Guía del usuario iDRAC10

1.10.xx Series

Diciembre de 2024
Rev. A00

DELL Technologies

Notas, avisos y advertencias

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

PRECAUCIÓN: CAUTION indica la posibilidad de daños en el hardware o la pérdida de datos y le informa cómo evitar el problema.

AVISO: WARNING indica la posibilidad de daños en la propiedad, lesiones personales o la muerte.

Historial de revisiones

Tabla 1. Historial de revisiones

Fecha	Revisión del documento	Descripción de los cambios
Diciembre de 2024	A00	iDRAC10 versión 1.10.17.00

Tabla de contenido

1

Descripción general de iDRAC

Integrated Dell Remote Access Controller (iDRAC) está diseñada para mejorar su productividad, como administrador del sistema, y mejorar la disponibilidad general de los servidores de Dell EMC. iDRAC alerta sobre los problemas de sistema, le ayuda a realizar la administración remota del sistema y reduce la necesidad de obtener 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, además de solucionar problemas sobre ellos, desde cualquier ubicación, sin utilizar agentes ni sistemas operativos.

NOTA: Es posible que el comportamiento de iDRAC no sea coherente cuando se utiliza con hardware que no es de Dell.

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

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

iDRAC está disponible en las variantes siguientes:

- iDRAC Core: disponible de manera predeterminada en todos los servidores
- iDRAC Enterprise: disponible en todos los modelos de servidores
- iDRAC Datacenter: disponible en todos los modelos de servidores

Temas:

Ventajas de utilizar iDRAC

Entre los beneficios, se incluyen los siguientes:

- Mayor disponibilidad: notificación temprana de errores potenciales o reales que ayudan a evitar un error de servidor o reducir el tiempo de recuperación después de un error.
- 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 proporcionar acceso seguro a servidores remotos, los administradores pueden realizar funciones críticas de administración mientras conservan la seguridad del servidor y la red.

Características 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 Funciones sujetas a licencia en la iDRAC10.. Para ver la lista de funciones que no son compatibles con la iDRAC10 versión 1.10.17.00, consulte la sección Funciones no compatibles con esta versión.

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.
- Visualización de las interfaces de red disponibles en los sistemas operativos host
- iDRAC10 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 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
- Cambios en la configuración del servidor mediante la función de perfil de configuración del servidor (SCP). Para obtener más información, consulte la Guía de referencia de SCP.
- Configuración de la política de persistencia de las direcciones virtuales, del iniciador y los objetivos 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 hot spare 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 la 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
- 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 energía.
- 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.
  - Habilite o deshabilite el estado de ciclo de encendido completo de todos los componentes del sistema, excepto la PSU.
  - Restablezca forzadamente de manera remota el iDRAC
  - Habilite las alertas de SNMP dentro de 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 en una recopilación de SupportAssist. Esto se aplica únicamente si se ha instalado el módulo de servicio de iDRAC versión 2.0 o posterior.

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 Technologies recomienda utilizar el puerto Gigabit Ethernet dedicado disponible en servidores en rack 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

La protección del acceso a recursos de red críticos es una prioridad. La iDRAC implementa una serie de funciones de seguridad que incluyen:

- 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 para cada versión de la iDRAC10.

Versión de firmware 1.10.17.00

En la versión iDRAC10 1.10.17.00, se agregaron las siguientes características en la iDRAC:

- Seguridad mejorada con procesador de seguridad dedicado:
  - Rendimiento de seguridad mejorado
  - Raíz de confianza (RoT) integrada, certificación a nivel de dispositivo y cifrado
  - Algoritmos de cifrado más fuertes
- Interfaz de usuario actualizada:
  - Experiencia de usuario coherente en todas las consolas de Dell Technologies
  - Interfaz simplificada
  - Navegación más sencilla
- Estructura de licencias simplificada en PowerEdge de 17.ª generación
- Cree funciones de usuario personalizadas de la iDRAC
- Recuperación de alimentación de CA controlada por la iDRAC (el BIOS de generaciones anteriores administraba esta configuración)

Funciones obsoletas

Las siguientes características están obsoletas en la iDRAC10:

- Administrador de grupo
- WS-MAN
- TLS 1.1
- vFLASH

Características no soportadas en esta versión inicial de la iDRAC10

Las siguientes características no son compatibles con las versiones 1.1x del firmware de la iDRAC10.

Tabla 2. Características no soportadas

Función	Funciones
GUI de iDRAC	Soporte para la GUI de la iDRAC para otros idiomas internacionales
	RACADM local (sistema operativo dentro de banda)
	RACADM remoto
	Herramientas de iDRAC
	Serie: serie RAC
	UI de Lifecycle Controller
	Serie: serie IPMI

Tabla 2. Características no soportadas (continuación)

Función	Funciones
NOTA: Se puede acceder a la CLI de RACADM a través de la interfaz del SSH.	
Redes y conectividad	Bloqueo de IP
	Rango IP
	Configuración del SCP de la iDRAC Direct (USB)
	Sincronización rápida
	Vista de conexión de red
Administración remota	Comunicación en serie en la LAN con SSH
	Carpetas virtuales
	Recurso compartido de archivos remotos
	Control de calidad/ancho de banda
	Colaboración de consola virtual (hasta seis usuarios en simultáneo)
	Chat de consola virtual
	Portapapeles virtual
	Seguimiento de recurso
	Seguimiento de uso del mercado (MUT)
	Kit de desarrollo de software (SDK)
	Medios virtuales: sesión única
iDRAC Service Module (iSM)	Restablecimiento forzado de la iDRAC y otras funciones
	Información de red
	IBIA
	Ciclo de apagado y encendido virtual
	Preparar para quitar
	SSO de la iDRAC
	Detalles del sistema operativo
	Monitoreo de chipset SATA
	RAID de software
	Replicación de registros de Lifecycle Controller
	SNMP dentro de la banda
	Integración de SupportAssist
	Correlación de eventos de SDS
	Instalación del iSM
Alertas	Eventos de ciclo de vida útil de Redfish (RLCE)
	Registro del sistema remoto: no seguro
	Registro del sistema remoto: seguro
	Telemetría: transmisión
	Telemetría: informes de métricas
	Activadores de telemetría

Tabla 2. Características no soportadas (continuación)

Función	Funciones
	Funciones de inyección de métricas del sistema operativo del iSM para telemetría
Administración de plataformas	SDPM de memoria
	NVDIMM de memoria
	Monitoreo de rendimiento fuera de banda
	Detección de servidores inactivos
	Monitoreo de enfriamiento líquido
Alimentación y elementos térmicos	Límites de alimentación
	Monitoreo de energía: medidor de alimentación en tiempo real
	Gráficos de alimentación en tiempo real
	Contadores de datos históricos de alimentación
	Integración del plug-in de administración de energía de OME
	Límite de corriente de entrada
	Aire fresco
	ASHERE
	Temperatura de salida personalizada
	Gráficos de temperatura
	Límite de sonido 1.0
	Consumo de flujo de aire del sistema, temperatura de entrada de PCIe personalizada
	Personalización de flujo de aire de PCIe
Storage Management	Administración de gabinetes externos
	Administrador de clave empresarial segura (SEKM) y administración de claves locales de la iDRAC (iLKM)
	HBA: inventario y monitoreo en tiempo real
	HBA: inventario en etapas
Administración de comunicación	DPU: inventario en tiempo real, monitoreo y configuración
	DPU: inventario y configuración en etapas
	Administración de dirección virtual
	Características de la DPU/SmartNIC
	FC: inventario y monitoreo en tiempo real
	FC: inventario y configuración en etapas
Administración de aceleradores	FPGA: inventario en etapas
	FGPA: inventario en tiempo real, alimentación y temperatura
Implementación/configuración del servidor	Paquete de controladores
	Perfil de configuración del servidor: actualización del repositorio
	Perfil de configuración del servidor: implementación del sistema operativo
	Configuración local

Tabla 2. Características no soportadas (continuación)

Función	Funciones
	Configuración sin intervención
Actualización del sistema	Actualización del catálogo
	Herramientas de actualización incorporadas
	Actualización automática
Fábrica, diagnóstico, servicio y registro	Restablecimiento de los valores predeterminados de iDRAC
	Borrado seguro
	Video de pantalla de bloqueo con el agente
	Captura de pantalla de bloqueo
	Registro de datos en serie
	Captura de video de bloqueo sin agente
	Notas de trabajo
	Registro del sistema remoto para alertas
Autenticación y autorización	Usuario local: cuenta reservada
	Servicios de directorio
	Active Directory: esquema estándar
	Active Directory: esquema extendido
	Inicio de sesión único (SSO)
	Autentificación de dos factores (2FA): tarjeta inteligente
	Autenticación de dos factores (2FA): simple
	Autenticación de clave pública de Secure Shell (SSH PKA)
	Autenticación de múltiples factores de RSA (RSA MFA)
	OAuth
	OpenID Connect
Seguridad	Certificado SSL: certificado de firma personalizado
	Certificado SSL: inscripción automática de certificados
	FIPS 140-2/140-3
	Banner de política de seguridad personalizable
	Bloqueo de IP/protección de denegación de servicio (DOS)
	Seguridad adicional de QuickSync 2.0
	Modo de bloqueo del sistema
	Filtrado de rango de IP
	Cadena personalizada de cifrado
	Configuración local
	Red de la iDRAC: seguridad 802.1x
	BIOS Livescan
Administración térmica	Personalización de flujo de aire PCIe (LFM)
	Control de escape personalizado

Tabla 2. Características no soportadas (continuación)

Función	Funciones
	Control delta-T personalizado
	Temperatura de entrada PCIe personalizada
	Consumo de flujo de aire del sistema
Otra opción	ICA adaptable

Cómo utilizar esta guía

Instrucciones del usuario

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

1. 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.
2. RADCAM: Aquí se proporciona el comando u objeto RACADM que debe usar. Para obtener más información, consulte la **Guía de la CLI de RACADM de la iDRAC10** que se encuentra disponible en el sitio de soporte de Dell.
3. Utilidad de ajustes de iDRAC: Aquí se proporciona solo la información relacionada con la tarea. Para obtener información sobre los campos y las opciones, consulte la **Ayuda en línea de la utilidad de configuración de iDRAC,** a la que puede acceder cuando hace clic en **Ayuda** en la GUI de configuración de iDRAC (presione <F2> durante el arranque y, a continuación, haga clic en **Ajustes de iDRAC** en la página **Menú principal de configuración del sistema**).
4. Redfish: aquí se proporciona solo la información relacionada con la tarea. Para obtener información sobre los campos y las opciones, consulte la **Guía de la API de Redfish de la iDRAC10** en el portal para desarrolladores.

Navegadores web compatibles

Para ver la lista de versiones compatibles, consulte las **Notas de la versión de la iDRAC10** en el sitio de soporte de Dell.

Hipervisores y sistemas operativos compatibles

Para ver la lista de versiones compatibles de sistemas operativos e hipervisores, consulte las **Notas de la versión de la iDRAC10** en el sitio de soporte de Dell.

Licencias de la iDRAC

Las funciones de la iDRAC están disponibles según el tipo de licencia. La licencia de la iDRAC Core está instalada de manera predeterminada. La licencia de la iDRAC Enterprise está disponible como una actualización y se puede comprar 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 iDRAC10.

Tipos de licencias

La licencia estándar de la iDRAC está disponible de manera predeterminada en el sistema. Las licencias de la iDRAC Enterprise y Datacenter incluyen todas las funciones con licencia y se pueden adquirir en cualquier momento. A continuación, se indican los tipos de ventas de productos de gama superior:

- Evaluación durante 30 días: las licencias de evaluación se basan en períodos y el tiempo transcurre desde que se enciende el sistema. Esta licencia no se puede ampliar.
- Perpetua: la licencia está enlazada a la etiqueta de servicio y es permanente.

En la siguiente tabla, se enumeran las licencias predeterminadas disponibles en los sistemas:

Tabla 3. Licencias predeterminadas

Licencia de la iDRAC Core	Licencia de iDRAC Enterprise	Licencia de iDRAC Datacenter
• Disponible para todos los servidores • Proporciona características principales de administración de sistemas.	• Disponible como una venta adicional en todos los servidores • Incluye todas las funciones de Core, automatización, consola virtual y seguridad. • Se incluye con las licencias de administración segura de claves empresariales (SEKM) y verificación segura de componentes (SCV).	• Disponible como una venta adicional en todos los servidores • Incluye todas las características de Core y Enterprise. • Incluye funciones clave, como streaming de telemetría y administración térmica. • Incluye aceleradores avanzados (GPU y DPU), administración del sistema y enfriamiento avanzado por aire y líquido.

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 la iDRAC, RACADM, Redfish y Lifecycle Controller-Remote Services para una administración de licencias de uno a uno y Dell License Manager para la administración de licencias de uno a varios:

- Ver: ver la información de la licencia actual.
- Importar: después de adquirir la licencia, guárdela en un almacenamiento local e impórtela en la 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.

- Exportar: permite exportar la licencia instalada. Para obtener más información, consulte la **Ayuda en línea de iDRAC**.
- 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.

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

- Visualización y exportación de 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 RACADM

Administración de licencias

1. Para administrar licencias mediante RACADM, utilice el subcomando **license**.
2. Para obtener más información, consulte Guía de la CLI RACADM de Integrated Dell Remote Access Controller.

