen, utilice HTTPS para evitar que se muestren las credenciales en la GUI y en RACADM. Si ingresa las credenciales en la URL, evite el uso del símbolo "@", debido a que es un carácter separador.

   Para las distribuciones 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
   ```

   En el que `user_defined_mount_point` corresponde a cualquier directorio que decida utilizar para el montaje similar a cualquier comando de montaje.

   En RHEL, el dispositivo de CD (dispositivo virtual **.iso**) es `/dev/scd0` y el dispositivo de disquete (dispositivo virtual **.img**) es `/dev/sdc`.

   En SLES, el dispositivo de CD es `/dev/sr0` y el dispositivo de disco flexible es /dev/sdc. Para asegurarse de utilizar el dispositivo correcto (para SLES o RHEL), al conectarse al dispositivo virtual en Linux, debe ejecutar el siguiente comando inmediatamente:

   ```
   tail /var/log/messages | grep SCSI
   ```

   Esto muestra texto que identifica el dispositivo (por ejemplo, sdc del dispositivo SCSI). Este procedimiento también se aplica a los medios virtuales cuando utiliza distribuciones Linux en el nivel de ejecución init 3. De manera predeterminada, los medios virtuales no se montan automáticamente en init 3.

Configuración de recursos compartidos de archivos remotos mediante RACADM

Para configurar el uso compartido de archivos remotos mediante RACADM, utilice los comandos siguientes:

`racadm remoteimage`

`racadm remoteimage <options>`

Las opciones disponibles son:

`-c` : conectar imagen

`-d` : desconectar imagen

`-u` <nombredeusuario>: nombre de usuario para acceder al recurso compartido de red

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

`-l` <ubicación_de_imagen>: ubicación de la imagen en el recurso compartido de red; debe indicar la ubicación entre comillas dobles. Para ver ejemplos de rutas de acceso de archivos de imagen, consulte 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 recursos compartidos CIFS alojados en sistemas Windows 7, modifique las siguientes claves de registro:

- Configure HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\LargeSystemCache en `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. Configure **Internal USB Port (Puerto USB interno)** en **On (Activado)**. Si se configura en **Off (Desactivado)**, 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 doble interno (IDSDM) solo está disponible en las plataformas correspondientes. IDSDM proporciona redundancia en la tarjeta SD del hipervisor utilizando otra tarjeta SD que duplica el contenido de la primera tarjeta SD.

Cualquiera de las dos tarjetas SD puede ser la principal. Por ejemplo, si se instalan dos tarjetas SD nuevas en el IDSDM, la SD1 es la tarjeta activa (principal) y la SD2 es la tarjeta de respaldo. Los datos se graban en ambas tarjetas, pero se leen de la tarjeta SD1. Si la tarjeta SD1 no funciona o se extrae, la tarjeta SD2 se convierte automáticamente en la tarjeta activa (principal).

Es posible ver el estado, la condición y la disponibilidad del IDSDM mediante la interfaz web de la iDRAC o RACADM. El estado de redundancia de la tarjeta SD y los sucesos de error se registran en el SEL y se muestran en el panel anterior, y las alertas PET se generan si están habilitadas.

28

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

La iDRAC proporciona un conjunto estándar de herramientas de diagnóstico de red similares a las herramientas que se incluyen con sistemas basados en Microsoft Windows o Linux. Mediante la interfaz web de la iDRAC, es posible acceder a las herramientas de depuración de errores de la red.

Para acceder a la consola de diagnósticos:

1. En la interfaz web de la iDRAC, vaya a **Maintenance (Mantenimiento)** > **Diagnostics (Diagnósticos)**.
   Aparecerá la página **Diagnostics Console Command (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 la *Ayuda en línea de la iDRAC*.
   Los resultados se muestran en la misma página.

Restablecer iDRAC y restablecer la configuración predeterminada de iDRAC

1. En la interfaz web de iDRAC, vaya a **Mantenimiento** > **Diagnósticos**.
   Tiene las siguientes opciones:

- Haga clic en **Restablecer el iDRAC** para restablecer el iDRAC. Se ejecutará una operación de reinicio normal en el iDRAC. Después del reinicio, actualice el explorador para volver a iniciar sesión en el iDRAC.
- Haga clic en **Restablecer el iDRAC a la configuración predeterminada** para restablecer el iDRAC a los valores predeterminados. Después de hacer clic en **Restablecer el iDRAC a la configuración predeterminada**, se mostrará la ventana **Restablecer el iDRAC a la configuración predeterminada de fábrica**. Esta acción restablece el iDRAC a la configuración predeterminada de fábrica. Seleccione cualquiera de las opciones siguientes:
  a. Conservar configuración de usuario y red.
  b. Descarte todos los valores de configuración y restablezca los usuarios a los valores de envío (root/valores de envío).
  c. Descartar todos los valores de configuración y restablecer el nombre de usuario y la contraseña.

2. Aparece un mensaje de aviso. Haga clic en **Aceptar** para 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 NFS, CIFS, HTTP o HTTPS con el comando RACADM `diagnostics export`. También puede ejecutar los diagnósticos mediante los comandos correspondientes 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 de manera 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 / HTTP / HTTPs share> -u
<username> -p <password>
```

Para obtener más información acerca de las opciones, consulte *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

Visualización de los códigos de la POST

Los códigos de la POST son indicadores de progreso del BIOS del sistema que indican las distintas etapas de la secuencia de arranque a partir de la operación de encendido al restablecer, y permiten diagnosticar los errores relacionados con el inicio del sistema. En la página **Post Codes (Códigos de POST)**, se puede ver el último código de la POST del sistema antes de iniciar el sistema operativo.

Para ver los códigos de la POST, vaya a **Maintenance (Mantenimiento)** > **Troubleshooting (Solución de problemas)** > **Post Code (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.

Viewing boot and crash capture videos

You can view the video recordings of:

- Last three boot cycles — A boot cycle video logs the sequence of events for a boot cycle. The boot cycle videos are arranged in the order of latest to oldest.
- Last crash video — A crash video logs the sequence of events leading to the failure.

This is a licensed feature.

iDRAC records fifty frames during boot time. Playback of the boot screens occur at a rate of 1 frame per second. If iDRAC is reset, the boot capture video is not available as it is stored in RAM and is deleted.

NOTE:

- You must have Access Virtual Console or administrator privileges to playback the Boot Capture and Crash Capture videos.
- The video capture time displayed in the iDRAC GUI video player may differ from the video capture time displayed in other video players. The iDRAC GUI video player displays the time in the iDRAC time zone while all other video players display the time in the respective operating system time zones.

NOTE:

- The reason for the delay in boot capture file availability is because the boot capture buffer is not full after the host boot.
- Default /inbox SLES/RHEL video players do not support the MPEG-1 video decoder. You need to install a MPEG decoder supported video player and play the files.
- MPEG-1 format videos are not supported in MAC OS native player.

To view the **Boot Capture** screen, click **Maintenance** > **Troubleshooting** > **Video Capture**.

The **Video Capture** screen displays the video recordings. For more information, see the *iDRAC Online Help*.

NOTE: When embedded video controller is disabled and server has add-on video controller, then certain latency is expected with respect to boot capture. Hence, End of Post Messages of a video will be recorded in next capture.

Configuración de los valores de captura de video

Para configurar los valores de captura de video:

1. En la interfaz web de la iDRAC, vaya a **Maintenance (Mantenimiento)** > **Troubleshooting (Solución de problemas)** > **Video Capture (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 eventos del sistema (SEL) y los registros de Lifecycle. Para obtener más información, consulte Visualización del registro de eventos 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 imagen 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 iDRAC o se produce un evento de ciclo de encendido de CA, se borran los datos de captura de bloqueo.

   NOTA: La resolución de la pantalla de último bloqueo siempre es de 1024x768, independientemente de la resolución del sistema operativo del host.

Visualización del estado del sistema

El estado del sistema resume el estado de los siguientes componentes del sistema:

- Resumen
- Baterías
- Enfriamiento
- CPU
- Panel frontal
- Intrusión
- Memoria
- Dispositivos de red
- Sistemas de alimentación
- Voltajes
- Medios flash extraíbles
- Controladora del chasis

Es posible visualizar el estado del sistema administrado:

- Servidores tipo bastidor y torre: estado del LED de ID del sistema y del panel frontal LCD o el estado del LED de ID del sistema de panel frontal LED.
- Servidores Blade: solo los LED de ID del sistema.

Visualización del estado del LCD del panel frontal del sistema

Para ver el estado del panel frontal LCD de los servidores tipo bastidor y torre respectivos, en la interfaz web de la iDRAC, vaya a **Sistema** > **Descripción general** > **Panel frontal**. Aparece la página **Panel frontal**.

En la sección **Panel frontal** se muestran las feed en directo de los mensajes que aparecen actualmente en el panel frontal LCD. Cuando el sistema funciona correctamente (lo que se indica con color azul sólido en el panel frontal LCD), aparecen atenuados **Ocultar error** y **Mostrar error**.