Administración de licencias mediante la interfaz web de iDRAC

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

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

Funciones sujetas a licencia en iDRAC10

En la siguiente tabla se proporcionan las funciones de la iDRAC10 activadas según la licencia adquirida:

Tabla 4. Funciones sujetas a licencia en iDRAC10

Funciones	iDRAC 10 Core	iDRAC 10 Enterprise	iDRAC 10 Datacenter
Interfaces y estándares			
Redfish y API RESTful de iDRAC	Sí	Sí	Sí
IPMI 2.0	Sí	Sí	Sí
DCMI 1.5	Sí	Sí	Sí
Interfaz gráfica web del usuario	Sí	Sí	Sí
Línea de comandos de RACADM (local/remota)	Sí	Sí	Sí
SSH	Sí	Sí	Sí
Redirección serial	Sí	Sí	Sí

Tabla 4. Funciones sujetas a licencia en iDRAC10 (continuación)

Funciones	iDRAC 10 Core	iDRAC 10 Enterprise	iDRAC 10 Datacenter
Protocolo de hora de red (NTP)	Sí	Sí	Sí
Conectividad			
NIC compartida (LOM)	Sí	Sí	Sí
NIC dedicado	Sí	Sí	Sí
Etiquetado VLAN	Sí	Sí	Sí
IPv4	Sí	Sí	Sí
IPv6	Sí	Sí	Sí
DHCP	Sí	Sí	Sí
DHCP sin intervención manual	No	Sí	Sí
DNS dinámico	Sí	Sí	Sí
Paso a través del sistema operativo	Sí	Sí	Sí
iDRAC directa: USB del panel frontal	Sí	Sí	Sí
Vista Conexión	Sí	Sí	Sí
DPU	No	Sí	Sí
Seguridad			
Autoridad basada en roles	Sí	Sí	Sí
Usuarios locales	Sí	Sí	Sí
Cifrado SSL	Sí	Sí	Sí
Administración de claves empresariales seguras y administrador de claves local de iDRAC	No	Sí (con licencia SEKM)	Sí (con licencia SEKM)
Bloqueo de dirección IP	No	Sí	Sí
Servicios de directorio (AD, LDAP)	No	Sí	Sí
Autentificación de dos factores (tarjeta inteligente)	No	Sí	Sí
Inicio de sesión único	No	Sí	Sí
Autentificación de PK (para SSH)	Sí	Sí	Sí
Integración de OAuth con servicios de autenticación basados en la Web	No	No	Sí
Control de acceso de red basado en puerto (IEEE 802.1x)	No	No	Sí
OpenID Connect para consolas Dell	No	No	Sí
FIPS 140-2	Sí	Sí	Sí
Inicio de UEFI seguro: administración de certificados	Sí	Sí	Sí

Tabla 4. Funciones sujetas a licencia en iDRAC10 (continuación)

Funciones	iDRAC 10 Core	iDRAC 10 Enterprise	iDRAC 10 Datacenter
Bloqueo del sistema	No	Sí	Sí
Contraseña predeterminada única de iDRAC	Sí	Sí	Sí
Banner de política de seguridad personalizable: página de inicio de sesión	Sí	Sí	Sí
Autenticación multifactor Easy	No	Sí	Sí
Inscripción automática de certificados (certificados SSL)	No	No	Sí
Quick Sync 2 de iDRAC: aut. opcional para operaciones de lectura	Sí	Sí	Sí
Quick Sync 2 de iDRAC: adición de número de dispositivo móvil en LCL	Sí	Sí	Sí
Borrado seguro	Sí	Sí	Sí
Escaneo activo del BIOS	No	Sí	Sí
Inscripción automática de certificado de SSL	No	Sí	Sí
Autenticación de dos factores (2FA) de RSA SecureID	No	Sí	Sí
Dispositivo RoT	Sí	Sí	Sí
Detección de intrusiones	Sí	Sí	Sí
Control de acceso USB	Sí	Sí	Sí
Verificación segura de componentes	No	Sí	Sí
Presencia remota			
Control de alimentación	Sí	Sí	Sí
Control de arranque	Sí	Sí	Sí
Comunicación en serie en la LAN	Sí	Sí	Sí
Medios virtuales	No	Sí	Sí
Carpetas virtuales	No	Sí	Sí
Recurso compartido de archivos remotos	No	Sí	Sí
Acceso de HTML5 a consola virtual	No	Sí	Sí
Consola virtual	No	Sí	Sí
Portapapeles virtual	No	Sí	Sí
Conexión VNC al sistema operativo	No	Sí	Sí
Control de calidad/ancho de banda	No	Sí	Sí

Tabla 4. Funciones sujetas a licencia en iDRAC10 (continuación)

Funciones	iDRAC 10 Core	iDRAC 10 Enterprise	iDRAC 10 Datacenter
Colaboración de consola virtual (hasta seis usuarios en simultáneo)	No	Sí	Sí
Chat de consola virtual	No	Sí	Sí
Compatibilidad con HTTP/ HTTPS junto con NFS/CIFS	Sí	Sí	Sí
Alimentación y elementos térmicos			
Administración térmica avanzada	No	Sí	Sí
Medidor de alimentación en tiempo real	Sí	Sí	Sí
Umbrales y alertas de alimentación	Sí	Sí	Sí
Gráficos de alimentación en tiempo real	No	Sí	Sí
Contadores de datos históricos de alimentación	No	Sí	Sí
Límites de alimentación	No	Sí	Sí
Integración de Power Center	No	Sí	Sí
Gráficos de temperatura	Sí	Sí	Sí
Personalización de flujo de aire PCIe (LFM)	No	Sí	Sí
Control de escape personalizado	No	Sí	Sí
Control Delta-T personalizado	No	Sí	Sí
Consumo de flujo de aire del sistema	No	Sí	Sí
Temperatura de entrada PCIe personalizada	No	Sí	Sí
Estado			
Supervisión completa sin agentes	Sí	Sí	Sí
Supervisión de la temperatura	Sí	Sí	Sí
Supervisión predictiva de fallas	Sí	Sí	Sí
SNMPv1 y v2 y v3 (capturas y obtenciones)	Sí	Sí	Sí
Alertas de correo electrónico	No	Sí	Sí
Umbrales configurables	Sí	Sí	Sí
Supervisión de ventiladores	Sí	Sí	Sí
Supervisión de suministros de energía	Sí	Sí	Sí
Supervisión de memoria	Sí	Sí	Sí
GPU	No	Sí	Sí
Supervisión de CPU	Sí	Sí	Sí

Tabla 4. Funciones sujetas a licencia en iDRAC10 (continuación)

Funciones	iDRAC 10 Core	iDRAC 10 Enterprise	iDRAC 10 Datacenter
Detección de fugas de GPU y CPU	Sí	Sí	Sí
Controladoras de almacenamiento	Sí	Sí	Sí
Supervisión de NIC	Sí	Sí	Sí
Inventario óptico	Sí	Sí	Sí
Estadísticas ópticas	No	No	Sí
Supervisión de disco duro	Sí	Sí	Sí
Supervisión de rendimiento fuera de banda	No	Sí	Sí
Alertas de desgaste excesivo de SSD	Sí	Sí	Sí
Configuración personalizable para temperatura de salida	Sí	Sí	Sí
Registros de datos en serie	No	Sí	Sí
Registros SMART para unidades de almacenamiento	No	Sí	Sí
Detección de servidores Idle	No	Sí	Sí
Telemetría	No	Sí	Sí
Recopilación de la condición	Sí	Sí	Sí
Actualizar			
Actualización remota sin agentes	Sí	Sí	Sí
Herramientas de actualización incorporadas	Sí	Sí	Sí
Actualizar desde el repositorio	Sí	Sí	Sí
Programar actualización desde el repositorio (actualización automática)	Sí	Sí	Sí
Actualizaciones de firmware	Sí	Sí	Sí
Implementación y configuración			
Configuración local a través de F2	No	Sí	Sí
Herramientas incorporadas de implementación del sistema operativo	Sí	Sí	Sí
Herramientas de configuración incorporadas	Sí	Sí	Sí
Autodiscovery	No	Sí	Sí
Implementación remota del sistema operativo	No	Sí	Sí
Paquete incorporado de controladores	Sí	Sí	Sí

Tabla 4. Funciones sujetas a licencia en iDRAC10 (continuación)

Funciones	iDRAC 10 Core	iDRAC 10 Enterprise	iDRAC 10 Datacenter
Configuración completa del inventario	Sí	Sí	Sí
Exportación de inventario	Sí	Sí	Sí
Configuración remota	Sí	Sí	Sí
Configuración sin intervención	No	Sí	Sí
Retiro/replanificación del sistema	Sí	Sí	Sí
Exportación de perfil de configuración del servidor	Sí	Sí	Sí
Importación de perfil de configuración del servidor	No	Sí	Sí
Vista previa de perfil de configuración del servidor	Sí	Sí	Sí
Configuración de BIOS	Sí	Sí	Sí
Configuración del almacenamiento	No	Sí	Sí
Diagnóstico, servicio y registro			
Seguimiento de recurso	Sí	Sí	Sí
Herramientas de diagnóstico incorporadas	Sí	Sí	Sí
Reemplazo de piezas	Sí	Sí	Sí
Easy Restore (configuración del sistema)	Sí	Sí	Sí
Indicadores LED de estado de la condición	Sí	Sí	Sí
iDRAC Quick Sync 2 (hardware BLE/Wi-Fi)	Sí	Sí	Sí
iDRAC directo (puerto de administración de USB frontal)	Sí	Sí	Sí
Módulo de servicio de iDRAC (iSM) integrado	Sí	Sí	Sí
Reenvío de alertas de iSM a alertas en banda para las consolas	Sí	Sí	Sí
Recopilación de SupportAssist (incorporada)	Sí	Sí	Sí
Captura de pantalla de bloqueo	Sí	Sí	Sí
Captura de video de bloqueo	No	Sí	Sí
Captura de video de bloqueo sin agente (solo Windows)	No	No	Sí
Captura de inicio	Sí	Sí	Sí
Restablecimiento remoto de iDRAC (requiere iSM)	Sí	Sí	Sí
NMI virtual	Sí	Sí	Sí

Tabla 4. Funciones sujetas a licencia en iDRAC10 (continuación)

Funciones	iDRAC 10 Core	iDRAC 10 Enterprise	iDRAC 10 Datacenter
2FA	No	Sí	Sí
Inventario y supervisión del dispositivo	Sí	Sí	Sí
Notas de trabajo	Sí	Sí	Sí
Vigilancia del sistema operativo	Sí	Sí	Sí
Registro de sucesos del sistema	Sí	Sí	Sí
Registro de Lifecycle	Sí	Sí	Sí
Registro mejorado en el registro de Lifecycle Controller	Sí	Sí	Sí
Syslog remoto	No	Sí	Sí

NOTA: Para ver la lista de funciones que no son compatibles con esta versión, consulte Funciones no compatibles con esta versión

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 5. 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 la iDRAC, además de otras funciones. Para acceder a la utilidad "Configuración de la iDRAC", presione <F2> durante el inicio y juego haga clic en **Configuración de la iDRAC** en la página **Menú principal de configuración del sistema**.
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.
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.

Tabla 5. Interfaces y protocolos para acceder a iDRAC (continuación)

Interfaz o protocolo	Descripción
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 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 va de servidores independientes 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. Consulte la guía API de Redfish de iDRAC.
Puerto USB Type-C	Acceda a la iDRAC mediante el puerto USB tipo C etiquetado.
SSH	Utilice el SSH para ejecutar comandos RACADM o iniciar una sesión de redirección de consola. El servicio SSH está activado de forma predeterminada en iDRAC. El servicio de SSH se puede deshabilitar en la iDRAC. La iDRAC solo admite el 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 **Guía del usuario de las utilidades de Dell OpenManage Baseboard Management Controller**. **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	La iDRAC soporta el protocolo de Server Message Block (SMB). Este es un protocolo de uso compartido de archivos de red. Las versiones de SMB compatibles son de la 2.0 a la 3.11. SMBv1 ya no se soporta.
NFS	La iDRAC 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.
TFTP	La iDRAC utiliza el protocolo de transferencia de archivos trivial (TFTP) para actualizaciones de firmware e instalaciones de certificados.
CIFS	La iDRAC utiliza el protocolo sistema de archivos de Internet común (CIFS) para compartir archivos de manera remota. El CIFS monta archivos de imagen ISO o IMG desde un recurso compartido de red al sistema operativo del servidor administrado como unidades virtuales.
HTTP y HTTPS	La iDRAC es compatible con el protocolo de transferencia de hipertexto (HTTP) y el protocolo de transferencia de hipertexto seguro (HTTPS) para la administración remota de servidores Dell.

Información sobre puertos iDRAC

En la siguiente tabla, se enumeran los puertos necesarios para acceder a iDRAC de manera remota a través del firewall. 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 puertos, consulte Servicios de configuración.

Tabla 6. Los puertos que iDRAC escucha para las conexiones

Número de puerto	Tipo	Función	Puerto configurable	Nivel máximo de cifrado
22	TCP	SSH	Sí	SSL de 256 bits
80	TCP	HTTP	Sí	Ninguna

Tabla 6. Los puertos que iDRAC escucha para las conexiones (continuación)

Número de puerto	Tipo	Función	Puerto configurable	Nivel máximo de cifrado
161	UDP	Agente SNMP	Sí	Ninguna
443	TCP	HTTPS	Sí	SSL de 256 bits
623	UDP	RMCP/RMCP+	No	SSL de 128 bits
5000	TCP	iDRAC a iSM	No	SSL de 256 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 7. Los puertos que iDRAC utiliza como cliente

Número de puerto	Tipo	Función	Puerto configurable	Nivel máximo de cifrado
25	TCP	SMTP	Sí	Ninguna
53	UDP	DNS	No	Ninguna
68	UDP	Dirección IP del DHCP-assigned	No	Ninguna
69	TFTP	TFTP	No	Ninguna
123	UDP	Protocolo de hora de red (NTP)	No	Ninguna
162	UDP	SNMP trap	Sí	Ninguna
445	TCP	Common Internet File System (CIFS)	No	Ninguna
636	TCP	LDAP mediante SSL (LDAPS)	No	SSL de 256 bits
2049	TCP	Network File System (NFS)	No	Ninguna
3269	TCP	LDAPS para catálogo global (GC)	No	SSL de 256 bits
5353	UDP	mDNS	No	Ninguna
514	UDP	Syslog remoto	Sí	Ninguna

Otros documentos que podrían ser de utilidad

La interfaz de usuario de iDRAC soporta la **Ayuda en línea** integrada a la que se puede acceder haciendo clic en la pestaña **Ayuda y comentarios**. 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 **Guía de la API de Redfish de la iDRAC**, se proporciona información sobre la API de Redfish.
- En la Guía de la CLI de RACADM de Integrated Dell Remote Access Controller, se proporciona información sobre los subcomandos RACADM, las interfaces soportadas y las definiciones de objetos y los grupos de bases de datos de propiedad de iDRAC.
- En el documento *Guía de visión 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 Dell Remote Access Configuration Tool** 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 la versión** proporcionan actualizaciones de última hora relativas al sistema o a la documentación o material avanzado de consulta técnica destinado a técnicos o usuarios experimentados.
- En el **Registro de atributos de Integrated Dell Remote Access Controller 10**, se proporcionan detalles sobre los grupos y objetos en la base de datos de propiedades de iDRAC.

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 comunicarse con Dell

Dell proporciona varias opciones de servicio y asistencia en línea y por teléfono. La disponibilidad varía según el producto, el país o la región y es posible que algunos servicios no estén disponibles en su área. Si desea comunicarse con Dell para tratar cuestiones relacionadas con las ventas, el soporte técnico o el servicio de atención al cliente, vaya a Comuníquese 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 de Dell.

Acceso a documentos desde el sitio de soporte de Dell

Haga clic en los siguientes enlaces para acceder a los documentos desde el sitio de soporte de Dell:

- Documentos de OpenManage Connections y Enterprise Systems Management
- Documentos de OpenManage
- Documentos de iDRAC y Lifecycle Controller
- Documentos sobre herramientas de facilidad de reparación
- Documentos de Client Command Suite Systems Management

Acceso a los documentos mediante la búsqueda de productos

1. Vaya al sitio Soporte de Dell.
2. En el cuadro de búsqueda **Ingresar una etiqueta de servicio**, **Número de serie...**, escriba el nombre del producto. Por ejemplo, **PowerEdge** o **iDRAC**. Se muestra una lista de archivos que coinciden.
3. Seleccione su producto y haga clic en el ícono 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. Vaya a Soporte de Dell.
2. Haga clic en **Buscar todos los productos**.
3. Haga clic en la categoría de producto necesaria, como Servidores, Software, Almacenamiento, etc.
4. Haga clic en el producto necesario y, luego, haga clic en la versión, si corresponde.

NOTA: En el caso de algunos productos, es posible que deba navegar por las subcategorías.

5. Haga clic en **DOCUMENTACIÓN**.
6. Haga clic en **MANUALES Y DOCUMENTOS**.

Acceso a la API de Redfish

La guía de API de Redfish ya está disponible en Dell API Marketplace

1. Vaya al portal para desarrolladores.
2. Haga clic en **Explorar API** y, a continuación, en **API**.
3. En API de Redfish de iDRAC10, 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 la 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 la iDRAC se asigna dinámicamente.

NOTA:

- Debe disponer del privilegio de inicio de sesión en iDRAC para poder completar dicha acción.
- La UI de iDRAC no admite los botones del explorador como **Atrás**, **Siguiente** o **Actualizar**.
- Después de detectar la dirección IP de la iDRAC, puede tardar un máximo de cinco minutos en iniciar sesión en la iDRAC. Si no puede iniciar sesión, comuníquese con el equipo de soporte técnico.

Banner de seguridad personalizable

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

Temas:

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

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

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

Puede configurar el nombre de usuario, la contraseña y los permisos de acceso para un usuario de iDRAC nuevo o existente mediante la opción **Agregar/editar usuario** en la GUI de iDRAC.

Para configurar el usuario, utilice un nombre de usuario único. Debe contener 16 caracteres, incluidos espacios en blanco. Se admiten los siguientes caracteres:

- Entre 0 y 9
- A-Z
- a-z
- Caracteres especiales: + %) > $ [| ! & = * . , - {] # (? < ; _ } I ^

Cuando el nombre de usuario se cambia, aparece el nombre nuevo en la interfaz web solo después del siguiente inicio de sesión del usuario.

NOTA: No utilice un espacio antes o después del nombre de usuario.

El campo Contraseña puede tener hasta 127 caracteres. Los caracteres están enmascarados. Se admiten los siguientes caracteres:

- Entre 0 y 9
- A-Z
- a-z
- Caracteres especiales: +, &, ? > - } | . ! (' , _ [" @ #) * ; $] / % = < : { I \ `

NOTA: Para mejorar la seguridad, se recomienda utilizar contraseñas complejas de al menos 8 caracteres, que incluyan letras minúsculas, mayúsculas, números y caracteres especiales. También se recomienda cambiar periódicamente las contraseñas, si es posible.

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

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

NOTA: La autenticación de LDAP con OpenDS es compatible. La clave DH debe ser mayor que 768 bits.

NOTA: La función RSA se puede configurar y habilitar para usuarios de LDAP, pero RSA no es compatible si LDAP está configurado en Microsoft Active Directory. Por lo tanto, falla el inicio de sesión del usuario de LDAP. RSA solo se admite para OpenLDAP.

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

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

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

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

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

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

   El dominio de Active Directory en el menú desplegable **Dominio** muestra el último dominio utilizado.
5. Para un usuario de LDAP, en los campos **Nombre de usuario** y **Contraseña**, escriba su nombre de usuario y contraseña de LDAP. El nombre de dominio no se requiere para un inicio de sesión de LDAP. De manera predeterminada, la opción **Esta iDRAC** se selecciona en el menú desplegable.
6. Haga clic en **Enviar**. Inició sesión en iDRAC con los privilegios de usuario requeridos.

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

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

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

- Cargar el certificado de tarjeta inteligente del usuario y el certificado de 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.

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 que inserte 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 lo siguiente:

- Cargue un certificado de autoridad de certificación (CA) de confianza (certificado de Active Directory firmado por una CA) en iDRAC.
- Configure el servidor DNS.

- Habilite el inicio de sesión de Active Directory.
- Habilite 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 que inserte la tarjeta inteligente.

   NOTA: Si se cambió el número de puerto HTTPS predeterminado (puerto 443), escriba: `https://[IP address]:[port number]`, en el que `[IP address]` es la dirección IP de iDRAC y `[port number]` es el número de puerto de HTTPS.

2. Inserte la tarjeta inteligente y haga clic en **Iniciar sesión**.
   Se muestra un símbolo del sistema para el **PIN** de la tarjeta inteligente.
3. Ingrese el PIN y haga clic en **Enviar**.

   Inició sesión en iDRAC con sus credenciales de Active Directory.

   NOTA: Si el usuario de la tarjeta inteligente está presente en Active Directory, no se necesita una contraseña de Active Directory.

   NOTA: Para las estaciones de trabajo cliente que forman parte del dominio de Active Directory, el uso de tarjetas inteligentes restringe la profundidad de la cadena de certificados a 10. Sin embargo, el uso de tarjetas inteligentes en estaciones de trabajo cliente que no forman parte del dominio no tienen límite en cuanto a la profundidad de las cadenas de certificados del cliente.

Inicio de sesión en iDRAC mediante inicio de sesión único

Cuando el Single Sign-On (SSO) está habilitado, puede iniciar sesión en el iDRAC sin introducir las credenciales de autenticación de usuario del dominio, como nombre de usuario y contraseña.

NOTA: Cuando un 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 Single Sign-On, asegúrese de lo siguiente:

- Haber iniciado sesión en el sistema con una cuenta de usuario válida de Active Directory.
- La opción Single Sign-On se habilita durante la configuración de Active Directory.

Para iniciar sesión en iDRAC mediante la interfaz web:

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

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

   NOTA: Si utiliza dirección IP en lugar de FQDN, se produce un error en el SSO.

   iDRAC le permite iniciar sesión con los privilegios correspondientes de Active Directoryde Microsoft y utilizar las credenciales almacenadas en el sistema operativo cuando inició sesión con una cuenta válida de Active Directory.

Acceso a iDRAC mediante RACADM remoto

RACADM remoto y local, que forman parte de la CLI de RACADM, no están disponibles en la versión 1.10.17.00 de la iDRAC10. Sin embargo, puede utilizar la CLI de RACADM a través de la interfaz SSH de la iDRAC.

Para obtener más información, consulte Guía de la CLI RACADM de Integrated Dell Remote Access Controller.

Si la estación de administración no almacenó el certificado SSL de iDRAC en su almacenamiento de certificados predeterminado, se muestra un mensaje de advertencia cuando se ejecuta el comando de RACADM. Sin embargo, el comando se ejecuta correctamente.

NOTA: El certificado de iDRAC es el certificado que iDRAC envía al cliente RACADM para establecer la sesión segura. Este certificado lo emite una CA o está autofirmado. En cualquier caso, si la estación de administración no reconoce a la CA o a la autoridad firmante, se muestra una precaución.

Validación del certificado de CA para usar RACADM remoto en Linux

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

Para validar el certificado para el uso de RACADM remoto:

1. Convierta el certificado en formato DER a 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, la ubicación para RHEL de 64 bits es **/etc/pki/tls/cert.pem**.
3. Anexe el certificado de CA con formato PEM al certificado de CA de la estación de administración.

   Por ejemplo, utilice el `cat command: cat testcacert.pem >> cert.pem`
4. Genere y cargue el certificado del servidor en iDRAC.

Acceso a la iDRAC mediante RACADM local

RACADM remoto o local, que forman parte de la CLI de RACADM, no están disponibles en la versión 1.10.17.00 de la iDRAC10. Sin embargo, puede utilizar la CLI de RACADM a través de la interfaz SSH de la iDRAC. Para obtener más información sobre cómo acceder a iDRAC mediante RACADM local, consulte Guía de la CLI RACADM de Integrated Dell Remote Access Controller.

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 RACADM de Integrated Dell Remote Access Controller.

Autenticación simple de dos factores (2FA simple)

Para mejorar la seguridad, la iDRAC ofrece una opción simple de autenticación de 2 factores a los usuarios locales. 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.

En un momento determinado, solo se recuerda una dirección IP de origen para el inicio de sesión, independientemente del intervalo de tiempo.

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.

Se puede establecer un tiempo de espera agotado para que un usuario que utiliza 2FA se autentique de forma periódica, independientemente del cambio de IP. El usuario puede establecer el rango de tiempo de espera.

NOTA:

- Para obtener un código de seis dígitos, es obligatorio configurar la opción “Dirección personalizada del remitente” y tener una configuración de SMTP válida.
- El código 2FA vence después del tiempo configurado 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 a través de cualquier interfaz de usuario con credenciales de usuario predeterminadas.
- Iniciar sesión en la iDRAC mediante la aplicación OMM a través de Quick Sync-2

NOTA: RACADM, Redfish, IPMI LAN, Serie, la CLI de una dirección IP de origen solo funcionan después de iniciar sesión correctamente desde interfaces compatibles, como la GUI de la 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 característica 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, vaya a la sección **Configuración** > **Ajustes del sistema** > **RSA SecurID** > **Autenticación de la API**, que generalmente se muestra como `l98cv5x195fdi86u43jw0q069byt0x37umlfwxc2gnp4s0xk11ve2lffum4s8302`. 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 **Active Service de Microsoft** 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 RSA AM desafía al usuario a que proporcione el “siguiente token”. Esto puede suceder aunque el usuario haya introducido 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 RSA AM desafiará al usuario a que proporcione el “siguiente token”. Este desafío ocurre aunque el usuario haya introducido el código de acceso correcto después. 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 realizar una tarea o activar un evento, puede utilizar RACADM para comprobar si el sistema se encuentra en un estado adecuado. Para ver el estado del servicio remoto desde RACADM, utilice el comando `getremoteservicesstatus`.

NOTA: El estado en tiempo real se muestra como **No aplicable** si no hay controladoras compatibles en tiempo real presentes en el sistema.

Tabla 8. Valores posibles para el estado del sistema

Sistemas de host	Lifecycle Controller (LC)	Estado en tiempo real	Estado general
• Apagados • En POST • Fuera de POST • Recopilación de inventario del sistema • Ejecución automatizada de tareas • Unified Server Configurator de Lifecycle Controller • El servidor se detuvo en el indicador de error F1/F2 debido a un error de POST • El servidor se detuvo en el indicador de F1/F2/F11 porque no hay dispositivos de arranque disponibles • El servidor ingresó al menú de configuración F2 • El servidor ingresó al menú del administrador de arranque F11	• Preparación • No inicializado • Volviendo a cargar datos • Deshabilitado • En recuperación • In Use	• Preparación • No preparado • No se aplica	• Preparación • No preparado

1. Lectura/escritura: solo lectura
2. Privilegio de usuario: usuario de inicio de sesión
3. Licencia requerida: iDRAC Core 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 ingresar una contraseña. También puede enviar un solo comando RACADM como argumento de línea de comandos a la aplicación SSH. Las opciones de la línea de comandos se comportan como RACADM remoto, ya que la sesión finaliza después de que se completa el comando.

Por ejemplo:

Inicio de sesión:

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

o

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

en el que `IP_address` es la dirección IP del iDRAC.

Envío de comandos de 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 9. Varias sesiones de iDRAC

Interfaz	Número de sesiones
Interfaz web del iDRAC	8
RACADM remoto	4
Firmware RACADM	SSH - 4, Serial - 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 Página Soporte de Dell.

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 local de la contraseña predeterminada de iDRAC

Si tiene acceso físico al sistema, puede restablecer la contraseña de la siguiente manera:

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

Restablecimiento remoto de la contraseña predeterminada de iDRAC

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

Cambio de la contraseña de inicio de sesión predeterminada

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

- Inicia sesión en iDRAC con privilegios de 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.

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

Cuando inicia sesión en la interfaz web de la iDRAC, si aparece la página **Advertencia de contraseña predeterminada**, puede cambiar la contraseña. Para hacerlo, realice estos pasos:

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

   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.

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

   Se configura la contraseña nueva y queda conectado a iDRAC.

   NOTA: **Continuar** está habilitada solo si las contraseñas ingresadas coinciden en los campos **Contraseña nueva** y **Confirmar contraseña**.

   Para obtener información acerca de los 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 de 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 RACADM de Integrated Dell Remote Access Controller.

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.

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

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

1. En la utilidad de configuración de iDRAC, vaya a **Configuración de usuario**.
   Se muestra la página **Configuración de usuario de Ajustes de iDRAC**.

2. En el campo **Cambiar contraseña**, ingrese la contraseña nueva.

   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.

3. Haga clic en **Back** (Atrás), haga clic en **Finish** (Terminar), y posteriormente, haga clic en **Yes** (Sí).
   Los detalles se guardan.

Activación o desactivación del mensaje de advertencia de contraseña predeterminada

Puede habilitar o deshabilitar la visualización del mensaje de advertencia de contraseña por defecto. Para ello, debe tener el privilegio de Configurar usuarios.

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 iDRAC10 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 10. Propiedades de restricción de reintentos de inicio de sesión

Property	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.

Tabla 10. Propiedades de restricción de reintentos de inicio de sesión (continuación)

Property	Definición
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 la iDRAC** > **Conectividad** > **Red** > **Paso del sistema operativo a la 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 del host se establece mediante la LOM o OCP.
   - **NIC de USB**: el vínculo de paso del sistema operativo al iDRAC entre el iDRAC y el sistema operativo del host se establece mediante el bus USB interno.

   NOTA: Si establece el modo de paso en LOM, asegúrese de lo siguiente:
   - El sistema operativo y la iDRAC se encuentran en la misma subred.
   - La selección de NIC en la Configuración de red está establecida en 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 funciona solamente en el modo LOM compartido con etiquetado de VLAN configurado en el host.

   NOTA:
   - Cuando el modo de paso está establecido en LOM, no es posible iniciar iDRAC desde el sistema operativo del host después de un arranque en frío.
   - El paso de LOM se elimina mediante la función de 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 de NIC de USB en el panel frontal cuando se utiliza un cable USB tipo C.

   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 "::"

   NOTA: Cuando modifica la dirección IP estática de la NIC de USB, se ajusta automáticamente el rango de direcciones DHCP para que se alinee con la nueva IP estática. Por ejemplo, si configura la IP estática en 169.254.1.1, la dirección DHCP se actualiza a 169.254.1.2. Este cambio es compatible con el administrador de red, Wicked, que acepta la nueva dirección DHCP.
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

Use el siguiente comando:

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

n=0: deshabilitado

n=1: habilitado

3

Open Server Manager 3.0.x

Puede actualizar a Open Server Manager (OSM) 3.0.x desde la iDRAC10.

Temas:

Preparación del sistema para una actualización de OSM

Asegúrese de que se cumplan los requisitos previos y de que el sistema esté preparado para una actualización de OSM.

- Compruebe si OSM es compatible con la plataforma de destino.
- La licencia de OSM está disponible.
- El DUP de OSM está disponible.