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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.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 la 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 (lo que se indica con un icono de estado de color azul en el panel frontal LED), entonces aparecen atenuados **Ocultar error** y **Mostrar error**. 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 *Guía de la CLI de RACADM para iDRAC* disponible en https://www.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 *Manual de instalación y servicio* disponible en https://www.dell.com/poweredgemanuals 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

Puede ver el estado de los siguientes componentes en las interfaces web de iDRAC, CMC y OME Modular:

- Baterías
- CPU
- Refrigeración
- Intrusión
- Memoria
- Fuentes 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 parpadea con luz ámbar y un servidor concreto tiene un error, la pantalla principal de estado del servidor en el panel LCD resalta en naranja el servidor afectado. Utilice los botones de navegación del panel LCD para resaltar el servidor afectado y haga clic en el botón central. Los mensajes de error y advertencia aparecerán en la segunda línea. Para obtener una lista de los mensajes de error que aparecen en el panel LCD, consulte el manual del propietario

Reinicio de iDRAC

Puede realizar un reinicio por hardware o por software de iDRAC sin apagar el servidor:

- Reinicio por hardware: en el servidor, mantenga presionado el botón LED durante 15 segundos.
- Reinicio por software: utilice la interfaz web de iDRAC o RACADM.

Restablecer a los valores predeterminados personalizados (RTD)

Puede usar la función Restablecer a los valores predeterminados personalizados para cargar un archivo de configuración personalizado y RTD a los ajustes. Los nuevos ajustes se aplican por sobre la conservación de los ajustes de red y usuario.

La función Restablecer a los valores predeterminados personalizados ofrece las siguientes opciones:

- Cargar ajustes de valores predeterminados personalizados:
  - Puede cargar el archivo de ajustes de valores predeterminados personalizados. Este archivo se puede obtener mediante la exportación del perfil de configuración del servidor (SCP) en formato XML (el formato JSON no es compatible con esta función). El cliente puede modificar el contenido del archivo para agregar o eliminar los ajustes.
  - Puede cargar el archivo XML de SCP mediante las interfaces RACADM o la GUI de iDRAC.
  - Las configuraciones cargadas se guardan en la base de datos predeterminada.
- Guardar los ajustes actuales como valores predeterminados personalizados:
  - Esta operación permite guardar los ajustes actuales como ajustes predeterminados.
  - Esto solo es compatible mediante la interfaz de RACADM.
- Descargar ajustes de valores predeterminados personalizados:

- Puede descargar el archivo XML de SCP de todos los valores predeterminados.
- Esto solo es compatible mediante la interfaz de RACADM.

- Iniciar restablecer a los valores predeterminados personalizados:
  - Se aplicarán los ajustes predeterminados cargados/guardados.

Reinicio de iDRAC mediante la interfaz web de iDRAC

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

- Cargar archivo de valores predeterminados personalizados:
  - Vaya a **Configuración** > **Perfil de configuración del servidor** > **Valores predeterminados personalizados** > **Cargar valores predeterminados personalizados**
  - Cargue el archivo *CustomConfigured.xml* personalizado desde la ruta de acceso Recurso compartido local.
  - Haga clic en **Aplicar**. Se creó el nuevo trabajo Cargar valores predeterminados personalizados.
- Restablecer a los valores predeterminados personalizados:
  - Cuando el trabajo Cargar valores predeterminados personalizados se complete correctamente, consulte **Mantenimiento** > **Diagnóstico**, haga clic en la opción **Restablecer iDRAC a los valores predeterminados de fábrica**.
  - Seleccione **Descartar todos los ajustes** y establezca la opción **Configuración predeterminada personalizada**.
  - Haga clic en **Continuar** para iniciar la configuración Restablecer a los valores predeterminados personalizados.

Reinicio de iDRAC mediante RACADM

Para reiniciar la iDRAC, utilice el comando **racreset**. Para obtener más información, consulte *Guía de la CLI de RACADM de la controladora de administración del chasis* disponible en https://www.dell.com/cmcmanuals.Para obtener más información, consulte *Guía de la CLI de RACADM de OME - Modular para el chasis PowerEdge MX7000* disponible en https://www.dell.com/openmanagemanuals

Para aplicar la función Restablecer a las operaciones predeterminadas, utilice los siguientes comandos:

- Cargar archivo de valores predeterminados personalizados: `racadm –r <iDracIP> -u <username> -p <Password> set -f <filename> -t xml --customdefaults`
- Guardar los ajustes actuales como ajustes predeterminados: `racadm –r <iDracIP> -u <username> -p <Password> set --savecustomdefaults`
- Descargar ajustes de valores predeterminados personalizados: `racadm –r <iDracIP> -u <username> -p <Password> get -f <filename> -t xml --customdefaults`
- Restablecer a los valores predeterminados personalizados: `Racadm –r <iDracIP> -u <username> -p <Password> racresetcfg -custom`

Borrado de datos del sistema y del usuario

NOTA: El borrado de datos del sistema y del usuario no se admite en la interfaz gráfica de usuario de la iDRAC.

Puede borrar componentes del sistema y datos del usuario para los siguientes componentes:

- Restablecimiento de los valores predeterminados del BIOS
- Diagnósticos incorporados
- Driver Pack para el sistema operativo incorporado
- Datos de Lifecycle Controller
- Restablecimiento de los valores predeterminados de iDRAC
- Sobrescriba los discos duros no compatibles con el borrado seguro instantáneo (ISE)
- Restablezca la configuración de la controladora
- Restablezca vFLASH
- Borre los discos duros, SSD y NVMe compatibles con ISE
- Borre todas las aplicaciones del sistema operativo

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 la iDRAC se reinicia. Toda la información anterior 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 integrados
- drvpack: paquete de controladores para el sistema operativo integrado
- lcdata: se borran los datos de Lifecycle Controller
- idrac: restablecimiento de los valores predeterminados de la iDRAC
- overwritepd: sobrescribe las unidades de disco duro que no son compatibles con el borrado seguro instantáneo (ISE)
- percnvcache: restablece la memoria caché de la controladora
- vflash: restablece vFLASH
- secureerasepd: borra las unidades de disco duro, SSD y NVMe que admiten ISE
- allapps: borra todas las aplicaciones del sistema operativo

NOTA: Mientras borra vFlash, asegúrese de que todas las particiones de la tarjeta vFlash estén desconectadas antes de ejecutar la operación.

NOTA: Si SEKM está habilitado en el servidor, desactive SEKM mediante el comando `racadm sekm disable` antes de utilizar este comando. Esto puede evitar que se bloqueen los dispositivos de almacenamiento protegidos por iDRAC, en caso de que la configuración de SEKM se borre de iDRAC mediante la ejecución de este comando.

Para obtener más información, consulte *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

NOTA: El vínculo de Dell TechCenter aparece en la interfaz gráfica de usuario de la iDRAC en sistemas con la marca Dell. Si borra los datos del sistema usando el comando WSMan y desea que el vínculo vuelva a aparecer, reinicie el host de forma manual y espere que se ejecute CSIOR.

NOTA: Una vez que se ha ejecutado el borrado del sistema, es posible que sigan mostrándose los discos virtuales. Ejecute CSIOR después de que se haya completado el borrado del sistema y de que se reinicie la 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 **Maintenance (Mantenimiento)** > **Diagnostics (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.

29

Integración de SupportAssist en iDRAC

SupportAssist le permite crear recopilaciones de SupportAssist y utilizar otras de sus funciones para monitorear el sistema y el centro de datos. iDRAC proporciona interfaces de aplicación para obtener información de plataforma que permita a los servicios de asistencia resolver los problemas de plataforma y del sistema. iDRAC le permite generar una recopilación de SupportAssist del servidor y luego exportarla a una ubicación en la estación de administración (local) o a una ubicación de red compartida, como FTP, protocolo trivial de transferencia de archivos (TFTP), HTTP, HTTPS, Common Internet File System (CIFS) o recurso compartido de archivos de red (NFS). La recopilación se genera en el formato .zip estándar. Puede enviar esta recopilación al servicio de asistencia técnica para la solución de problemas o la recopilación de inventario.

Temas:

Registro de SupportAssist

Para aprovechar al máximo las funciones predictivas, proactivas y automatizadas de SupportAssist, debe registrar su sistema en dicho servicio.

Puede generar una recopilación y guardarla de forma local o en una red, también enviarla a Dell EMC sin registro.

NOTA: Algunos clientes OEM no tienen el nombre del modelo. El Support Assist de back-end no permite registrar esos sistemas con DELL.

Información de contacto y envío

Para completar el registro, debe proporcionar la información de contacto y envío.

Información de contacto principal

Ingrese el nombre de la empresa, el país, el nombre*, el apellido*, el número de teléfono*, un número alternativo y la dirección de correo electrónico*. Compruebe si los detalles se muestran correctamente y realice los cambios necesarios si desea editar alguno de los campos.

* Indica que los campos son obligatorios.

Información de contacto secundario

Introduzca el nombre, el apellido, el número de teléfono, el número alternativo y la dirección de correo electrónico. Además, compruebe si los detalles se muestran correctamente y realice los cambios necesarios si desea editar alguno de los campos.