1. Asegúrese de que el firmware más reciente de la iDRAC, FPGA y BIOS se esté ejecutando en su sistema.
2. Cargue la licencia de OSM adquirida de Dell.
3. Asegúrese de que OSM esté disponible en el Inventario de firmware de Redfish URI (**redfish/v1/UpdateService/FirmwareInventory**) y en la interfaz de usuario de la iDRAC (**Sistema** > **Inventario** > **Inventario de Firmware**).

Actualización de OSM en el sistema

1. Cargue el DUP de OSM e inicie una actualización.
   El host se apaga automáticamente antes de que comience la actualización. Si el host no se apaga, utilice la interfaz disponible (IU, Redfish, IPMI) para apagar el host manualmente a fin de que la actualización pueda continuar.
2. Una vez finalizada la actualización, la iDRAC se reinicia y arranca con OSM.
3. Consulte la Guía del usuario de Dell Open Server Manager basada en OpenBMC™ más reciente para conocer los pasos para acceder a la interfaz de usuario de OSM y SSH.

4

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

NOTA: En caso de que una actualización requiera el restablecimiento/reinicio de la iDRAC, o si se reinicia la iDRAC, se recomienda verificar si la iDRAC está completamente lista; para ello, espere unos segundos hasta un máximo de cinco minutos antes de usar cualquier otro comando.

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 de configuración de iDRAC
- Lifecycle Controller (Consulte *Guía del usuario de Dell LifeCycle Controller*)

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

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 Página Soporte de Dell)

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

Para configurar la dirección IP de la iDRAC:

1. Encienda el sistema administrado.
2. Presione <F2> durante la autoprueba de encendido (POST).
3. En la página **System Setup Main Menu**, haga clic en **iDRAC Settings**.
   Se muestra la página **Configuración de iDRAC**.
4. Haga clic en **Red**.
   Aparecerá la página **Red**.
5. Especifique los siguientes ajustes:
   - Configuración de red
   - Configuración común
   - Configuración de IPv4
   - Configuración de IPv6
   - Configuración de IPMI
   - Configuración de VLAN
6. Haga clic en **Atrás**, en **Finalizar** y, a continuación, en **Sí**.
   La información de red se guarda 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 la lista **Selección de NIC**, seleccione uno de los puertos siguientes en función de los requisitos de red:
   - **Dedicado**: permite al dispositivo de acceso remoto utilizar la interfaz de red dedicada disponible en Remote Access Controller (RAC). Esta interfaz no se comparte con el sistema operativo host y dirige el tráfico de administración a una red física separada, lo que permite separarlo del tráfico de la aplicación.

     NOTA: 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.

   - **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.

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: 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.

   - **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 deshabilitada 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.

5. En **Negociación automática**, seleccione **Activado** si la 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. En **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 **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.

Ajustes comunes

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 la iDRAC:

1. Habilite **Register DRAC on DNS**.
2. Ingrese el **DNS DRAC Name**.
3. Seleccione **Configuración automática de nombre del dominio** para obtener automáticamente el nombre de dominio del DHCP. De lo contrario, proporcione el **DNS Domain Name**.

   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
   - Entre 0 y 9
   - Guion (-)

Configurar los ajustes de IPv4

Para configurar los valores de IPv4:

1. Seleccione la opción **Activado** en **Activar IPv4**.
2. Seleccione la opción **Habilitado** en **Habilitar DHCP**, de modo que DHCP pueda asignar automáticamente la dirección IP, el gateway y la máscara de subred a iDRAC. De lo contrario, seleccione **Deshabilitado** e ingrese los valores para los siguientes elementos:
   - Dirección IP estática
   - Puerta de enlace estática
   - Máscara de subred estática

   Las opciones **Usar DHCP para obtener direcciones del servidor DNS**, **Usar DHCPv6 para obtener direcciones de servidor DNS** y **Configuración automática de nombre de dominio** están habilitadas de manera predeterminada.

Configurar los ajustes de IPv6

En función de la configuración de la infraestructura, puede utilizar el protocolo de dirección IPv6.

Para configurar los valores IPv6:

NOTA: Si el IPv6 se configura como estático, asegúrese de configurar la puerta de enlace del IPv6 manualmente, que no es necesario en el IPV6 dinámico. En el IPv6 estático, no realizar la configuración manual produce una pérdida de la comunicación.

1. Seleccione la opción **Activado** en **Activar IPv6**.
2. Para que el servidor DHCPv6 asigne de forma automática la dirección IP y el largo del prefijo al iDRAC, seleccione la opción **Activado** en **Activar configuración automática**.

   NOTA: Puede configurar un IP estático y un IP de DHCP de forma simultánea.

3. En el cuadro **Dirección IP estática 1**, introduzca la dirección IPv6 estática.
4. En el cuadro **Longitud de prefijo estático**, introduzca un valor entre 1 y 128.
5. En el cuadro **Puerta de enlace estática**, introduzca la dirección de la puerta de enlace.

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

   Las opciones **Usar DHCP para obtener direcciones del servidor del DNS**, **Usar DHCPv6 para obtener direcciones de servidor del DNS** y **Configuración automática de nombre de dominio** están habilitadas de manera predeterminada.
6. Si es necesario, configure lo siguiente:
   - En el cuadro **Servidor DNS preferido estático**, introduzca la dirección IPv6 del servidor DNS.
   - En el cuadro **Servidor DNS alternativo estático**, introduzca el servidor DNS alternativo estático.
7. Cuando la información de DNS no se puede obtener mediante DHCPv6 o la configuración estática, puede usar RFC 8106 “Opciones de anuncios del enrutador IPv6 para la configuración de DNS”. Se identifica con el enrutador IPv6. El uso de la configuración de DNS de RA no afecta las configuraciones de DNS existentes (DHCPv6 o estáticas).
   - El iDRAC puede obtener información del servidor de nombres DNS y del dominio de búsqueda de DNS a partir de mensajes de anuncios del enrutador IPv6. Consulte RFC 8106 y la guía del usuario del enrutador IPv6 para obtener información sobre cómo configurar el enrutador para anunciar esta información.
   - Si la información de DNS está disponible tanto en el servidor DHCPv6 como en el anuncio del enrutador IPv6, el iDRAC utiliza ambos. En conflicto, la información del DNS del servidor DHCPv6 tiene prevalencia en los ajustes /etc/resolv.conf de la iDRAC.

   NOTA: Para que la iDRAC utilice la información del DNS de RA, IPv6. Las opciones “Habilitar” e “IPv6.Autoconfig” deben estar habilitadas. Si la configuración automática está deshabilitada, el iDRAC no procesa los mensajes de RA de IPv6 y utiliza solo los ajustes de DNS estáticos según lo configurado.

Configuración de los ajustes de IPMI

Para habilitar los ajustes de IPMI:

1. En **Habilitar IPMI a través de LAN,** seleccione **Habilitado**.
2. En **Límite de privilegios del canal**, seleccione **Administrador**, **Operador** o **Usuario**.
3. En el cuadro **Clave de cifrado**, ingrese la clave de cifrado en el formato de 0 a 40 caracteres hexadecimales (sin caracteres en blanco). El valor predeterminado es ceros.

Configuración de VLAN

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

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.

Control de acceso de red basado en puerto (IEEE 802.1x)

La iDRAC proporciona control de acceso de red basado en puertos (IEEE802.1x). Proporciona un mecanismo de autenticación seguro a los dispositivos que desean conectarse a una LAN.

Para esta función, se requiere la licencia iDRAC Datacenter.

Para acceder a esta característica mediante la GUI de iDRAC, vaya a **Ajustes de iDRAC** > **Conectividad** > **Red** > **Ajustes avanzados de la red** > **Seguridad 802.1x**. Puede activar o desactivar la opción mediante el menú desplegable. La característica está activada de manera predeterminada.

NOTA: El efecto de 802.1x no funciona en el modo LOM compartida con VLAN activada.

El control de acceso de red basado en puertos tiene tres formas de configurar los certificados de autenticación:

- **IDevID predeterminado**: este es el certificado de iDRAC predeterminado instalado de fábrica.
- **LDevID de firma personalizado**: con esta opción, puede definir una solicitud de firma de certificado (CSR) firmada por el certificado de firma de LDEVID cargado.
- **LDevID personalizado**: con esta opción, puede cargar un certificado personalizado de su elección.

Existe la opción para habilitar o deshabilitar el **certificado del servidor de autenticación** a fin de proporcionar la información necesaria para validar el certificado. Esta opción está deshabilitada de manera predeterminada.

NOTA:

- Esta característica está deshabilitada de manera predeterminada en los servidores modulares.
- Cualquier cambio en la configuración de 802.1x, incluidas las cargas de certificados y la habilitación/deshabilitación de ajustes, se aplica en el próximo arranque de iDRAC.
- El cambio de la red de iDRAC entre el switch habilitado para 802.1x y el switch no habilitado para 802.1x requiere que se reinicie iDRAC.
- Si los puertos del switch Ethernet que están conectados a los puertos LOM del servidor están habilitados para la seguridad 802.1x, entonces todos los dispositivos descendentes en esos puertos deben estar habilitados para la seguridad 802.1x. Esto significa que el host se ve afectado si no se ha habilitado para la seguridad 802.1X.

Autodiscovery

La característica de descubrimiento automático 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.

El descubrimiento automático funciona con una dirección IP estática. La característica de descubrimiento automático 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, dirección IP, número de puerto de Redfish, 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 descubrimiento automático, se omite el descubrimiento, por lo que no se necesita DHCP ni DNS.

El descubrimiento automático se puede habilitar de las siguientes maneras:

1. Mediante la UI de iDRAC: **Configuración de iDRAC** > **Conectividad** > **Detección automática de iDRAC**
2. Utilizando RACADM: `racadm set iDRAC.AutoDiscovery.EnableIPChangeAnnounce 1`

Para habilitar el descubrimiento automático a través de la utilidad Configuración de iDRAC:

1. Encienda el sistema administrado.
2. Durante la POST, presione F2 y vaya a **Configuración de iDRAC** > **Activación remota**.
   Se muestra la página **Activación remota de la configuración de iDRAC**.
3. Habilite el descubrimiento automático, ingrese 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**.
   Se muestra la página **Red de configuración de iDRAC**.
5. Active NIC.
6. Active IPv4.

   NOTA: No se soporta IPv6 para el descubrimiento automático.

7. Active DHCP y obtenga el nombre de dominio, la dirección del 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 la iDRAC. 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 11. 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.

`-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.

`-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 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 (el valor predeterminado es 60 minutos).

Se admiten archivos de perfil de formato JSON. Los siguientes nombres de archivo se utilizan 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:

- 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`, los archivos `.json` también se pueden utilizar con los sistemas de 15/16 G. 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.

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 configure los atributos de los servidores Dell.
2. Coloque el archivo SCP en una ubicación compartida a la que pueda acceder el servidor DHCP y todos los servidores Dell a los que se les asigne la dirección IP desde el servidor DHCP.
3. Especifique la ubicación del archivo SCP en el campo opción de proveedor 43 del servidor DHCP.
4. Durante la adquisición de la dirección IP, iDRAC anuncia el identificador de clase de proveedor. (Opción 60)
5. El servidor DHCP hace coincidir la clase de proveedor con la opción de proveedor en el archivo `dhcpd.conf` y envía la ubicación del archivo SCP y, si se especifica, el nombre del archivo SCP al iDRAC.
6. La iDRAC procesa el archivo SCP y configura todos los atributos enumerados en el archivo.

Opciones de DHCP

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

La opción DHCP 43 se utiliza para enviar información del servidor DHCP al cliente DHCP. La opción se define como una cadena de texto. Esta cadena de texto está configurada para contener los valores del nombre de archivo 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";
```

en el que -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 remoto.

La opción DHCP 60 identifica y asocia un cliente DHCP con un proveedor específico. Cualquier servidor DHCP configurado para realizar acciones en función del ID de proveedor de un cliente debe tener configuradas las opciones 60 y 43. Con los servidores Dell PowerEdge, la iDRAC se identifica con el ID de proveedor: **iDRAC.** Por lo tanto, debe agregar una nueva “Clase de proveedor” y crear una “opción de alcance” debajo de ella para el “código 60” y, a continuación, habilitar la nueva opción de alcance 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 del servidor DHCP.
2. Busque el servidor y expanda todos los elementos debajo de él.
3. Haga clic con el botón secundario en **Opciones de alcance** y seleccione **Configurar opciones**.
   Aparece el cuadro de diálogo **Opciones del alcance**.
4. Desplácese hacia abajo y seleccione **043 Información específica del proveedor**.
5. En el campo **Entrada de datos**, haga clic en cualquier lugar del área en **ASCII** e ingrese la dirección IP del servidor que tiene la ubicación del recurso compartido, que contiene el archivo SCP.
   El valor aparece a medida que lo escribe en **ASCII**, pero también aparece en binario a la izquierda.
6. Haga clic en **Aceptar** para guardar las configuraciones.

Configuración de la opción 60 en Windows

Para configurar la opción 60 en Windows:

1. En el servidor de DHCP, vaya a **Inicio** > **Herramientas de administración** > **DHCP** para abrir la herramienta de administración del servidor de DHCP.
2. Busque el servidor y expanda los elementos debajo de él.
3. Haga clic con el botón secundario en **IPv4** y seleccione **Definir clases de proveedor**.
4. Haga clic en **Agregar**.
   Aparecerá un cuadro de diálogo con los siguientes campos:
   - **Nombre para mostrar:**
   - **Descripción:**
   - **ID: Binario: ASCII:**
5. En el campo **Nombre para mostrar:**, escriba `iDRAC.`
6. En el campo **Descripción:**, escriba `Vendor Class.`
7. Haga clic en la sección **ASCII:** y escriba `iDRAC.`
8. Haga clic en **Aceptar** y, a continuación, en **Cerrar**.
9. En la ventana DHCP, haga clic con el botón secundario en **IPv4** y seleccione **Establecer opciones predefinidas**.
10. En el menú desplegable **Clase de opción**, seleccione **iDRAC** (creado en el paso 4) y haga clic en **Agregar**.
11. En el cuadro de diálogo **Tipo de opción**, ingrese los siguientes detalles:
    - **Nombre**: `iDRAC`

- **Tipo de datos**: cadena
- **Código**: 060
- **Descripción**: identificador de clase de proveedor de Dell

12. Haga clic en **Aceptar.** para volver a la página **DHCP**.
13. Expanda todos los elementos en el nombre del servidor, haga clic con el botón secundario en **Opciones de alcance** y seleccione **Configurar opciones**.
14. Haga clic en la pestaña **Opciones avanzadas**.
15. De la lista **Clase de proveedor**, seleccione **iDRAC**.
    La opción `060 iDRAC` se muestra en la columna **Opciones disponibles**.
16. Seleccione la opción **060 iDRAC**.
17. Ingrese el valor de cadena que se debe enviar a iDRAC (junto con una dirección IP proporcionada por DHCP estándar). El valor de cadena ayudará a importar el archivo de SCP correcto.

    Para los ajustes de la opción **Entrada de DATOS, Valor de cadena**, use un parámetro de texto que tiene las siguientes opciones de letras y valores:

    - `Filename (-f)`: indica el nombre del archivo de perfil de configuración del servidor (SCP) exportado.
    - `Sharename (-n)`: indica el nombre del recurso compartido de red.
    - `ShareType (-s)`: además de la compatibilidad con el uso compartido de archivos basado en NFS y CIFS, el firmware de la iDRAC también es compatible con el acceso a archivos de perfil mediante HTTP y HTTPS. La marca `-s option` se actualiza de la siguiente manera, en `-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 de archivos compartidos.

      NOTA: `Sharename (-n)`, `ShareType (-s)` y `IPAddress (-i)` son atributos obligatorios que se deben aprobar. -n no se necesita para HTTP ni HTTPS.

    - `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. La configuración predeterminada es 300.
    - `EndHostPowerState (-e)`: indica el estado de la alimentación del host. 0 Indica APAGADO y 1 indica ENCENDIDO. La configuración predeterminada es 1.

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

NFS: -f system_config.xml -i 192.168.1.101 -n /nfs_share -s 0 -d 1
CIFS: -f system_config.xml -i 192.168.1.101 -n cifs_share -s 2 -u <**USERNAME**> -p <**PASSWORD**> -d 1 -t 400
HTTP: -f system_config.json -i 192.168.1.101 -s 5
HTTP: -f http_share/system_config.xml -i 192.168.1.101 -s http
HTTP: --f system_config.xml -i 192.168.1.101 -s http -n http_share
HTTPS: -f system_config.json -i 192.168.1.101 -s https

Configuración de la opción 43 y la opción 60 en Linux

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

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