NOTA: Puede quitar la información de contacto secundaria en cualquier momento.

Despacho automático

Cuando se informa de un evento crítico a Dell EMC a través de la iDRAC registrada en SupportAssist, es posible que se inicie el envío automático del flujo de trabajo. Este flujo de trabajo se basa en el evento reenviado y el nivel de garantía de SupportAssist del dispositivo registrado. Debe ingresar la **información de despacho** durante el proceso de registro de SupportAssist para habilitar la función del despacho automático del flujo de trabajo. Si se requiere de soporte en el sitio junto con las piezas despachadas, seleccione **Despacho de piezas con soporte en el sitio**.

NOTA: El despacho automático está habilitado en los sistemas con el módulo de servicio de la iDRAC (iSM) v3.4.0 para Windows. Las versiones futuras del iSM serán compatibles con el despacho automático para sistemas operativos adicionales.

Dirección de envío

Ingrese una dirección y las horas de contacto recomendadas.

Acuerdo de licencia de usuario final

Después de proporcionar toda la información requerida, debe aceptar el acuerdo de licencia de usuario final (EULA) para completar el proceso de registro. Tiene la opción para imprimir el EULA para referencia futura. Puede cancelar y terminar el proceso de registro en cualquier momento.

Instalación del módulo de servicios

Para registrarse y utilizar SupportAssist, debe tener instalado iDRAC Service Module (iSM) en el sistema. Una vez que ejecute **initiate Service Module Installation** (**Iniciar instalación de Service Module)**, podrá ver las instrucciones de instalación. El botón **Next (Siguiente)** se mantiene deshabilitado hasta que iSM se instala correctamente.

Información de proxy del sistema operativo del servidor

En caso de que haya un problema con la conexión, se le pedirá al usuario que brinde la información de proxy del sistema operativo. Para configurar los ajustes del proxy, introduzca la información necesaria en **Server (Servidor), Port (Puerto), Username (Nombre de usuario)** y **Password (Contraseña)**.

SupportAssist

Una vez que se configure SupportAssist, podrá revisar su tablero para ver el **resumen de solicitud de servicio**, el **estado de la garantía**, la **descripción general de SupportAssist**, las **solicitudes de servicio** y el **registro de recopilación**. No es necesario estar registrado para ver o enviar el registro de recopilación.

Portal de solicitudes de servicio

En **Solicitud de servicio**, se muestran los detalles de **Estado** (abierto/cerrado), **Descripción, Origen** (evento/teléfono), **Identificador de solicitud de servicio**, **Fecha de apertura** y **Fecha de cierre** de cada evento. Puede seleccionar cada evento para ver más detalles. Tiene la opción de seleccionar Service Request Portal (Portal de solicitudes de servicio) para ver información adicional de cualquier caso específico.

Registro de recopilación

En el **Registro de recopilaciones**, se muestran los detalles de **Hora y fecha, y tipo de recopilación** (manual, programado, basado en eventos), **Datos recopilados** (selección personalizada, todos los datos), **Estado de recopilación** (completa con errores, completa), **Identificador de trabajo**, **Estado de envío** y **Fecha y hora de envío**. Puede enviar a Dell la última recopilación que persiste en la iDRAC.

NOTA: Una vez generado, se pueden filtrar los detalles de registro de recopilación para quitar la información de identificación personal (PII) según la selección del usuario.

Generating SupportAssist Collection

For generating the OS and Application logs:

- iDRAC Service Module must be installed and running in Host Operating System.
- OS Collector, which comes factory installed in iDRAC, if removed must be installed in iDRAC.

NOTE: SupportAssist Collection takes more than 10 minutes to complete when performed from OS/iDRAC while OMSA 10.1.0.0 is running with it.

If you have to work with Tech Support on an issue with a server but the security policies restrict direct internet connection, then you can provide Tech Support with necessary data to facilitate troubleshooting of the problem without having to install software or download tools from Dell and without having access to the Internet from the server operating system or iDRAC.

You can generate a health report of the server and then export the Collection log:

- To a location on the management station (local).
- To a shared network location such as Common Internet File System (CIFS) or Network File Share (NFS). To export to a network share such as CIFS or NFS, direct network connectivity to the iDRAC shared or dedicated network port is required.
- To Dell EMC.

The SupportAssist Collection is generated in the standard ZIP format. The collection may contain the following information:

- Hardware inventory for all components (includes system component configuration and firmware details, Motherboard System Event Logs, iDRAC state information and Lifecycle Controller logs).
- Operating system and application information.
- Storage Controller logs.
- iDRAC Debug Logs.
- It contains an HTML5 viewer, that can be accessed once the collection is complete.
- The collection provides a massive amount of detailed system information and logs in a user friendly format that can be viewed without uploading the collection to the Tech Support site.

After the data is generated, you can view the data which contains multiple XML files and log files.

Each time the data collection is performed, an event is recorded in the Lifecycle Controller log. The event includes information such as the user who initiated the report, interface used, and the date and time of export.

On Windows, If WMI is disabled, OS Collector collection stops with an error message.

Check the appropriate privilege levels and make sure there is no firewall or security settings that may prevent from collecting the registry or software data.

Before generating the health report, make sure:

- Lifecycle Controller is enabled.
- Collect System Inventory On Reboot (CSIOR) is enabled.
- You have Login and Server Control privileges.

Generación de SupportAssist Collection en forma manual mediante la interfaz web del iDRAC

Para generar la recopilación de SupportAssist manualmente:

1. En la interfaz web de iDRAC, vaya a **Maintenance (Mantenimiento)** > **SupportAssist**.
2. Si el servidor no está registrado para SupportAssist, se mostrará el asistente de registro de SupportAssist. Haga clic en **Cancelar** > **Cancelar registro**.

3. Haga clic en **Start a Collection (Iniciar recopilación)**.
4. Seleccione los conjuntos de datos que se incluirán en la recopilación.
5. Puede optar por filtrar la recopilación para PII.
6. Seleccione el destino donde se debe guardar la recopilación.
   a. Si el servidor está conectado a Internet y la opción **Enviar ahora** está activada, se transmite el registro de recopilación a Dell EMC SupportAssist mediante la selección de esta opción.
   b. La opción **Save locally (Guardar localmente)** le permite guardar la recopilación generada en el sistema local.
   c. La opción **Save to Network (Guarda en la red)** guarda la recopilación generada en una ubicación compartida de NFS o CIFS definida por el usuario.

      NOTA: Si se selecciona la opción *Save to Network (Guarda en la red)* y no hay ninguna ubicación predeterminada disponible, los detalles de la red proporcionados se guardarán como ubicación predeterminada para recopilaciones futuras. Si ya existe una ubicación predeterminada, la recopilación utilizará los detalles especificados solo una vez.

   Si la opción **Save to Network (Guarda en la red)** está seleccionada, los detalles de la red proporcionados por el usuario se guardarán como los valores predeterminados (si antes no se ha guardado ninguna ubicación de recurso compartido de red) para cualquier recopilación futura.
7. Haga clic en **Collect (Recopilar)** para continuar con la generación de la recopilación.
8. Si se le solicita, acepte el acuerdo **End User Level Agreement (EULA) (Acuerdo de licencia de usuario final [EULA])** para continuar.

   La opción de datos de las aplicaciones y del sistema operativo aparecerá desactivada 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 se ha extraído de la iDRAC, o
   - El conector de OS-BMC está deshabilitado en la iDRAC, o
   - Los datos de las aplicaciones del sistema operativo almacenado en la memoria caché no están disponibles en la iDRAC de una recopilación anterior.

Configuración

Mediante esta página, podrá ajustar la configuración del registro de recopilación y, en caso de que esté registrado, podrá actualizar los detalles de contacto, activar o desactivar las notificaciones por correo electrónico y cambiar la configuración de idioma.

Configuración de recopilación

Puede guardar las recopilaciones en una ubicación de red preferida. Utilice la opción **Set Archive Directory (Establecer directorio de archivo)** para establecer la ubicación de red. Puede guardar las recopilaciones en una ubicación de red preferida. Utilice la opción Set Archive Directory (Establecer directorio de archivo) para establecer la ubicación de red. Introduzca el tipo de protocolo (CIFS/NFS) que desee elegir, las direcciones IP correspondientes, el nombre de recurso compartido, el nombre de dominio, el nombre de usuario y la contraseña antes de probar la conexión de red. El botón Test Network Connection (Probar conexión de red) confirmará si hay una conexión al recurso compartido de destino.

Si está registrada, puede optar por incluir la información de identificación durante el envío de los datos a Dell en la configuración de la recopilación.

Es posible habilitar y programar las opciones de **Automatic Collection (Recopilación automática)** para evitar la intervención manual y mantener una comprobación periódica del sistema De manera predeterminada, cuando se desencadena un evento y se abre un caso de asistencia, SupportAssist está configurado para recopilar automáticamente los registros del sistema desde el dispositivo que generó la alerta y cargarlos a Dell. Es posible habilitar o deshabilitar la recopilación automática basada en eventos Es posible programar las recopilaciones automáticas en función de los requisitos que desee. Las opciones disponibles son: semanalmente, mensualmente, trimestralmente o nunca. También es posible configurar la fecha y hora de los eventos periódicos programados. Tiene la opción de habilitar o deshabilitar la opción **ProSupport Plus Recommendation Report (Informe de recomendación de ProSupport Plus)** mientras configura las recopilaciones.

Información de contacto

En esta página, figuran los detalles de la información de contacto que se agregaron durante el proceso de registro de SupportAssist, y es posible actualizarlos.

30

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 navegador. 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.

Configuración personalizada de correo electrónico del remitente para alertas de iDRAC

El correo electrónico generado de alerta no se encuentra en el conjunto de correo electrónico personalizado del remitente en el servicio de correo electrónico basado en la nube.

Debe registrar su correo electrónico en la nube a través de este proceso: Support.Google.com.

Seguridad de la red

Si accede a la interfaz web de la iDRAC, se muestra una advertencia de seguridad en la que se indica que el certificado SSL emitido por la autoridad de certificados (CA) no es de confianza.

iDRAC incluye un certificado de servidor predeterminado para iDRAC a fin de garantizar la seguridad de red cuando se accede a ella a través de la interfaz basada en Web y el RACADM remoto. Este certificado no lo emite una CA de confianza. Para resolver esto, cargue un certificado de servidor para 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.

Si accede a la interfaz basada en Web de la iDRAC, se muestra una advertencia de seguridad en la que se indica que el nombre de host del certificado SSL no coincide con el nombre de host de la iDRAC.

iDRAC incluye un certificado de servidor predeterminado para iDRAC a fin de garantizar la seguridad de red cuando se accede a ella a través de la interfaz basada en Web y el RACADM remoto. Cuando se utiliza este certificado, el explorador web muestra una advertencia de seguridad debido a que el certificado predeterminado que se emite a la iDRAC no coincide con su nombre de host (por ejemplo, la dirección IP).

Para solucionar esto, cargue un certificado de servidor para iDRAC emitido para la dirección IP o el nombre de host de la iDRAC. Cuando se genere la CSR (que se utiliza para emitir el certificado), asegúrese de que el nombre común (CN) de la CSR coincida con la dirección IP de la iDRAC (si el certificado se emitió a la IP) o con el nombre DNS registrado de la iDRAC (si el certificado se emitió al nombre registrado de la iDRAC).

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

1. En la interfaz web de la 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**.

¿Por qué no puedo acceder a la iDRAC desde mi explorador web?

Este problema puede producirse si la seguridad estricta de transporte de HTTP (HSTS) está activado. HSTS es un mecanismo de seguridad web que permite a los exploradores web interactuar solamente mediante el protocolo seguro HTTPS y no con HTTP.

Para resolver el problema, active HTTPS en su explorador e iniciar sesión en la iDRAC.

¿Por qué no puedo completar las operaciones que implican un recurso compartido CIFS remoto?

La operación de importar/exportar o cualquier otra operación de recurso compartido de archivos remotos que implique un recurso compartido CIFS fallará si solo utiliza SMBv1. Asegúrese de que el protocolo SMBv2 esté activado en el servidor que proporciona SMB o el recurso compartido CIFS. Consulte la documentación del sistema operativo sobre cómo habilitar el protocolo SMBv2.

Transmisión de telemetría

Faltan algunos datos del informe durante la transmisión de los informes de telemetría para los servidores de Rsyslog.

Es posible que las versiones anteriores de los servidores rsyslog no pierdan ocasionalmente algunos datos del informe en algunos informes. Puede actualizar a una versión más reciente para evitar este problema.

Active Directory

Ocurrió un error de inicio de sesión en Active Directory. ¿Cómo se resuelve este problema?

Para diagnosticar el problema, en la página **Active Directory Configuration and Management (Configuración y administración de Active Directory)**, haga clic en **Test Settings (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 la iDRAC mediante las credenciales locales. Después de iniciar sesión, compruebe lo siguiente:
  - La opción **Active Directory activado** está seleccionada en la página **Configuración y administración de Active Directory**.
  - La configuración de DNS se ha configurado correctamente en la página **Configuración de redes iDRAC**.
  - Se ha cargado el certificado de CA raíz de Active Directory correcto en iDRAC si se ha activado la validación de certificados.
  - El nombre de iDRAC y el nombre de dominio de iDRAC coinciden con la configuración del entorno de Active Directory si utiliza el esquema extendido.
  - El nombre de grupo y el nombre de dominio de grupo coinciden con la configuración del entorno de Active Directory si utiliza el esquema estándar.
  - Si el usuario y el objeto de la iDRAC se encuentran en un dominio diferente, no seleccione la opción **User Domain from Login (Dominio de usuario desde inicio de sesión)**. En cambio, seleccione la opción **Specify a Domain (Especificar un dominio)** e introduzca el nombre del dominio en el que reside el objeto de la 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.

Ocurre un error de inicio de sesión en Active Directory incluso si la validación de certificados está habilitada. 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 habilitado la validación de certificados, cuando la iDRAC establece la conexión SSL con el servidor de directorios, la iDRAC utiliza el certificado de CA cargado para verificar el certificado de servidor de directorios. Los motivos más comunes de error en esta validación son los siguientes:

- La fecha de la iDRAC no se encuentra dentro del período de validez del certificado del servidor o de CA. Compruebe la hora de la iDRAC y el período de validez del certificado.
- Las direcciones de la controladora de dominio configuradas en la 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, **nombredeservidor.ejemplo.com** en lugar de **ejemplo.com**.

Ocurre un error durante la validación de certificados incluso si la dirección IP se utiliza como dirección de la controladora de dominio. ¿Cómo se resuelve este problema?

Compruebe el campo Subject (Asunto) o Subject Alternative Name (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 de asunto o de nombre alternativo del asunto del certificado de la controladora de dominio. Para solucionar esto, realice cualquiera de las siguientes acciones:

- 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, son necesarias las direcciones de catálogo global. En este caso, solo puede utilizar el grupo universal.

Si está utilizando un esquema estándar y todos los usuarios y grupos de roles se encuentran en el mismo dominio, no son necesarias las direcciones de catálogo global.

Si utiliza un esquema extendido, no se utiliza la dirección de catálogo global.

¿Cómo funciona la consulta del esquema estándar?

La iDRAC se conecta primero a las direcciones de la controladora de dominio configuradas. Si el usuario y los grupos de roles están en el dominio, se guardarán los privilegios.

Si están configuradas las direcciones de la controladora global, la iDRAC seguirá consultando el catálogo global. Si se recuperan privilegios adicionales desde el catálogo global, estos privilegios se acumulan.

¿iDRAC siempre usa LDAP a través de SSL?

Sí. Todo el transporte se realiza a través del puerto seguro 636 o 3269. Durante la configuración de la prueba, la iDRAC realiza una conexión LDAP solamente 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?

La iDRAC aplica un nivel sólido de seguridad para garantizar la identidad de la controladora de dominio a la que se conecta. Sin la validación de certificados, un pirata informático puede suplantar una controladora de dominio y tomar el control de la conexión SSL. Si opta por confiar en todas las controladoras de dominio en el límite de seguridad sin activar la validación de certificados, puede deshabilitar esta opción en 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 de DNS cuando un servidor DNS está fuera de servicio. La iDRAC inicia la sesión mediante el servidor DNS alternativo.

Active Directory está configurado para un dominio presente en Windows Server 2008 Active Directory. Hay un dominio secundario o un subdominio presentes 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 la iDRAC mediante el usuario presente en el dominio secundario, ocurre un error durante el inicio de sesión único de Active Directory.

Esto puede deberse a un tipo de grupo incorrecto. Hay dos tipos de grupos en el servidor de Active Directory:

- Seguridad: los grupos de seguridad permiten administrar el acceso de usuarios y equipos a los recursos compartidos y filtrar la configuración de la política de grupo.
- Distribución: los grupos de distribución tienen la finalidad de utilizarse solo como listas de distribución por correo electrónico.

Asegúrese siempre de que el tipo de grupo sea Security (Seguridad). No es posible utilizar grupos de distribución para asignar permisos para objetos. Sin embargo, puede usarlos para filtrar la configuración de la política de grupo.

Inicio de sesión único

Ocurre un error durante el inicio de sesión único (SSO) en Windows Server 2008 R2 x64. ¿Cuál es la configuración necesaria para resolver este problema?