```
option myname code 43 = text;
subnet 192.168.0.0 netmask 255.255.0.0  {
#default gateway
    option routers            192.168.0.1;
    option subnet-mask        255.255.255.0;
    option nis-domain        "domain.org";
    option domain-name        "domain.org";
    option domain-name-servers    192.168.1.1;
```

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

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

- 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 nomenclatura de archivo, consulte Configuración de servidores y componentes del servidor mediante la configuración automática .

- Sharename (-n): indica el nombre del recurso compartido de red.
- ShareType (-s): Indica el tipo de recurso compartido. 0 indica NFS, 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`

    NOTA: 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 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. La configuración predeterminada es 300.
- EndHostPowerState (-e): Indica el estado de la alimentación del host. 0 Indica APAGADO y 1 indica ENCENDIDO. La configuración predeterminada 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.

Requisitos antes de habilitar la configuración automática

Antes de habilitar la característica de configuración automática, asegúrese de que ya estén configuradas las siguientes opciones:

- El recurso compartido de red soportado (NFS, CIFS, HTTP y HTTPS) está disponible en la misma subred que el servidor de iDRAC y DHCP. Pruebe el recurso compartido de red para asegurarse de que se puede acceder a él y de que el firewall y los permisos de usuario están configurados correctamente.
- El perfil de configuración del servidor se exporta al recurso compartido de red. Además, asegúrese de que se hayan completado los cambios necesarios en el archivo SCP, de modo que se puedan aplicar los ajustes adecuados cuando se inicie el proceso de configuración automática.
- Se establece el servidor DHCP y se actualiza según sea necesario para que iDRAC llame al servidor e inicie la característica Configuración automática.

Habilitación de la configuración automática mediante la interfaz web de iDRAC

Asegúrese de que las opciones DHCPv4 y Habilitar IPv4 estén habilitadas y que la detección automática esté deshabilitada.

Para habilitar la configuración automática:

1. En la interfaz web de la iDRAC, vaya a **Ajustes de la iDRAC** > **Conectividad** > **Red** > **Configuración automática**. Aparecerá la página **Red**.
2. En la sección **Configuración automática**, seleccione una de las siguientes opciones en el menú desplegable **Habilitar aprovisionamiento DHCP**:
   - **Habilitar una vez**: configura el componente solo una vez mediante el archivo SCP al que hace referencia el servidor DHCP. Después de esto, se deshabilita la configuración automática.
   - **Habilitar una vez después del restablecimiento**: después de restablecer iDRAC, configura los componentes solo una vez mediante el archivo SCP al que hace referencia el servidor DHCP. Después de esto, se deshabilita la configuración automática.
   - **Deshabilitar**: deshabilita la característica de configuración automática.
3. Haga clic en **Aplicar** para aplicar la configuración.
   La página de 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 RACADM de Integrated Dell Remote Access Controller.

Para obtener más información sobre la característica de configuración automática, consulte la documentación técnica **Aprovisionamiento sin intervención de servidores de bajo nivel mediante Dell iDRAC con la función de configuración automática de Lifecycle Controller** disponible en Página Soporte de Dell.

Cómo usar contraseñas de algoritmos hash para obtener una mayor seguridad

Puede configurar contraseñas de usuario y contraseñas del BIOS mediante un formato hash unidireccional. El mecanismo de autentificación 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. 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 ni Redfish para la configuración de contraseñas de algoritmo hash o el reemplazo para la iDRAC. Puede utilizar el SCP para la configuración de contraseñas de algoritmo hash o el reemplazo en la RACADM remota 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 de usuario de la iDRAC, muestran 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 hash en el perfil de configuración del servidor

Las nuevas contraseñas de hash se pueden exportar de manera opcional en el perfil de configuración del servidor.

Cuando se importa el perfil de configuración del servidor, puede quitar la marca de comentario del atributo de contraseña existente o de los nuevos atributos de hash de contraseña. Si ambos están sin comentarios, se genera un error y la contraseña no se establece. Un atributo comentado no se aplica durante una importación.

Generación de contraseña hash sin autenticación SNMPv3 e IPMI

La contraseña de hash se puede generar sin autenticación SNMPv3 e IPMI con o sin salt. Ambos necesitan SHA256.

Para generar una contraseña hash con salt:

1. En el caso de las cuentas de usuario de iDRAC, debe usar salt en la contraseña mediante SHA256.
   - Cuando se agrega salt a la contraseña, se agrega una cadena binaria de 16 bytes. Salt debe tener una longitud de 16 bytes, si se proporciona. Una vez anexada, 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 los siguientes comandos:

```
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 de hash y salt en el perfil de configuración del servidor importado usando los comandos de RACADM o Redfish.

   NOTA: Si desea borrar una contraseña previamente con salt, asegúrese de que contraseña-salt esté configurado explícitamente en una cadena vacía.

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

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

4. Después de establecer la contraseña, funciona la autenticación normal de contraseña de texto sin formato, excepto que la autenticación SNMP v3 e IPMI falla para las cuentas de usuario de la iDRAC cuyas contraseñas se actualizaron con hash.

Modificación de los ajustes de la cuenta de administrador local

Después de establecer la dirección IP de iDRAC, puede modificar los ajustes de la cuenta de administrador local (es decir, el usuario 2) mediante la utilidad de configuración de iDRAC.

1. En la utilidad de configuración de iDRAC, vaya a **Configuración de usuario**.
   Se muestra la página **Configuración de usuario de Ajustes de la iDRAC**.
2. Especifique los detalles de **Nombre de usuario**, **Privilegio de usuario de LAN**, **Privilegio de usuario de puerto serial** y **Cambiar contraseña**.

   Para obtener información acerca de las opciones, consulte la **Ayuda en línea de la utilidad de configuración de iDRAC**.
3. Haga clic en **Back** (Atrás), haga clic en **Finish** (Terminar), y posteriormente, haga clic en **Yes** (Sí).
   Se configuran los ajustes de la cuenta de administrador local.

Configuración de la ubicación de un sistema administrado

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 del sistema administrado mediante la interfaz web

Para especificar los detalles de la ubicación del sistema:

1. En la interfaz web de iDRAC, vaya a **Sistema** > **Detalles** > **Detalles del sistema**.
   Se muestra la página **Detalles del sistema**.
2. En **Ubicación del sistema**, ingrese 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 iDRAC**.
3. Haga clic en **Aplicar**. Los detalles de la ubicación del sistema se guardan en iDRAC.

Configuración de la ubicación del sistema administrado 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 RACADM de Integrated Dell Remote Access Controller.

Configuración de la ubicación del sistema administrado mediante la utilidad de configuración de iDRAC

Para especificar los detalles de la ubicación del sistema:

1. En la utilidad de configuración de iDRAC, vaya a **Ubicación del sistema**.
   Se muestra la página **Ubicación del sistema Ajustes de iDRAC**.
2. Ingrese los detalles de 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 **Back** (Atrás), haga clic en **Finish** (Terminar), y posteriormente, haga clic en **Yes** (Sí).
   Los detalles se guardan.

Optimización del rendimiento y el consumo de energía 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.

Mediante la interfaz web de iDRAC, RACADM o la utilidad de configuración de iDRAC, puede cambiar los siguientes ajustes térmicos:

- Optimizar para el rendimiento
- Optimizar para un consumo de energía mínimo
- Establecer la temperatura máxima de salida de aire
- Aumentar el flujo de aire a través de una compensación del 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 los ajustes térmicos mediante la interfaz web de iDRAC

Para modificar los ajustes térmicos, realice lo siguiente:

1. En la interfaz web de iDRAC, vaya a **Configuración** > **Configuración del sistema** > **Configuración de hardware** > **Configuración de enfriamiento**.
2. Especifique los siguientes elementos:
   - **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 del 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.

  NOTA: La velocidad del ventilador no cambia incluso cuando se selecciona “Máximo rendimiento” para algunas configuraciones específicas.

- **Alimentación mínima (Rendimiento por vatio optimizado)**:
  - Optimizado para reducir al máximo 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 del 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.

  NOTA: 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 hace funcionar a todos los ventiladores a su velocidad máxima.

  NOTA:
  - 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.

- **Umbrales**
  - **Límite máximo de temperatura de entrada PCIe**: el valor predeterminado es de 55 °C. Seleccione la temperatura más baja de 45 °C para las tarjetas PCIe de otros fabricantes que requieran una temperatura de entrada más baja.
  - **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**: establece la velocidad mínima del ventilador en un valor predeterminado según lo que determine el algoritmo de enfriamiento del sistema.
    - **Personalizado**: ingrese el porcentaje que desee cambiar respecto de la velocidad del ventilador. El rango es entre 9 y 100.

    NOTA:
    - 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 %).
    - Para todas las configuraciones de almacenamiento SAS/SATA, la velocidad del ventilador se limita al 95 %.
    - 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.
    - El 0 % de PWM no indica que el ventilador está apagado. Es la velocidad más baja que puede alcanzar el ventilador.
    - En servidores con múltiples zonas, una falla del ventilador en cualquiera de las zonas, como el módulo de procesador de host (HPM) y la placa base PCIe (PCB), provoca que todos los ventiladores funcionen a una velocidad máxima.

  Los ajustes son persistentes, lo que significa que una vez que se establezcan y apliquen, no cambian automáticamente a los ajustes predeterminados durante el reinicio del sistema, el ciclo de encendido, el uso de iDRAC o las actualizaciones del BIOS. Es posible que las opciones personalizadas de refrigeración no sean compatibles con todos los servidores. Si las opciones no son soportadas, estas no se muestran, o bien no puede 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: La activación del ventilador depende de la configuración térmica pertinente (bucle abierto) que se activará, lo que depende nuevamente de las configuraciones de hardware respectivas presentes en la configuración. Por ejemplo, las unidades de HDD posteriores requeridas.

NOTA: Debe reiniciar el sistema para que los ajustes se implementen.

Modificación de la configuración térmica mediante RACADM

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

Tabla 12. Ajustes térmicos

Objetos	Descripción	Uso	Ejemplo

`AirExhaustTemp`	Permite establecer el límite máximo de temperatura de salida de aire.	Establezca cualquiera 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`
			• La salida es:
			`AirExhaustTemp=70`
			• Esta salida indica que el sistema está configurado para limitar la temperatura de salida del aire a 70 °C. Para establecer el límite de temperatura de salida a 60 °C:
			`racadm set system.thermalsettings.AirExhaustTemp 4`
			• La salida es:
			`Object value modified successfully.`
			• Si un sistema no soporta un límite de temperatura de salida de aire específico, cuando ejecute el siguiente comando:
			`racadm set system.thermalsettings.AirExhaustTemp 0`
			• Se muestra el siguiente mensaje de error:
			`ERROR: RAC947: Invalid object value specified.`
			• Asegúrese de especificar el valor en función del tipo de objeto. Para obtener más información, consulte la Ayuda de RACADM. Para establecer el límite en el valor predeterminado:
			`racadm set system.thermalsettings.AirExhaustTemp 255`

`FanSpeedHighOffsetVal`	• Al obtener esta variable, se obtiene una lectura del valor de desplazamiento de la velocidad del ventilador en %PWM para la configuración de desplazamiento de alta velocidad del ventilador. • Este valor depende del sistema. • Use el objeto `FanSpeedOffset` para establecer este valor	Valores de 0 a 100	`racadm get system.thermalsettings FanSpeedHighOffsetVal` Se devuelve un valor numérico, por ejemplo 66. Este valor indica que cuando se utiliza el siguiente comando, se aplica un desplazamiento de la velocidad del

Tabla 12. Ajustes térmicos (continuación)

Objetos	Descripción	Uso	Ejemplo
	mediante el valor de índice 1.		ventilador de alta (66 % PWM) sobre la velocidad base del ventilador `racadm set system.thermalsettings FanSpeedOffset 1`

`FanSpeedLowOffsetVal`	• Al obtener esta variable, se obtiene una lectura del valor de desplazamiento de la velocidad del ventilador en %PWM para la configuración de desplazamiento de baja velocidad del ventilador.
	• Este valor depende del sistema.
	• Use el objeto `FanSpeedOffset` para establecer este valor mediante el valor de índice 0.
		Valores de 0 a 100	`racadm get system.thermalsettings FanSpeedLowOffsetVal`
			Esto devuelve un valor como “23”. Esto significa que cuando se utiliza el siguiente comando, se aplica un desplazamiento de velocidad del ventilador de baja (23 % PWM) sobre la velocidad base del ventilador.
			`racadm set system.thermalsettings FanSpeedOffset 0`

`FanSpeedMaxOffsetVal`	• Al obtener esta variable, se obtiene una lectura del valor de desplazamiento de la velocidad del ventilador en %PWM para la configuración de desplazamiento de velocidad máxima del ventilador.
	• Este valor depende del sistema.
	• Use `FanSpeedOffset` para establecer este valor mediante el valor de índice 3
		Valores de 0 a 100	`racadm get system.thermalsettings FanSpeedMaxOffsetVal`
			Esto devuelve un valor como “100”. Esto significa que cuando se utiliza el siguiente comando, se aplica un desplazamiento de velocidad del ventilador de máxima (es decir, velocidad total, 100 % PWM). Por lo general, esta compensación hace que la velocidad del ventilador aumente a velocidad máxima.
			`racadm set system.thermalsettings FanSpeedOffset 3`

`FanSpeedMediumOffsetVal`	• Al obtener esta variable, se obtiene una lectura del valor de desplazamiento de la velocidad del ventilador en %PWM para la configuración de desplazamiento de velocidad media del ventilador.
	• Este valor depende del sistema.
	• Use el objeto `FanSpeedOffset` para establecer este valor mediante el valor de índice 2.
		Valores de 0 a 100	`racadm get system.thermalsettings FanSpeedMediumOffsetVal`
			Esto devuelve un valor como “47”. Esto significa que cuando se utiliza el siguiente comando, se aplica un desplazamiento de la velocidad del ventilador de media (47 % PWM) sobre la velocidad base del ventilador
			`racadm set system.thermalsettings FanSpeedOffset 2`

Tabla 12. Ajustes térmicos (continuación)

Objetos	Descripción	Uso	Ejemplo

`FanSpeedOffset`	• Cuando se utiliza este objeto con el comando get, se muestra el valor existente de compensación de la velocidad del ventilador.
	• El uso de este objeto con el comando set permite configurar el valor de compensación de velocidad del ventilador necesario.
	• El valor del índice decide la compensación que se aplica y los objetos `FanSpeedHighOffsetVal`, `FanSpeedLowOffsetValFanSpeedMaxOffsetVal` y `FanSpeedMediumOffsetVal` (definidos anteriormente) son los valores a los que se aplican las compensaciones.
		Los valores son los siguientes:
		• 0: velocidad baja del ventilador
		• 1: velocidad alta del ventilador
		• 2: velocidad media del ventilador
		• 3: velocidad máxima del ventilador
		• 255: ninguno
			Para ver la configuración existente:
			`racadm get system.thermalsettings.FanSpeedOffset`
			NOTA: Para establecer el desplazamiento de la velocidad del ventilador en el valor Alto (como se define en `FanSpeedHighOffsetVal`)
			`racadm set system.thermalsettings.FanSpeedOffset 1`

`MFSMaximumLimit`	Límite máximo de lectura para MFS	Valores del 1 al 100	Para mostrar el valor más alto que se puede establecer mediante la opción `MinimumFanSpeed`: `racadm get system.thermalsettings.MFSMaximumLimit`
`MFSMinimumLimit`	Límite mínimo de lectura para MFS	Los valores entre 0 y `MFSMaximumLimitPre` determinado son 255 (significa Ninguno)	Para mostrar el valor más bajo que se puede establecer mediante la opción `MinimumFanSpeed`. `racadm get system.thermalsettings.MFSMinimumLimit`
`MinimumFanSpeed`	• Permite configurar la velocidad mínima del ventilador necesaria para que el sistema funcione. • Define el valor de base (piso) para la velocidad del ventilador y el sistema permite que los ventiladores disminuyan a este valor definido de velocidad del ventilador. • Este valor es el valor %PWM para la velocidad del ventilador.	Valores de `MFSMinimumLimit` a `MFSMaximumLimit` Cuando el comando get informa 255, significa que el desplazamiento configurado por el usuario no se aplica.	Para asegurarse de que la velocidad mínima del sistema no disminuya menos del 45 % de PWM (45 debe ser un valor entre `MFSMinimumLimit` a `MFSMaximumLimit`): `racadm set system.thermalsettings.MinimumFanSpeed 45`

Tabla 12. Ajustes térmicos (continuación)

Objetos	Descripción	Uso	Ejemplo

`ThermalProfile`	• Permite especificar el algoritmo de base térmica.
	• Permite establecer el perfil del sistema según sea necesario para el comportamiento térmico asociado al perfil.
		Valores:
		• 0: automático
		• 1: máximo rendimiento
		• 2: alimentación mínima
			Para ver la configuración del perfil térmico existente:
			`racadm get system.thermalsettings.ThermalProfile`
			NOTA: Para establecer el perfil térmico en Máximo rendimiento:
			`racadm set system.thermalsettings.ThermalProfile 1`

`ThirdPartyPCIFanResponse`	• Reemplazos térmicos para tarjetas PCI de otros fabricantes. • Permite habilitar o deshabilitar la respuesta predeterminada del ventilador del sistema para las tarjetas PCI de otros fabricantes detectadas. • Para confirmar la presencia de una tarjeta PCI de otros fabricantes, consulte el PCI3018 de ID del mensaje en el registro de Lifecycle Controller.	Valores: • 1: habilitado • 0: deshabilitado **NOTA:** El valor predeterminado es 1.	Para deshabilitar cualquier respuesta de velocidad del ventilador predeterminada configurada para una tarjeta PCI de otros fabricantes detectada: `racadm set system.thermalsettings.ThirdPartyPCIFanResponse 0`

Modificación de los ajustes térmicos mediante la utilidad de configuración de iDRAC

Para modificar los ajustes térmicos, realice lo siguiente:

1. En la utilidad de configuración de iDRAC, vaya a **Térmico**.
   Se muestra la página **Térmico de Configuración de iDRAC**.
2. Especifique los siguientes elementos:
   - Perfil térmico
   - Límite de temperatura de salida máximo
   - Desplazamiento de la velocidad del ventilador
   - Velocidad mínima del ventilador

   Los ajustes son persistentes, lo que significa que una vez que se establezcan y apliquen, no cambian automáticamente a los ajustes predeterminados durante el reinicio del sistema, el ciclo de encendido, el uso de iDRAC o las actualizaciones del BIOS. Algunos servidores Dell pueden o no soportar algunas o todas estas opciones de enfriamiento personalizadas para el usuario. Si las opciones no son soportadas, estas no se muestran, o bien no puede proporcionar un valor personalizado.
3. Haga clic en **Back** (Atrás), haga clic en **Finish** (Terminar), y posteriormente, haga clic en **Yes** (Sí).
   Se configuran los ajustes 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 para las unidades M.2 conectadas a través de tarjetas elevadoras directas o BOSS.

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 en la sección de configuración del ventilador.
2. Especifique los siguientes elementos:
   - **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: Reinicie el sistema para aplicar la configuración.

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. 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 RACADM de Integrated Dell Remote Access Controller.
4. Instale los elementos siguientes según los requisitos:
   - Cliente SSH
   - TFTP
   - Dell OpenManage Essentials

Acceso a iDRAC de manera remota

Para acceder de manera remota a la interfaz de usuario de la iDRAC desde una estación de administración, configure la NIC de la iDRAC en **Dedicada** o **LOM1** para asegurarse de que la estación de administración esté en la misma red que la 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 Manuales de iDRAC.

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 ajustes incluyen deshabilitar bloqueadores de elementos emergentes, habilitar la compatibilidad del plug-in de eHTML5, etc.

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

NOTA: Si usa 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 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:

- Deshabilitación de la característica de lista blanca
- Configuración de Firefox para habilitar el SSO 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.

Deshabilitación de la característica de lista blanca en Firefox

Firefox tiene una función de seguridad de "lista blanca" que requiere permiso del usuario para instalar plug-ins para cada sitio distinto que aloja un plug-in. Si la función de lista blanca está habilitada, requiere que instale un visor de la consola virtual para cada iDRAC que visite, aunque las versiones del visor sean idénticas.

Para deshabilitar la característica de lista blanca y evitar instalaciones innecesarias de plug-ins, realice los siguientes pasos:

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

   Los valores de **Nombre de preferencia**, **Estado**, **Tipo** y **Valor** cambian a texto en negrita. El valor **Estado** cambia a configurado por el usuario y el **Valor** cambia a falso.
4. En la columna **Nombre de preferencias**, busque **xpinstall.enabled.**
   Asegúrese de que **Valor** sea **verdadero**. Si no es así, haga doble clic en **xpinstall.enabled** para establecer **Valor** en **verdadero**.

Configuración de Firefox para habilitar el SSO de Active Directory

Para configurar los ajustes del navegador Firefox:

1. En la barra de direcciones de Firefox, ingrese `about:config`.
2. En **Filtro**, ingrese `network.negotiate`.
3. Agregue el nombre de dominio a network.negotiate-auth.trusted-uris (mediante una lista separada por comas).
4. Agregue el nombre de dominio a network.negotiate-auth.delegation-uris (mediante una lista separada por comas).

Configuración de exploradores web para usar la consola virtual

NOTA: La consola virtual solo utiliza eHTML5. Java y ActiveX ya no son compatibles.

Para utilizar la consola virtual en la estación de administración:

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

   NOTA: En el SO RHEL con el navegador Mozilla, se observa lo siguiente durante la caída de la red (después de extraer y reinsertar el cable de red):
   - Es posible que el mensaje de reconexión no aparezca en vConsole hasta que la red esté en funcionamiento.
   - Es posible que vea el mensaje emergente **Inicio de sesión denegado**, en lugar del error **No se pudo volver a conectar**, si la red está inactiva durante más de 180 segundos.

   NOTA: Cuando se utiliza el navegador Safari, se recomienda anular la selección de la opción **NSURLSession WebSocket** si está seleccionada y, luego, abrir vConsole. Para deshabilitar **NSURLSession WebSocket** en Safari, desmarque la opción **Safari** > **Desarrollo** > **Funciones experimentales** > **Funciones experimentales**.

Para obtener más información sobre las versiones de exploradores soportadas, consulte las **Notas de la versión** disponibles en Manuales de iDRAC.

NOTA: Se recomienda deshabilitar la característica de búsqueda virtual en el navegador Edge. Está habilitada de forma predeterminada. Es posible que exista el riesgo de que se busquen imágenes sin su conocimiento. Por lo tanto, puede deshabilitar este comportamiento en la configuración de los ajustes del navegador Edge.

2. Para utilizar Microsoft Edge, seleccione la opción del navegador **Ejecutar como administrador**.
3. Configure el navegador web para usar el plug-in eHTML5.
4. Importe los certificados raíz en el sistema administrado para evitar las ventanas emergentes que solicita la verificación de los certificados.
5. Instale el paquete **compat-libstdc++-33-3.2.3-61**.

   NOTA: En Windows, el paquete relacionado `compat-libstdc++-33-3.2.3-61` puede estar incluido 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.

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.

Para obtener más información acerca de la inscripción automática de certificados (ACE), consulte Inscripción automática de certificados.

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. Haga clic en la pestaña **Seguridad** y, a continuación, 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**, busque, seleccione el certificado de CA (en formato codificado Base64) y haga clic en **Abrir**.
   El certificado seleccionado se importa al almacén de certificados de confianza del inicio web.
5. Haga clic en **Cerrar** y, a continuación, en **Aceptar**. La ventana del **Panel de control de Java** se cerrará.

Visualización de versiones localizadas de la interfaz web

La interfaz web de iDRAC soporta los siguientes idiomas:

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

Los identificadores ISO entre paréntesis denotan las variantes de idioma soportado. Para algunos idiomas soportados, es necesario cambiar el tamaño de la ventana del navegador a 1024 píxeles de ancho para ver todas las características.

La interfaz web de iDRAC está diseñada a fin de funcionar con teclados localizados para las variantes de idioma soportadas. Algunas características de la interfaz web de iDRAC, como la consola virtual, pueden necesitar pasos adicionales para acceder a ciertas funciones o letras. Otros teclados no están soportados y pueden causar problemas inesperados.

NOTA: Consulte la documentación del navegador sobre cómo configurar o establecer diferentes idiomas y ver versiones localizadas de la interfaz web de iDRAC.

Actualización del firmware de dispositivos

Puede actualizar la iDRAC, el BIOS y el firmware de todos los dispositivos, como:

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

PRECAUCIÓN: La actualización de firmware de la PSU puede tardar varios minutos en función de la configuración del sistema y el modelo de la PSU. Para evitar dañar la PSU, no interrumpa el proceso de actualización ni encienda el sistema durante una actualización de firmware de la PSU.

NOTA:

- El registro de LC puede informar mensajes de advertencia de pérdida y restauración de la comunicación durante una actualización de firmware de la GPU.
- Después de realizar una actualización del firmware de la PSU, el sistema inicia un ciclo de encendido de CA virtual.

NOTA:

- Cuando se intenta realizar una actualización de firmware en un disco conectado directamente, se espera que vea un mensaje de PR7 duplicado en los registros de Lifecycle.
- Cuando el estado del trabajo es **En ejecución** y no hay ninguna actualización de estado desde los módulos de actualización, se agota el tiempo de espera después de 6 horas y se marca como fallido.
- Si el estado del trabajo es **En ejecución**, es posible que el trabajo de actualización de firmware se marque como **Fallido** después reiniciar la iDRAC.
- No utilice IP desde el sitio downloads.dell.com mientras realiza las actualizaciones. Puede que no funcione según lo esperado. Cuando se especifica downloads.dell.com como la dirección HTTPS, no es necesario proporcionar una ruta de catálogo. El catálogo correspondiente se selecciona de forma automática.

Debe cargar el firmware requerido en iDRAC. Una vez completada la carga, se muestra la versión actual del firmware que se instala en el dispositivo y la versión que se aplicará. Si el firmware que se está cargando no es válido, se muestra un mensaje de error. Las actualizaciones que no requieren un reinicio se aplican de inmediato. Las actualizaciones que sí lo requieren se configuran y se ejecutarán en el siguiente reinicio del sistema. Solo se requiere un reinicio del sistema para realizar todas las actualizaciones.

En una situación de actualización de firmware en tiempo real desde iDRAC, si el estado del trabajo se completa con **Completado, CA virtual pendiente**, realice el ciclo de apagado y encendido de CA físico o el ciclo de apagado y encendido de CA virtual del servidor. Para realizar un ciclo de apagado y encendido de CA virtual, utilice el siguiente URI de Redfish. Si se utiliza cualquier otro método para realizar el ciclo de apagado y encendido de CA, el trabajo en tiempo real puede fallar. Sin embargo, la versión actualizada aún se refleja en el ciclo de apagado y encendido de CA.

NOTA:

- Cuando se habilita el modo iLKM en una controladora, la actualización/reversión del firmware de la iDRAC fallará cuando se intente desde un modo iLKM a una versión de la iDRAC no iLKM. La actualización/reversión del firmware de la iDRAC pasará cuando se realice dentro de las versiones iLKM.
- Cuando se habilita el modo SEKM en una controladora, la actualización/reversión del firmware de la iDRAC fallará cuando se intente desde un modo SEKM a una versión de la iDRAC no de SEKM. La actualización/reversión del firmware de la iDRAC pasará cuando se realice dentro de las versiones del SEKM.
- La degradación del firmware de PERC arrojará un error cuando SEKM esté activado.

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

Los tipos de archivo de imagen admitidos del firmware son:

- `.exe`— Dell Update Package (DUP) basado en Windows. Debe tener el privilegio de control y configuración para utilizar este tipo de archivo de imagen.
- `.d10`— Incluye el firmware de la iDRAC y de Lifecycle Controller.

Para los archivos con extensión `.exe`, debe contar con privilegio de Control del sistema. La función con licencia de actualización remota del firmware y Lifecycle Controller deben estar activados. Esto se aplica a la actualización de RACADM, la actualización simple de Redfish y la actualización de la UI de iDRAC.

Para los archivos con extensión `.d10`, debe tener el privilegio Configurar. Esto se aplica solo al método `racadm fwupdate`.