1. Realice el procedimiento que se indica en **http://technet.microsoft.com/es-es/library/dd560670(WS.10).aspx** 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 las computadoras cliente o los servicios y las aplicaciones del entorno. Los tipos de cifrado de configuración permitidos para el ajuste de la política de Kerberos se encuentran en **Computer Configuration (Configuración de la computadora)** > **Security Settings (Configuración de seguridad)** > **Local Policies (Políticas locales)** > **Security Options (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 la antigua ficha keytab usando 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 habilitar los tipos de cifrado para Windows 7 y Windows Server 2008 R2. Para hacerlo:

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 directivas de grupo local**, vaya a **Configuración del equipo local** > **Configuración de Windows** > **Configuración de seguridad** > **Directivas locales** > **Opciones de seguridad** .
2. Haga clic con el botón derecho del mouse en **Seguridad de la red: Restricción de NTLM: Tráfico de NTLM de salida al servidor remoto** y seleccione **Propiedades**.
3. Seleccione **Permitir todo**, haga clic en **Aceptar** y, a continuación, cierre la ventana **Editor de directivas de grupo local**.
4. Vaya a **Inicio** y ejecute el comando cmd. Aparecerá la ventana Símbolo del sistema.
5. Ejecute el comando `gpupdate /force`. Se actualizarán las políticas de grupo. Cierre la ventana 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** > **System** > **CurrentControlSet** > **Control** > **LSA**.
8. En el panel derecho, haga clic con el botón derecho del mouse y seleccione **Nuevo** > **DWORD (32-bit) Value**.
9. Asigne a la nueva clave el nombre **SuppressExtendedProtection**.
10. Haga clic con el botón derecho del mouse en **SuppressExtendedProtection** y haga clic en **Modificar**.
11. En el campo de datos **Valor**, escriba **1** y haga clic en **Aceptar**.
12. Cierre la ventana **Editor del Registro**. Ahora puede iniciar sesión en el iDRAC mediante el inicio de sesión único.

Si ha habilitado el SSO para la iDRAC y está utilizando Internet Explorer para iniciar sesión en la iDRAC, ocurrirá un error durante el SSO y se le pedirá que introduzca el nombre de usuario y la contraseña. ¿Cómo se resuelve este problema?

Asegúrese de que la dirección IP de la iDRAC figure en **Herramientas** > **Opciones de Internet** > **Seguridad** > **Sitios de confianza**. Si no figura, ocurrirá un error durante el SSO y se le pedirá 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 mediante tarjeta inteligente de Active Directory 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 **Network (Red)** y el primero ha fallado. Se espera que se produzcan tiempos de espera de DNS cuando un servidor DNS está fuera de servicio. La iDRAC 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 Microsoft Windows. Windows admite una cantidad limitada de proveedores de servicios criptográficos (CPS) de tarjeta inteligente.

En general si los CSP de tarjetas inteligentes están presentes en un cliente particular, inserte la tarjeta inteligente en el lector en la pantalla de inicio de sesión (Ctrl-Alt-Supr) de Windows y compruebe si Windows detecta esa tarjeta y muestra el cuadro de diálogo para introducir el PIN.

PIN incorrecto de la tarjeta inteligente.

Verifique si la tarjeta está bloqueada debido a demasiados intentos de inicio de sesión con un PIN incorrecto. Si es así, póngase 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?

Se requiere Java 8 o posterior para usar esta función y para iniciar la consola virtual de iDRAC a través de una red IPv6.

La sesión de la consola virtual permanece activa aunque se haya cerrado la sesión de la interfaz web de la iDRAC. ¿Este comportamiento es el previsto?

Sí. Cierre la ventana del visor de la consola virtual para cerrar la sesión correspondiente.

¿Se puede iniciar una nueva sesión de video de consola remota cuando el video local del servidor está apagado?

Sí.

¿Por qué tarda 15 segundos apagar el video 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 siguiente comando:

```
racadm get idrac.virtualconsole.attachstate
```

O bien, utilice el comando siguiente desde una sesión de 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 habilitada, se muestra un estado de color verde junto al nombre del servidor. Cuando se deshabilita, un punto amarillo indica que la iDRAC ha bloqueado la consola local.

¿Por qué la parte inferior de la pantalla del sistema no se puede ver desde la ventana de la consola virtual?

Compruebe que la resolución del monitor de la estación de administración sea de 1280 x 1024.

¿Por qué la ventana Visor de la consola virtual está corrupta en el sistema operativo Linux?

El visor de la consola en Linux requiere un conjunto de caracteres UTF-8. Compruebe la configuración regional y restablezca el conjunto de caracteres si es necesario.

¿Por qué el mouse no se sincroniza bajo la consola de texto de Linux en Lifecycle Controller?

La consola virtual requiere el controlador del ratón USB, pero este solo está disponible para el sistema operativo X-Window. En el visor de la consola virtual, realice cualquiera de las siguientes acciones:

- Vaya a la pestaña **Herramientas** > **Opciones de sesión** > **Mouse**. En **Mouse Acceleration (Aceleración del ratón)**, seleccione **Linux**.
- En el menú **Herramientas**, seleccione la opción **Cursor único**.

¿Cómo se sincronizan los punteros del mouse en la ventana Visor de la consola virtual?

Antes de iniciar una sesión de consola virtual, asegúrese de seleccionar el mouse correcto para el sistema operativo.

Asegúrese de seleccionar la opción **Single Cursor (Cursor único)** en **Tools (Herramientas)** en el menú de la consola virtual de la iDRAC del cliente de la consola virtual de la 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 compatible en un sistema con la consola virtual habilitada en el BIOS, se envía un mensaje de conexión EMS que le pide que seleccione **OK (Aceptar)** de manera remota. Debe seleccionar **OK (Aceptar)** en el sistema local o reiniciar el servidor administrado de manera remota, volver a realizar la instalación y, luego, apagar la consola virtual en el BIOS.

Este mensaje lo genera Microsoft para alertar al usuario que la consola virtual está habilitada. Para asegurarse de que este mensaje no aparezca, apague siempre la consola virtual en la utilidad de configuración de la 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 la iDRAC, el indicador Bloq Num de la estación de administración no coincide necesariamente con el estado de Bloq Num del servidor remoto. El estado de Bloq Num depende de la configuración del servidor remoto cuando se conecta la sesión remota, independientemente del estado de Bloq Num de la estación de administración.

¿Por qué aparecen varias ventanas de Session Viewer cuándo se establece una sesión de consola virtual desde el host local?

Está configurando una 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 lo controlarán.

¿Cuánto ancho de banda se necesita para ejecutar una sesión de consola virtual?

Se recomienda disponer de una conexión de 5 Mb/s para un rendimiento adecuado. Se requiere una conexión de 1 Mb/s para un rendimiento mínimo.

¿Cuáles son los requisitos mínimos del sistema para que la estación de administración ejecute la consola virtual?

La estación de administración requiere un procesador Intel Pentium III a 500 MHz con un mínimo de 256 MB de RAM.

¿Por qué la ventana del visor de consola virtual a veces muestra el mensaje Sin señal?

Este mensaje puede aparecer porque el complemento de consola virtual de la iDRAC no recibe el video de escritorio del servidor remoto. Por lo general, este comportamiento se produce cuando el servidor remoto está apagado. De vez en cuando, el mensaje puede aparecer debido a un funcionamiento defectuoso de la recepción de video en el escritorio del servidor remoto.

¿Por qué la ventana del visor de consola virtual a veces muestra un mensaje Fuera de alcance?

Este mensaje puede aparecer debido a que un parámetro necesario para capturar el video está fuera del alcance de captura de video de la iDRAC. Determinados parámetros, como una resolución de pantalla o una frecuencia de actualización muy altas, pueden causar esta situación. Normalmente, las limitaciones físicas, 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 la iDRAC no se encuentre en una lista de sitios de confianza. Para evitar que aparezca la ventana emergente de seguridad cada vez que inicie una sesión de consola virtual, agregue la iDRAC a la lista de sitios de confianza en el navegador del cliente. Para ello, realice lo siguiente:

1. Haga clic en **Herramientas** > **Opciones de Internet** > **Seguridad** > **Sitios de confianza**.
2. Haga clic en **Sitios** e introduzca la dirección IP o el nombre DNS de iDRAC.
3. Haga clic en **Agregar**.
4. Haga clic en **Nivel personalizado**.
5. En la ventana **Configuración de seguridad**, seleccione **Petición** en **Descargar controles ActiveX no firmados**.

¿Por qué la ventana del visor de consola virtual está en blanco?

Si dispone de privilegios de medios virtuales, pero no para la consola virtual, puede iniciar el visor para acceder a la función de medios virtuales; no obstante, la consola del servidor administrado no se mostrará.

¿Por qué el mouse no se sincroniza en DOS cuando se ejecuta la consola virtual?

El BIOS de Dell emula el driver del ratón como un ratón PS/2. Debido al diseño, el ratón PS/2 utiliza la posición relativa para el puntero, lo que ocasiona un retraso en la sincronización. La iDRAC tiene un driver de ratón USB, lo que permite la posición absoluta y un seguimiento más cercano del puntero. Incluso si la iDRAC le transmite la posición absoluta del ratón USB al BIOS de Dell, la emulación del BIOS lo vuelve a convertir en la posición relativa y el comportamiento permanece igual. Para solucionar este problema, establezca el modo de ratón en USC/Diags (USC/Diagnóstico) en la pantalla Configuration (Configuración).

Después de iniciar la consola virtual, el cursor del ratón 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 **Mouse Mode (Modo de ratón)** se configura en **USC/Diags (USC/Diagnóstico)**. Presione las teclas de acceso rápido **Alt + M** para utilizar el ratón en el sistema local. Presione las teclas de acceso rápido **Alt + M** nuevamente para utilizar el ratón en la consola virtual.