NOTA: Asegúrese de que todos los nodos del sistema estén apagados antes de actualizar el firmware de PSU.

NOTA: Después de actualizar el firmware de iDRAC, es posible que observe una diferencia en la fecha y la hora del registro de Lifecycle Controller. La hora que se muestra en el registro de LC difiere de la hora del BIOS/NTP de algunos registros durante el restablecimiento de la iDRAC.

Puede realizar actualizaciones de firmware mediante los siguientes métodos:

- La carga de un tipo de imagen admitida, de una a la vez, desde un sistema local o recurso compartido de red.
- Conexión a un sitio FTP, TFTP, HTTP o HTTPS o a un repositorio de red que contenga los DUP de Windows y un archivo de catálogo correspondiente. Puede crear repositorios personalizados con Dell Repository Manager. Para obtener más información, consulte la **Guía del usuario de Dell Repository Manager Data Center**. La iDRAC puede proporcionar un informe de diferencias entre el BIOS y el firmware instalado en el sistema y las actualizaciones disponibles en el repositorio. Todas las actualizaciones aplicables que están contenidas en el repositorio se aplican al sistema. Esta función está disponible con la licencia iDRAC Enterprise o Datacenter.

  NOTA: Las actualizaciones del firmware mediante un FTP fallan si el proxy HTTP utilizado se configura sin ninguna autenticación. Asegúrese de cambiar la configuración de proxy para permitir que el método CONNECT utilice puertos que no son SSL. Por ejemplo, mientras usa un proxy Squid, quite la línea “http_access deny CONNECT !SSL_ports” que impide el uso del método CONNECT en puertos que no son SSL.

  NOTA: HTTP/HTTPS solo es compatible con la autenticación de acceso o sin autenticación.

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

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

Tabla 13. Tipos de archivos de imagen y dependencias

	Imagen .D10		DUP de iDRAC	
Interfaz	**Soportado**	**Requiere LC activado**	**Soportado**	**Requiere LC activado**
Actualización de RACADM (nuevo)	Sí	Sí	Sí	Sí
UI de iDRAC	Sí	Sí	Sí	Sí
DUP del sistema operativo dentro de banda	No	N/D	Sí	No
NOTA: Después de realizar una actualización de DUP dentro de banda, si la actualización no se organiza en la iDRAC, se crea un trabajo de reversión de varias partes.				
Redfish	Sí	N/D	Sí	N/D
Diagnósticos	No	No	No	No
Paquete de controladores del sistema operativo	No	No	No	No
iDRAC	Sí	No	No*	Sí
BIOS	Sí	Sí	Sí	Sí

Tabla 13. Tipos de archivos de imagen y dependencias (continuación)

Imagen .D10			DUP de iDRAC	
Interfaz	**Soportado**	**Requiere LC activado**	**Soportado**	**Requiere LC activado**
Controladora RAID	Sí	Sí	Sí	Sí
BOSS	Sí	Sí	Sí	Sí
NVDIMM	No	Sí	Sí	Sí
Planos posteriores	Sí	Sí	Sí	Sí
NOTA: En el caso de los backplanes (activos) de expansión, se requiere reiniciar el sistema.				
Gabinetes	Sí	Sí	No	Sí
NIC	Sí	Sí	Sí	Sí
Unidad de fuente de alimentación	Sí	Sí	Sí	Sí
NOTA: Cuando se realiza un reinicio manual o cuando la actualización se realiza desde el SO, se requiere un reinicio en frío para iniciar la actualización de la PSU.				Sí
FPGA	No	Sí	Sí	Sí
NOTA: Después de que se completa la actualización de firmware del FPGA, la iDRAC se reinicia automáticamente. **NOTA:** La actualización del repositorio no es soportada para el FPGA mientras este se actualiza por sí solo o se apila con otras actualizaciones. **NOTA:** Cuando se realice un ciclo de CA, espere hasta que se drene la energía residual (durante aproximadamente 20 segundos) para garantizar un restablecimiento adecuado del sistema; de lo contrario, es posible que vea LCL y SEL: • SWC9016: No se puede autenticar el FPGA debido a un problema de integridad o de autenticación criptográfica fallida. • SWC9018: no se puede recuperar la operación de recuperación automática del FPGA debido a un error interno.				
Tarjetas de FC	Sí	Sí	Sí	Sí
Unidades SSD PCIe NVMe	Sí	No	Sí	No
Unidades de disco duro SAS/SATA	No	Sí	Sí	No
TPM	No	Sí	Sí	Sí
Aplicación de software y periféricos no SDL	No	No	No	No

Actualización del firmware mediante la interfaz web de iDRAC

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

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 del iDRAC y tienen un límite aproximado de 300 MB.

3. Haga clic en **Browse** (Examinar), seleccione el archivo de la imagen de firmware para los componentes necesarios y, a continuación, haga clic en **Upload** (Cargar). El firmware necesario se carga en iDRAC.
4. Una vez que se completa la carga, en la sección **Update Details**, se muestra cada archivo de firmware cargado en iDRAC y su estado.

NOTA: 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 necesitan un reinicio del sistema host, haga clic en **Instalar** (única opción disponible). Por ejemplo, el archivo de firmware de iDRAC.
   - Para las imágenes de firmware que requieren un reinicio del sistema host, haga clic en **Instalar y reiniciar** o **Instalar en el próximo reinicio**. Las actualizaciones que sí lo requieren se configuran y se ejecutarán en el siguiente reinicio del sistema. Solo se requiere un reinicio del sistema para realizar todas las actualizaciones.
   - Para cancelar la actualización del firmware, haga clic en **Cancel** (Cancelar).

NOTA: 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 puede 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. A continuación, se le redirigirá a la página de inicio de sesión.

7. Si el estado del trabajo es **Completado, CA virtual pendiente**, realice el ciclo de alimentación de CA física o el ciclo de alimentación de CA virtual del servidor.

NOTA: Utilice la URI de Redfish (Redfish/v1/Chassis/System.Embedded.1/Actions/OEM/DellOemChassis.ExtendedReset with ResetType=powercycle and FinalState=On/Off (para encender el sistema después de que se complete el VAC o dejarlo en el estado Apagado) para realizar el ciclo de encendido virtual. Si se utiliza cualquier otro método para realizar el ciclo de apagado y encendido de CA, el trabajo en tiempo real puede fallar. Sin embargo, la versión actualizada aún se refleja en el ciclo de apagado y encendido de CA.

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 Manuales de OpenManage > Repository Manager.

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.

Actualización del firmware de dispositivos mediante RACADM

Para actualizar el firmware del dispositivo mediante RACADM, utilice el subcomando `update`. Para obtener más información, consulte **CLI de RACADM de Integrated Dell Remote Access Controller** disponible en Manuales de iDRAC.

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 DUP

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

- Instale y active los controladores de IPMI y del sistema administrado.
- Habilite e inicie 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. El uso de NDT09 por sí mismo actualiza los dispositivos del grupo A y el grupo B. El uso de 8J1P7 por sí mismo actualiza los dispositivos del grupo B y el grupo C. Sin embargo, si intenta utilizar ambos DUP al mismo tiempo, puede 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 según el sistema operativo instalado y ejecútelo en el sistema administrado.
2. Ejecute 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.d10`
2. Ejecute el siguiente comando de RACADM:

   Servidor TFTP:

   - Mediante el comando `fwupdate`:

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

     path

     la ubicación en el servidor TFTP en el que `firmimg.d10` está almacenado.
   - Mediante el comando `update`:

     ```
     racadm -r <iDRAC IP address> -u <username> -p <password> update –f <filename>
     ```

   Servidor FTP:

   - Mediante el comando `fwupdate`:

     ```
     racadm -r <iDRAC IP address> -u <username> -p <password> fwupdate –f <ftpserver IP>
     <ftpserver username> <ftpserver password> -d <path>
     ```

     path

     la ubicación en el servidor FTP en el que `firmimg.d10` está almacenado.
   - Mediante el comando `update`:

     ```
     racadm -r <iDRAC IP address> -u <username> -p <password> update –f <filename>
     ```

   Para obtener más información, consulte Guía de la CLI RACADM de Integrated Dell Remote Access Controller.

Actualizaciones sin reinicio

La iDRAC admite actualizaciones sin reinicio. Esta característica permite actualizar el firmware desde iDRAC sin reiniciar el servidor host para iniciar y realizar la actualización en un entorno previo al sistema operativo. Para determinar si el DUP soporta la actualización de banda lateral, hay etiquetas que permiten identificar si el firmware del DUP soporta la actualización directa de banda lateral (PLDM, NVMe-MI, etc.) o el método de actualización de FMP de UEFI y el tipo de carga útil presente en el DUP.

Cuando iDRAC realiza un inventario de los componentes, decide si el componente en particular soporta la actualización directa de banda lateral o la actualización basada en FMP de UEFI heredada, y si requiere reiniciar el host o no.

NOTA: Es posible que algunos dispositivos, como los adaptadores de red, necesiten un ciclo de apagado y encendido para actualizar el firmware.

Dos propiedades específicas de las funcionalidades de actualización de firmware de PLDM se indican en el inventario de software: **PLDMCapabilitiesDuringUpdate** y **PLDMFDPCapabilitiesDuringUpdate**. Estos parámetros están disponibles solo para los dispositivos que soportan la actualización de firmware de PLDM.

NOTA: La característica de actualización basada en PLDM solo se soporta en plataformas con memoria de 1 GB de iDRAC.

Los módulos de actualización de iDRAC/LC manejan los métodos de reinicio o sin reinicio según el soporte. A continuación, se indican los diferentes métodos de actualización:

- Se identificó el reinicio de la actualización directa de banda lateral en el tiempo de ejecución
- Actualización directa de banda lateral sin reinicio.
- Actualización basada en SMA/SSM (basado en FMP de UEFI)
- Actualización de FPGA Redstone desde la iDRAC

- Actualización de FPGA desde iDRAC

NOTA: En el caso de las actualizaciones del repositorio, las actualizaciones de aplicaciones que no requieren el reinicio del host se deben realizar inmediatamente.

NOTA: En el caso de las actualizaciones directas (actualizaciones de FW en tiempo real) desde iDRAC, hay un LCLOG (SUP200, SUP0518, SUP516) con una descripción del dispositivo (información descriptiva de FQDD), en lugar de la descripción del producto.

NOTA: Cuando las unidades NVMe se encuentran detrás de PERC (en la parte frontal) y se conectan directamente en el backplane posterior, o viceversa, la actualización sin reinicio no funciona para las unidades de conexión directa.

NOTA: Si se realizan actualizaciones de firmware mediante la interfaz de usuario de LC para componentes de almacenamiento capaces de realizar actualizaciones sin reinicio, las actualizaciones fallan. Por lo tanto, utilice las interfaces de iDRAC para todas las actualizaciones de firmware.

Visualización y administración de actualizaciones preconfiguradas

Puede 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 la fila de espera para ejecutarse en el próximo reinicio.

NOTA: Cuando haya alguna actualización u otras tareas y trabajos en progreso, no reinicie o apague, ni realice un ciclo de encendido/apagado de CA en el host o iDRAC en ningún modo (de forma manual o con las teclas “Ctrl + Alt + Supr”, u otras a través de las interfaces de iDRAC). El sistema (host e iDRAC) siempre se debe reiniciar/apagar de forma adecuada cuando no hay tareas ni trabajos en ejecución en el iDRAC o host. Apagarlo de forma incorrecta o interrumpir una operación, puede causar resultados impredecibles, como daños en el firmware, generación de archivos principales, RSOD, YSOD, eventos de error en LCL, etc.

NOTA: En caso de que una actualización requiera el restablecimiento/reinicio de la iDRAC, o si se reinicia la iDRAC, se recomienda verificar si la iDRAC está completamente lista; para ello, espere unos segundos hasta un máximo de cinco minutos antes de usar cualquier otro comando.

Visualización y administración de actualizaciones en etapas mediante RACADM

Para ver las actualizaciones en etapas mediante RACADM, utilice el subcomando `jobqueue`. Para obtener más información, consulte Guía de la CLI RACADM de Integrated Dell Remote Access Controller.

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

Para ver la lista de trabajos programados mediante la interfaz web de la iDRAC, vaya a **Mantenimiento** > **Cola de trabajos**. La página **Cola de trabajos** muestra el estado de los trabajos en la cola de trabajos de Lifecycle Controller. Para obtener más información acerca de los campos que se muestran, consulte la **Ayuda en línea de iDRAC**.

Para eliminar los trabajos, seleccione los trabajos y haga clic en **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 en cola para ejecutarse durante el próximo reinicio. No puede eliminar trabajos que estén activos; es decir, con un estado **En ejecución** o **Descargando**.

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

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 mediante la UI de Lifecycle Controller, puede revertirlo a través de la interfaz web de iDRAC. Puede realizar la reversión del firmware para varios dispositivos con un solo reinicio del sistema.

Se recomienda mantener el firmware actualizado para asegurarse de que tiene las funciones y actualizaciones de seguridad más recientes. Revierta una actualización o instale 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.

Puede realizar la reversión del firmware para los siguientes componentes:

- Integrated Dell Remote Access Controller
- BIOS
- Tarjeta de interfaz de red (NIC)
- Unidad de fuente de alimentación (PSU)
- Controladora de almacenamiento
- Backplane
- Memoria persistente definida por software (SDPM)

NOTA: No puede realizar la reversión de firmware para Lifecycle Controller, diagnósticos, paquetes de controladores y FGPA.

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 OME-Modular
- iDRAC RACADM CLI
- UI de Lifecycle Controller
- Interfaz de programación de aplicaciones de Redfish

Reversión del firmware mediante la interfaz web de iDRAC

Para revertir el firmware del dispositivo:

1. En la interfaz web de la iDRAC, vaya a **Mantenimiento** > **Actualización del sistema** > **Reversión**.
   En la página **Reversión**, se muestran los dispositivos para los que puede revertir el firmware. Puede ver el nombre del dispositivo, los dispositivos, la versión del firmware instalado en la actualidad y la versión de reversión del firmware disponible.
2. Seleccione uno o más de los dispositivos cuya versión de firmware desea revertir.
3. Según los dispositivos seleccionados, haga clic en **Instalar y reiniciar** o en **Instalar en el próximo reinicio**. Si solo iDRAC está seleccionado, 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 trabajos**.
   Aparece la página **Fila de trabajo en espera**, donde podrá ver y administrar las actualizaciones de firmware apiladas.

   NOTA:
   - Mientras está en modo de reversión, el proceso de reversión continúa en segundo plano, incluso si sale de esta página.

   Aparece un mensaje de error en los siguientes casos:

   - No tiene privilegios de control de servidores para revertir firmware que no sea iDRAC o privilegios de configuración para revertir el firmware de iDRAC.
   - La reversión de firmware ya está en curso en otra sesión.
   - Las actualizaciones están programadas en etapas para ejecutarse, o bien ya están en ejecución.