¿Por qué se agota el tiempo de espera de la sesión de GUI después de iniciar una consola virtual desde la interfaz de iDRAC que se inicia desde la CMC?

Al iniciar la consola virtual en la iDRAC desde la interfaz web de CMC, se abre una ventana emergente para iniciar la consola virtual. Esta ventana se cierra poco después de abrirse la consola virtual.

Al iniciar la GUI y la consola virtual en el mismo sistema iDRAC en una estación de administración, se agota el tiempo de espera de la GUI de la iDRAC si dicha GUI se inicia antes de que se cierre la ventana emergente. Si la GUI de la iDRAC se inicia desde la interfaz web de CMC después de que se cierre la ventana emergente de la consola virtual, este problema no sucede.

NOTA: No es válido para las plataformas MX.

¿Por qué la clave Linux SysRq no funciona con Internet Explorer?

El comportamiento de la clave Linux Pet Sis es diferente cuando se utiliza la consola virtual desde Internet Explorer. Para enviar la clave Pet Sis, presione la tecla **Imprimir pantalla** y suéltela mientras mantiene apretadas las teclas **Ctrl** y **Alt**. Para enviar la clave Pet Sis a un servidor Linux remoto a través de la iDRAC si usa Internet Explorer, haga lo siguiente:

1. Active la función de tecla mágica en el servidor Linux remoto. Puede utilizar el siguiente comando 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, la iDRAC se desconecta mientras el BIOS restablece la tarjeta de red. El tiempo es más prolongado en las tarjetas de 10 Gb y puede ser excepcionalmente prolongado si el switch de red conectado tiene habilitado el protocolo de árbol de expansión (STP). En este caso, es recomendable activar "portfast" para el puerto del switch conectado al servidor. En la mayoría de los casos, la consola virtual se restablece sola.

El inicio de la consola virtual con el complemento de Java no funciona después de la actualización de firmware de iDRAC.

Elimine la memoria caché de Java y, a continuación, inicie la consola virtual.

Para activar la redirección de consola mediante el puerto del servidor web (443)

```
racadm>>set iDRAC.VirtualConsole.WebRedirect Enabled
```

Para cerrar el puerto de la consola virtual externa (5900), configure la siguiente propiedad de iDRAC.

Para cerrar el puerto de la consola virtual externa (5900), ambos `iDRAC.VirtualConsole.WebRedirect` e `iDRAC.VirtualConsole.CloseUnusedPort` deben estar habilitados.

```
racadm>>set iDRAC.VirtualConsole.CloseUnusedPort Enabled
```

NOTA:

- Si el puerto de medios virtuales está deshabilitado, no se podrá acceder a los medios virtuales independientes y podrá utilizar los medios virtuales a través de la consola virtual.
- Aunque CloseUnusedPort está activado, la consola virtual y los medios virtuales basados en ActiveX y Java no funcionarán, ya que requieren un puerto externo dedicado. La consola virtual y los medios virtuales que usan el complemento HTML5 funcionarán en el puerto del servidor web (443) de iDRAC.

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 cuente con una función de inicio automático. En este caso, el firmware puede agotar el tiempo de espera y la conexión se pierde si el sistema cliente tarda demasiado en leer el CD. Si se pierde la conexión, vuelva a conectarse desde la GUI y continúe 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 de Herramientas de administración de sistemas y documentación de Dell* y la conexión de red es lenta, es posible que el procedimiento de instalación prolongue la cantidad de tiempo que llevará acceder a la interfaz web de iDRAC debido a la latencia de red. La ventana de instalación no indica el progreso de la instalación.

¿Cómo se configura el dispositivo virtual como dispositivo de inicio?

En el sistema administrado, acceda a la configuración del BIOS y diríjase al menú de arranque. Ubique el CD virtual, el disco flexible virtual o el vFlash y cambie el orden de arranque del dispositivo según sea necesario. Además, presione la “barra espaciadora” en la secuencia de arranque de la configuración de CMOS para que el dispositivo virtual se pueda iniciar. Por ejemplo, a fin de realizar el arranque desde una unidad de CD, configure la unidad de CD como el primer dispositivo en el orden de arranque.

¿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?

Además, puede arrancar con un disco de inicio Windows 98 y copiar los archivos del sistema desde el disco de inicio a la llave USB. Por ejemplo, en el aviso de DOS, 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 están conectados al disco flexible remoto. Sin embargo, no se puede ubicar el dispositivo virtual del disco flexible o el CD virtual que ejecuta sistemas operativos 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 con el mismo método. Para montar la unidad de disco flexible virtual, ubique el nodo del dispositivo que Linux asigna a la unidad de disco flexible. A fin de montar la unidad de disco flexible virtual, 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
```

   `/dev/sdx` es el nombre del dispositivo que se encuentra en el paso 4 y `/mnt/floppy` es el punto de montaje.

Para montar la unidad de CD virtual, ubique el nodo del dispositivo que Linux asigna a la unidad de CD virtual. A fin de montar la unidad de CD virtual, 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
```

   `/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 provocan que el iDRAC se restablezca, se pierda la conexión remota y se desmonten las unidades virtuales. Las unidades vuelven a aparecer cuando se completa el restablecimiento del iDRAC.

¿Por qué todos los dispositivos USB se desconectan después de conectar un dispositivo USB?

Los dispositivos de medios virtuales y vFlash están conectados como un dispositivo USB compuesto al bus USB del host y comparten un puerto USB común. Siempre que algún medio virtual o un dispositivo USB vFlash está conectado al bus USB del host o desconectado de él, todos los medios virtuales y dispositivos vFlash se desconectan momentáneamente del bus USB del host y, a continuación, 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 que conecte 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 está utilizando algún sistema operativo del servidor Windows, detenga el servicio de Windows denominado Windows Event Collector. Para ello, diríjase a **Iniciar** > **Herramientas administrativas** > **Servicios**. Haga clic con el botón secundario en **Windows Event Collector** y haga clic en **Detener**.

Mientras visualiza el contenido de una unidad de disco flexible o USB, ¿aparece un mensaje de error de conexión si se conecta la misma unidad a través de los medios virtuales?

No se permite el acceso simultáneo a las unidades de disco flexible virtual. 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 de recurso compartido de archivos remotos (RFS) también se encuentra en uso. A la vez, puede utilizar RFS o medios virtuales, pero no ambos.

No se puede acceder a los medios virtuales, aunque iDRAC muestre el *Estado de conexión* como *Conectado*.

Si intenta acceder a los medios virtuales mediante un plug-in ActiveX o Java mientras el **Modo conectar** está establecido en **Desconectar** en iDRAC, el estado de conexión se puede mostrar como **Conectado**. Cambie el **Modo conectar** a **Conectar automáticamente** o a **Conectar** para acceder a los medios virtuales.

Tarjeta vFlash SD

¿Cuándo se bloquea la tarjeta vFlash SD?

La tarjeta SD vFlash 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 de la detección, IT Assistant intenta verificar los nombres de comunidad get y set del dispositivo. En IT Assistant, usted tiene el nombre de comunidad get = public y el nombre de comunidad set = private. De manera predeterminada, el nombre de comunidad del agente SNMP para el agente iDRAC es public. Cuando IT Assistant envía una solicitud set, el agente iDRAC genera un error de autenticación SNMP porque acepta solicitudes solamente de nombre de comunidad = public.

Para evitar la generación de errores de autenticación SNMP, debe introducir nombres de comunidad aceptados por el agente. Dado que la iDRAC solo permite un nombre de comunidad, deberá utilizar el mismo nombre de comunidad get y set para la configuración de detección de IT Assistant.

Dispositivos de almacenamiento

OpenManage Storage Management muestra más dispositivos de almacenamiento que la iDRAC y no muestra la información de todos los dispositivos de almacenamiento conectados al sistema. ¿Por qué?

iDRAC muestra información solamente para los dispositivos capacidad CEM (administración incorporada completa).

En el caso de los JBOD externos/información detrás del HBA, el mensaje de EEMI para la eliminación del conector SAS/IOM se genera con el ID del mensaje de EEMI ENC42; sin embargo, no se genera el mensaje de EEMI ENC41 para la restauración del conector SAS/IOM.

Para confirmar la restauración de IOM en la interfaz web de iDRAC, realice lo siguiente:

1. Vaya a **Almacenamiento** > **Descripción general** > **Gabinetes**
2. Seleccione el gabinete.
3. En las **Propiedades avanzadas**, asegúrese de que el valor de la **ruta redundante** sea **Presente** y, a continuación, se confirma la restauración de IOM.

GPU (aceleradores)

Aparece atenuada la sección de aceleradores en CPU y Aceleradores en la GUI de iDRAC.

Es posible que algunas páginas de GUI no muestren la respuesta esperada cuando el atributo correspondiente está deshabilitado en Redfish.

Módulo de servicios de iDRAC

Faltan los detalles de iSM o no se actualizaron correctamente en la página GUI de iDRAC de algunos servidores PowerEdge

Cuando un usuario agrega SUB NIC en la agrupación, la configuración no es válida. Esto hace que iSM no se comunique correctamente con 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 iDRAC Service Module, asegúrese de que haya detenido las funciones de Server Administrator que proporciona iDRAC Service Module.

¿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 iDRAC Service Module está instalado, el estado que se muestre será **instalado**.

- En sistemas que ejecutan ESXi: ejecute el comando en `esxcli software vib list|grep -i open` en el host. Aparece el módulo de servicio de la iDRAC.

NOTA: Para verificar si iDRAC Service Module 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/Programas y características**. La versión de iDRAC Service Module instalada aparecerá en una lista en la ficha **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 iDRAC Service Module versión 2.0 y anteriores, cuando se instala iDRAC Service Module, aparece un mensaje de error que indica que este servidor no es compatible. Ya consulté la Guía del usuario para obtener información adicional sobre los servidores admitidos. ¿Cómo se resuelve este error?

Antes de instalar iDRAC Service Module, asegúrese de que el servidor sea un servidor PowerEdge de 12.ª generación o posterior. Asimismo, asegúrese de que dispone de un sistema de 64 bits.

Aparecerá el siguiente mensaje en el registro del sistema operativo, incluso cuando el paso de sistema operativo a la iDRAC mediante la función NIC de USB se haya configurado correctamente. ¿Por qué?

The iDRAC Service Module is unable to communicate with iDRAC using the OS to iDRAC Pass-through channel

iDRAC Service Module utiliza la función de paso de sistema operativo a la iDRAC por medio de la función NIC de USB para establecer la comunicación con la iDRAC. A veces, la comunicación no se establece a pesar de que la interfaz de la NIC de USB está configurada con los extremos IP correctos. Esto puede ocurrir cuando la tabla de encaminamiento del sistema operativo host contiene varias entradas para la misma máscara de destino y el destino de la NIC de USB no aparece primero en la lista de orden de enrutamiento.

Tabla 64. Ejemplo de una 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	1024	0	0 em1
10.94.148.0	0.0.0.0	255.255.255.0	U	0	0	0 em1
vínculo local	0.0.0.0	255.255.255.0	U	0	0	0 em1
vínculo local	0.0.0.0	255.255.255.0	U	0	0	0 enp0s20u12u3

En el ejemplo, **enp0s20u12u3** es la interfaz de la NIC de USB. La máscara de destino de vínculo local se repite y la NIC de USB no es la primera en el orden. Esto genera el problema de conectividad entre iDRAC Service Module e iDRAC mediante el paso del sistema operativo a la iDRAC. Para solucionar el problema de conectividad, asegúrese de que sea posible acceder a la dirección IPv4 de la NIC de USB de la iDRAC (el valor predeterminado es 169.254.1.1) desde el sistema operativo host.

Caso contrario:

- Cambie la dirección de la NIC de USB de iDRAC en una máscara de destino única.
- Elimine las entradas que no son necesarias de la tabla de enrutamiento a fin de asegurarse de que la NIC de USB quede seleccionada por ruta cuando el host desea alcanzar la dirección IPv4 de la NIC de USB de iDRAC.

En iDRAC Service Module versión 2.0 y anteriores, cuando desinstalo iDRAC Service Module desde un servidor VMware ESXi, el switch virtual recibe el nombre vSwitchiDRACvusb y el grupo de puertos recibe el nombre de la red de la iDRAC en el cliente vSphere. ¿Cómo puedo eliminarlos?

Mientras se instala el VIB de iDRAC Service Module en un servidor VMware ESXi, iDRAC Service Module crea el switch virtual y el grupo de puertos para comunicarse con la iDRAC a través del paso del sistema operativo a la iDRAC en el modo de NIC de USB. Después de la desinstalación, el switch virtual **vSwitchiDRACvusb** y el grupo de puertos **Red de iDRAC** no se eliminan. Para solucionar este problema, 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 switch virtual: `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:

Tabla 65. Ubicación de los registros de Lifecycle

Sistema operativo	Ubicación
Microsoft Windows	**Visor de eventos** > **Registros de Windows** > **Sistema**. Todos los registros de Lifecycle de iDRAC Service Module se replican en el nombre de origen de **iDRAC Service Module**. **NOTA:** En iSM versión 2.1 y posteriores, los registros de Lifecycle se replican en el nombre de origen del registro de Lifecycle Controller. En iSM versión 2.0 y anteriores, los registros se replican en el nombre de origen de iDRAC Service Module. **NOTA:** La ubicación del registro de Lifecycle se puede configurar mediante el instalador de IDRAC Service Module. Puede configurar la ubicación cuando instala iDRAC Service Module o modificando el instalador.
Red Hat Enterprise Linux, SUSE Linux, CentOS y Citrix XenServer	`/var/log/messages`
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 *Guía del usuario del módulo de servicio de iDRAC* disponible en https://www.dell.com/idracmanuals.

¿Cómo aumentar el rendimiento de la GPU para ciertas configuraciones?

Establezca el perfil del rendimiento del sistema del BIOS como rendimiento

En la configuración del procesador, establezca los valores de NPS como 4 y de CCX como automático

Mínimo 1 DIMM por canal

IOmmu = paso a través del sistema operativo Linux

RACADM

Después de realizar un restablecimiento de la iDRAC (mediante el comando racreset de RACADM), si se emite algún comando, aparece el siguiente mensaje. ¿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 de RPM:

```
rpm -ivh --force < filename >
```

Donde `filename` es el archivo de los paquetes openssl o libopenssl de RPM.

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.
- La propiedad iDRAC.Webserver.HttpsPort se cambia, incluso 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 particiones está en curso. Sin embargo, la partición se elimina después de cierto tiempo y aparecerá un mensaje que confirma la eliminación. Si esto no sucede, espere hasta que se complete la operación de creación de particiones y, luego, elimine la partición.

Configuración en forma permanente de la contraseña predeterminada a calvin

Si el sistema se envió con una contraseña predeterminada única de la iDRAC, pero desea establecer *calvin* como la contraseña predeterminada, debe utilizar los puentes disponibles en la tarjeta madre del sistema.

PRECAUCIÓN: El cambio de la configuración de los puentes cambia en forma permanente la contraseña predeterminada a *calvin.* No se podrá volver a la contraseña única incluso si se restablece la iDRAC a la configuración predeterminada de fábrica.

Para obtener más información sobre el procedimiento y la ubicación del puente, consulte la documentación para su servidor en https://www.dell.com/support.

Varios

La actualización falla cuando se actualiza a la versión más reciente.

NOTA: 3.30.30.30 es la versión mínima de iDRAC necesaria para actualizar a 4.00.00.00/4.10.10.10 de compilación posterior.

Después del restablecimiento del iDRAC, es posible que no se muestren todos los valores en la GUI del iDRAC.

NOTA: Si restablece el iDRAC por algún motivo, asegúrese de esperar al menos dos minutos después de restablecer el iDRAC para acceder o modificar cualquier ajuste en iDRAC.

Cuando se instala un sistema operativo, el nombre de host puede aparecer o no, o bien puede cambiar automáticamente.

Hay dos escenarios posibles:

- Escenario 1: la iDRAC no muestra el nombre de host más reciente una vez instalado un sistema operativo. Deberá instalar OMSA o iSM junto con la iDRAC para que se refleje el nombre de host.
- Escenario 2: la iDRAC tenía un nombre de host para un sistema operativo específico y se ha instalado otro sistema operativo diferente; aún el nombre de host aparece como el nombre anterior sin sobrescribir el nombre de host. La razón de esto es que el nombre de host es una información que proviene del sistema operativo; la iDRAC solo guarda la información. Si se ha instalado un nuevo sistema operativo, la iDRAC no restablece el valor del nombre de host. Sin embargo, las versiones más recientes de los sistemas operativos son capaces de actualizar el nombre de host en la 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** > **Implementación**. En la tabla que se muestra, observe la dirección IP del servidor.

- **Mediante la consola virtual**: reinicie el servidor para ver la dirección IP de iDRAC durante la autoprueba de encendido (POST). Seleccione la consola “Dell CMC” en la interfaz OSCAR para iniciar sesión en CMC a través de una conexión en serie local. Los comandos de RACADM de CMC se pueden enviar desde esta conexión.

  Para obtener más información sobre cómo descargar los comandos de CMC RACADM, consulte *Guía de la CLI de RACADM de la controladora de administración del chasis* disponible en https://www.dell.com/cmcmanuals.

  Para obtener más información sobre los comandos de iDRAC RACADM, consulte *Guía de la CLI de RACADM para iDRAC* disponible en https://www.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 iDRAC para un servidor blade?

NOTA: La opción de la interfaz web de OME Modular se puede aplicar solamente a las plataformas MX.

- **Mediante el uso de la interfaz web de OME-Modular**:

  Vaya a **Dispositivos** > **Procesamiento**. Seleccione el sled de la computadora y la IP de iDRAC se muestra como **IP de administración**.

- **Utilización de la aplicación OMM**: consulte *Guía del usuario de Dell EMC OpenManage Mobile* disponible en https://www.dell.com/openmanagemanuals
- **Mediante una conexión en serie**
- **Mediante la pantalla LCD**: en el menú principal, resalte el servidor y presione el botón de comprobación. Seleccione el servidor necesario y presione el botón de comprobación.

¿Cómo se busca una dirección IP de CMC relacionada con un servidor Blade?

NOTA: No es válido para las plataformas MX.

- **Desde la interfaz web de iDRAC**:

  Vaya a **Configuración de iDRAC** > **CMC**. Se mostrará la página **CMC Summary (Resumen de CMC)** con la dirección IP de CMC.

- **Desde la consola virtual**:

  Seleccione la consola “Dell CMC” en la interfaz OSCAR para iniciar sesión en CMC a través de una conexión en serie local. Los comandos de 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 cómo descargar los comandos de CMC RACADM, consulte *Guía de la CLI de RACADM de la controladora de administración del chasis* disponible en https://www.dell.com/cmcmanuals.

Para obtener más información sobre los comandos de iDRAC RACADM, consulte *Guía de la CLI de RACADM para iDRAC* disponible en https://www.dell.com/idracmanuals.

¿Cómo encontrar la dirección IP de OME Modular?

NOTA: Es válido solamente para las plataformas MX.

- **Desde la interfaz web de iDRAC**:

  Vaya a **Configuración de iDRAC** > **Módulo de administración**. Se mostrará la página **Módulo de administración** con la dirección IP de OME Modular.

¿Cómo se busca una dirección IP de iDRAC para un servidor tipo bastidor o torre?

- **Desde el RACADM local**:

  Utilice el comando `racadm getsysinfo`.

- **Desde el LCD**:

  En el servidor físico, utilice los botones de navegación del panel LCD para ver la dirección IP de iDRAC. Vaya a **Vista de configuración** > **Ver** > **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. (no para las plataformas MX)
- 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.

No se puede acceder a la iDRAC desde la LOM compartida

Es posible que la iDRAC esté inaccesible si hay errores irrecuperables en el sistema operativo host, como un error de BSOD en Windows. Para acceder a la iDRAC, reinicie el host para recuperar la conexión.

La LOM compartida no funciona después de activar el protocolo de control de agregación de vínculos (LACP).

Se debe cargar el controlador del sistema operativo host para el adaptador de red antes de activar LACP. Sin embargo, si se utiliza una configuración de LACP pasiva, la LOM compartida puede estar en funcionamiento antes de que se cargue el controlador del sistema operativo host. Consulte la documentación del switch para la configuración de LACP.

NOTA: No se puede acceder a la IP de LOM compartida en el estado previo al arranque cuando el switch está configurado con LACP.

El servidor Blade se ha insertado en el chasis y se ha presionado el interruptor de corriente, pero el servidor no se encendió.

- La iDRAC requiere hasta dos minutos para inicializar antes de que el servidor pueda encenderse.
- Compruebe el presupuesto de alimentación de CMC yOME Modular (solo para las plataformas MX). Es posible que se haya superado el presupuesto de alimentación del chasis.

¿Cómo se recupera el nombre de usuario y la contraseña de usuario administrativo de iDRAC?

Debe restaurar iDRAC a sus valores predeterminados. Para obtener más información, consulte Restablecimiento de iDRAC a los valores predeterminados de fábrica en la página 366.

¿Cómo se cambia el nombre de la ranura para el sistema en un chasis?

NOTA: No es válido para las plataformas MX.

1. Inicie sesión en la interfaz web de CMC y vaya a **Chasis** > **Servidores** > **Configuración**.
2. Ingrese 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 CMC (no para plataformas MX) y OME Modular (válido para las plataformas MX) para ver si la iDRAC se muestra como un componente actualizable. Si es así, siga las instrucciones en Actualización del firmware mediante la interfaz web de la CMC en la página 85 para actualizar el firmware.

NOTA: La función de actualización no es válida para las plataformas MX.

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.

No se puede iniciar sesión en la interfaz web de la iDRAC con el explorador Firefox en Linux ni Ubuntu. No se puede ingresar la contraseña.

Para resolver este problema, reinstale o actualice el explorador Firefox.

No se puede acceder a la iDRAC a través de la NIC de USB en SLES y Ubuntu

NOTA: En SLES, establezca la interfaz de la iDRAC en DHCP.

En Ubuntu, utilice la utilidad Netplan para configurar la interfaz de la iDRAC en el modo DHCP. Realice lo siguiente para configurar el DHCP:

1. Utilice `/etc/netplan/01-netcfg.yaml`.
2. Especifique Sí para el DHCP de la iDRAC.
3. Aplique la configuración.

Ilustración 5. Cómo configurar la interfaz de la iDRAC en el modo DHCP en Ubuntu

El modelo, el fabricante y otras propiedades no aparecen en la lista de adaptadores de red integrados en Redfish

No se mostrarán los detalles FRU de los dispositivos integrados. No habrá objetos FRU para los dispositivos integrados en la placa base. Por lo tanto, la propiedad dependiente no estará ahí.

31

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 la solución de problemas y poner el servidor en servicio mediante iDRAC.

Antes de realizar la solución de problemas de un servidor inaccesible, asegúrese de que se cumplan los siguientes prerrequisitos:

- Activación de la última pantalla de último bloqueo
- Activación de las alertas en iDRAC

Para identificar la causa, compruebe lo siguiente en la interfaz web de iDRAC y restablezca la conexión al sistema:

NOTA: Si no puede acceder a la interfaz web de iDRAC, vaya al servidor, acceda al panel LCD, escriba la dirección IP o el nombre de host y luego realice las siguientes operaciones mediante la interfaz web del iDRAC desde su estación de administración:

- Estado del LED del servidor: parpadea en color ámbar o permanece sólido en ámbar.
- Estado del LCD del panel anterior o mensaje de error: color ámbar del LCD o mensaje de error.
- La imagen del sistema operativo se muestra en la consola virtual. Si puede ver la imagen, restablezca el sistema (inicio flexible) 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 la iDRAC, vaya a **Overview (Descripción general)** > **Summary (Resumen)** para ver la información del sistema y acceder a los distintos vínculos de esta página y evaluar el estado 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 eventos 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 **Maintenance (Mantenimiento)** > **System Event Logs (Registros de eventos del sistema)** para ver el SEL y a **Lifecycle Log (Registro de Lifecycle)** para ver el registro de Lifecycle.

   NOTA: El SEL también se registra en el registro de Lifecycle. Use las opciones de filtrado para ver el SEL.

2. Exporte el SEL o el registro de Lifecycle en el formato XML a una ubicación externa (estación de administración, USB, recurso compartido de red, etc.). Como alternativa, puede activar el registro de sistema remoto, de modo que los registros que se escriban 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
- Interfaz de programación de aplicaciones de Redfish
- RACADM CLI (iDRAC_) y CMC (no se aplica a las plataformas MX)
- Dell Update Package (DUP)
- Interfaz web CMC (no se aplica a las plataformas MX)OME Modular (solo se aplica a las plataformas MX)
- 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 **Dashboard (Tablero)**, seleccione **Graceful Shutdown (Apagado ordenado)** y haga clic en **Apply (Aplicar)**.

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

Creación de una nueva cuenta de usuario de administrador

Puede modificar la cuenta de usuario de administrador local predeterminada o crear una cuenta de usuario de administrador nueva. Para modificar la cuenta local, consulte Modificación de la configuración de la cuenta de administrador local.

Para crear una cuenta de usuario de administrador nueva, consulte las secciones siguientes:

- Configuración de usuarios locales
- Configuración de usuarios de Active Directory
- Configuración de los usuarios LDAP genéricos

Inicio de la consola remota de servidores y montaje de una unidad USB

Para iniciar la consola remota de servidores y montaje de una unidad USB:

1. Conecte una unidad flash USB (con la imagen necesaria) a una estación de administración.
2. Utilice el siguiente método para iniciar la consola virtual a través de la interfaz web de iDRAC:
   - Vaya a **Dashboard (Tablero)** > **Virtual Console (Consola virtual)** y haga clic en **Launch Virtual Console (Iniciar consola virtual)**.

   Se muestra el **Vista previa de consola virtual**.
3. En el menú **File (Archivo)**, haga clic en **Virtual Media (Medios virtuales)** > **Launch Virtual Media (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 asignará al sistema administrado.

Instalación del sistema operativo básico conectado a los medios virtuales y los recursos compartidos de archivos remotos

Consulte la sección Implementación del sistema operativo mediante un recurso compartido de archivos remotos.

Administración de la densidad de bastidor

Antes de instalar servidores adicionales en un estante, debe determinar la capacidad restante en el estante.

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 ajustes de configuración de la identidad de E/S para varias tarjetas de red en un arranque individual del sistema host

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. Exportar el archivo del perfil de configuración del servidor (SCP) de iDRAC.
4. Edite la configuración de optimización de la identidad de E/S en el archivo de SCP.
5. Importe el archivo de SCP a iDRAC.