   Si Lifecycle Controller está deshabilitado o en estado de recuperación y el usuario intenta realizar una reversión de firmware para un dispositivo que no es iDRAC, se muestra un mensaje de advertencia correspondiente junto con los pasos para habilitar Lifecycle Controller.

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 lo siguiente:

   ```
   racadm rollback <FQDD>
   ```

   Para obtener más información, consulte Guía de la CLI RACADM de Integrated Dell Remote Access Controller.

Restauración fácil

En la restauración fácil, se utiliza la memoria flash de la restauración fácil para respaldar los datos. Cuando reemplaza el módulo de control seguro (SCM) 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 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.
- Easy Restore no realiza copias de seguridad de otros datos, como imágenes de firmware o datos de tarjetas adicionales.
- El reemplazo del módulo de memoria del procesador del host (HPM) no inicia el proceso de Easy Restore.

NOTA: Durante el reemplazo de la SCM, debe elegir manualmente entre **Enfriamiento por líquido** o **Enfriamiento por aire**. La selección incorrecta de estas opciones genera problemas térmicos en la plataforma y, en esos casos, comuníquese con el soporte técnico de Dell para realizar la recuperación.

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

- Etiqueta de servicio del sistema
- Etiqueta de activo
- Datos de licencias
- Aplicación de diagnóstico UEFI
- Ajustes de configuración del sistema: BIOS, la iDRAC
- Registro de eventos del sistema (SEL)
- Módulo de ID de OEM

A continuación, se indican los detalles de duración de tiempo que se necesitan 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) puede tardar varios minutos (en ocasiones, 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 detectar y monitorear iDRAC mediante Dell Management Console o Dell OpenManage Essentials. También puede utilizar Dell Remote Access Configuration Tool (DRACT) para detectar iDRAC, actualizar el firmware y configurar Active Directory. Para obtener más información, consulte las guías del usuario.

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.

NOTA: Se requiere una licencia Enterprise o Datacenter para importar el SCP. Con la licencia Core solo puede exportar el SCP.

Puede importar y exportar desde una estación de administración local y desde un recurso compartido de red a través de CIFS, NFS, HTTP o HTTPS. Con el SCP, puede seleccionar e importar o exportar configuraciones a nivel de componente para el BIOS, la NIC y el 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 del 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 UI. El estado de los trabajos puede verse en la página Línea de espera de trabajos.

NOTA:

- Solo se aceptan el nombre de host o las direcciones IP para la dirección de destino.
- Puede buscar una ubicación específica para importar los archivos de configuración de servidor. Seleccione 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, .
- Durante la exportación, el nombre de archivo del SCP puede cambiar. Por ejemplo, con.xml to _con.xml.
- El SCP aplica la configuración completa en un solo trabajo con una 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.
- Para asegurarse de que las funciones de usuario se importen con precisión, establezca los valores **PasswordHashSaltset** y **Configurar importación** en **Verdadero** en el archivo de exportación del SCP.

El 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 del SCP.
6. Una vez finalizada la configuración y las actualizaciones, el sistema operativo host se apaga.

   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 del 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`.

Para obtener información detallada sobre la característica general junto con el flujo de trabajo de implementación, consulte Uso de perfiles de configuración de servidor para implementar sistemas operativos en servidores Dell PowerEdge.

Para obtener más información sobre el SCP, consulte Guía de referencia: perfiles de configuración del servidor.

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

Antes de importar el archivo SCP, se recomienda realizar la operación de vista previa de importación. Esta operación identifica todos los posibles problemas de formato o los ajustes de atributos no válidos sin afectar el estado del servidor.

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 o HTTPS.

   NOTA: Según el tipo de ubicación, debe ingresar la configuración de red, o la configuración de HTTP o HTTPS. Si el proxy se configuró para HTTP o 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 se configuró para HTTP o HTTPS, también se requiere la configuración de proxy.
4. Seleccione los componentes para los que debe respaldar la configuración.
5. Seleccione el **Tipo de exportación**; a continuación, se presentan las opciones:
   - **Básica**: crea una instantánea no destructiva de la configuración.
   - **Exportación de reemplazo**: reemplaza la configuración del servidor con ajustes nuevos o restaura la configuración del servidor a una base conocida.
   - **Exportación de clones**: clona la configuración de un servidor a otro servidor con hardware idéntico. Se actualizan todos los ajustes, excepto la identidad de I/O. Los ajustes de esta exportación son destructivos cuando se cargan en otro sistema.
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 se puede producir durante una transferencia entre el firmware de UEFI y el sistema operativo de UEFI (sistema operativo). 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 sistema operativo.

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.

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 sistemas operativos 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 ejecutar un archivo de imagen, asocie el archivo con una clave o valor hash en db; no lo asocie 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	Imagen EFI del certificado X.509 (solo formato DER binario) (el BIOS del sistema calculará e importará la recopilación de la imagen)	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 soportar 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.

Al configurar 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, la base de datos 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 enlace correspondiente. En cada sección, se incluyen enlaces para realizar las operaciones de Importar, Exportar, Eliminar y Restablecer. Los enlaces se habilitan según lo que corresponda, lo cual depende de la configuración en ese momento. Eliminar todo y Restablecer todo son las operaciones que tienen un 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 las 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 y Redfish. 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 Manuales de iDRAC.

Recuperación de iDRAC

La iDRAC es compatible con dos imágenes del sistema operativo para que una iDRAC de arranque esté siempre disponible. Durante un error catastrófico imprevisto, si pierde ambas rutas de arranque, el cargador de arranque de la iDRAC detecta que no hay ninguna imagen de arranque. El cargador de arranque muestra los mensajes de video de arranque temprano en el monitor conectado.

Complete los siguientes pasos para recuperar la iDRAC:

1. Formatee la unidad USB con FAT32 con el sistema operativo Windows, EXT3 o EXT4, mediante un sistema operativo Linux.
2. Copie **firmimg.d10** o DUP.exe en la ubicación de la unidad USB **/scm/images/** .
3. Inserte la unidad USB en el puerto USB posterior superior del servidor y realice el ciclo de apagado y encendido de CA en el servidor. El cargador de arranque detecta la unidad USB, lee la carga útil, reprograma la iDRAC y, a continuación, reinicia iDRAC.

5

Unidad de procesamiento de datos (DPU)

Una unidad de procesamiento de datos (DPU) es un sistema en un chip que consta de núcleos ARM, una ASIC de NIC y motores de aceleración. Una DPU es programable y potencialmente capaz de ejecutar un sistema operativo. Las DPU combinan la conectividad de red con núcleos de CPU independientes del hipervisor o sistema operativo, a fin de permitir servicios de descarga y aceleración. Las DPU se distinguen de los motores de descarga tradicionales por su flexibilidad y capacidad de programación y de alojamiento de una amplia variedad de servicios.

NOTA: Las DPU requieren una licencia iDRAC10 Enterprise o Datacenter.

El uso de DPU ofrece las siguientes ventajas:

- Aísla los servicios de infraestructura de las aplicaciones y el sistema operativo del host.
- Permite que un entorno brinde nuevos servicios independientemente del entorno de aplicación del host.
- Permite la aceleración de hardware para realizar operaciones con uso intensivo de datos a máxima velocidad.
- Libera los núcleos de CPU x86 o del servidor para activar las aplicaciones del cliente en plataformas de borde de un solo conector y de factor de forma pequeño.

Luego del arranque del sistema operativo de la DPU, se pueden inicializar funciones de PCIe adicionales. Por lo tanto, la enumeración de PCIe del BIOS (y el proceso de arranque del hipervisor/sistema operativo del host) se producirá solo después de que el sistema operativo de la DPU haya arrancado o esté listo.

iDRAC le permite establecer los ajustes del modo listo del sistema operativo de la DPU (sincronización de arranque) en cada ranura compatible con DPU. Los posibles valores son:

- **Habilitado:** la DPU participa en el proceso de mantener la enumeración de PCIe del BIOS y el arranque del hipervisor/sistema operativo del host.
- **Deshabilitado:** la DPU no participa en el proceso de mantener la enumeración de PCIe del BIOS y el arranque del hipervisor/sistema operativo del host.

Puntos que se deben tener en cuenta acerca de la DPU:

- Solo unas pocas ranuras son compatibles con la DPU. La iDRAC le permite configurar la sincronización de arranque de la DPU solo en esas ranuras.
- Los ajustes de sincronización de arranque de DPU se basan en ranuras (no se basan en identidad). Es decir, si el dispositivo DPU se traslada a una ranura diferente, este se comportará de acuerdo con la configuración de la ranura en la que se insertó recientemente.
- Los ajustes de sincronización de arranque de DPU se puede establecer incluso sin la presencia de un dispositivo DPU.
- Después de la detección, si la ranura no tiene un dispositivo DPU instalado, las configuraciones de sincronización de arranque de DPU NO son efectivas.
- Las DPU con sistema operativo listo individuales y las DPU con sistema operativo listo generales se informan en LCL.
- En una plataforma de DPU no compatible, mientras se realiza un borrado del sistema, los registros de LC de DPU muestran el mensaje SYS560 (`some of the DPU devices failed to reset`). En una plataforma de DPU compatible, si la DPU no está presente y se realiza un borrado del sistema, los registros muestran el mensaje SYS564 (`unable to perform system erase of DPU because there is no DPU available in the system`).
- Cuando las tarjetas NVIDIA BF3 están deshabilitadas desde la configuración del BIOS, el **Estado** en la página **Dispositivos de red**. (**Sistema** > **Visión general** > **Dispositivos de red** > **Resumen**) en la IU de iDRAC se muestra en verde.
- Cuando las ranuras PCIe de las tarjetas NVIDIA BF3 DPU están establecidas en **Controlador de arranque deshabilitado** en la configuración del BIOS (**Configuración del BIOS del sistema** > **Dispositivos integrados** > **Deshabilitación de ranura)**, los registros PR7 y PR8 se muestran en los registros de LC de la iDRAC.
- El inventario del hardware del dispositivo se muestra para las tarjetas NVIDIA BF3 cuando la ranura PCIe está establecida en **Unidad de arranque deshabilitada** en la configuración del BIOS.
- Cuando la tarjeta de DPU RAN Nokia está configurada en el modo de ahorro energético, se muestran los registros de LC críticos.

Las siguientes son las características de la DPU:

- Puede configurar la sincronización de arranque de la DPU para cada ranura compatible con la DPU.
- Puede configurar el valor de tiempo de espera agotado de la DPU con sistema operativo listo en minutos (de 0 a 30).
- Según la configuración del usuario, la enumeración de PCIe del BIOS y el proceso de arranque del hipervisor/sistema operativo del host se produce solo después de que en cada **DPU habilitada para la sincronización de arranque** se haya informado que el sistema operativo de la DPU está listo.

- El BIOS enumera otras funciones de PCIe expuestas por el sistema operativo de la DPU y se informan en el Inventario de hardware de iDRAC.
- En el BIOS, se muestran varios mensajes relacionados con la DPU durante la POST:
  - **Detectando unidades de procesamiento de datos...**: durante la detección de los dispositivos DPU.
  - **Detectando unidades de procesamiento de datos... Listo**: cuando se completa el descubrimiento de la DPU.
  - **Inicializando unidad de procesamiento de datos (NO reinicie el sistema)**: indica el avance en 0, 10, 20, 30, 40, 50, 60, 70, 80, 90 y 100 % del proceso de sincronización de arranque.
  - **Inicializando unidad de procesamiento de datos... Listo**: cuando el proceso de sincronización de arranque llega al 100 % y se realiza correctamente.
- Los mensajes de DPU con sistema operativo listo individuales y generales se informan en LCL.

  NOTA: La marca de la DPU con sistema operativo listo persiste en todos los reinicios del host y el mensaje de la DPU con sistema operativo listo se registra en cada reinicio del host.

- Si hay alguna tarea de LC-SSM presente, el BIOS omite la espera en la sincronización de arranque de DPU.

Inventario y monitoreo de las DPU

El inventario del sistema iDRAC proporciona la marca y el modelo de la DPU mientras monitorea el estado de los núcleos, los periféricos y el sistema operativo instalado de la DPU. `GET` se utiliza para recuperar información de inventario. Esta acción garantiza que no se instalen dispositivos no autorizados de forma maliciosa. Mediante la operación GET, puede comprobar periódicamente el estado de la DPU. Si el sistema está en buen estado, genera una respuesta de carga útil y una actualización de estado para proporcionar actualizaciones de estado.

Para detectar instalaciones maliciosas o accidentales del sistema operativo de la DPU, utilice la operación GET. Con la operación GET, puede recuperar el nombre del sistema operativo, el nombre del proveedor, la versión y el estado del sistema operativo de la DPU.

Puede ver la DPU instalada desde la UI de la iDRAC: **Sistema** > **Inventario** > **Inventario de firmware**

Redfish

Con Redfish, puede establecer una configuración de arranque único que se utiliza para arrancar la DPU con el valor configurado una vez que se reinicia. En el siguiente reinicio, el arranque de la DPU se basa en el orden de arranque configurado. Redfish también permite actualizar el firmware de la ARM-UEFI y la BMC. Para obtener más información, consulte developer.dell.com.

Consola de serie

Para acceder al control en serie mediante RACADM, inicie sesión en el SSH de la iDRAC y ejecute el comando `Racadm> console dpu`

Apagado coordinado

El proceso de apagado del sistema operativo de ESXi apaga internamente ESXi de la DPU para evitar que el archivo ESXi resulte dañado.

6

Administración de plug-ins

Los plug-ins son componentes de software que amplían la funcionalidad de iDRAC. Los plug-ins se empaquetan de forma individual en una DUP. Los plug-ins no se eliminan durante el reinicio, el restablecimiento o los ciclos de CA de la iDRAC. Para eliminar los plug-ins, se utiliza la operación de corrección de iDRAC o de borrado de LC. Puede habilitar o deshabilitar los plug-ins.

Para administrar los plug-ins desde la interfaz de usuario de iDRAC, vaya a **Ajustes de iDRAC** > **Ajustes** > **Plug-ins**.

NOTA: Debe tener privilegios de inicio de sesión, de control y de configuración para instalar, actualizar y eliminar los plug-ins. Solo puede ver los plug-ins instalados con privilegios de inicio de sesión.

Temas:

Instalar un plugin

Instale un plug-in si desea ampliar la funcionalidad de iDRAC. Algunos plug-ins vienen preinstalados en la iDRAC desde la fábrica de Dell para los servidores PowerEdge de 15G, 16G y generaciones posteriores.

Cuando se instala una tarjeta de la lista de dispositivos no estándar (No SDL), iDRAC no puede detectar un plug-in de SDK. Busque e instale manualmente el plug-in de SDK. La actualización, la degradación o la reversión del firmware de la iDRAC no afectan la funcionalidad de los plug-ins.

1. Descargue el plug-in desde Dell.com.
2. Vaya a **Ajustes de la iDRAC** > **Ajustes** > **Plug-ins**
3. Haga clic en **Agregar/Actualizar**.
4. Seleccione el **Tipo de ubicación**, haga clic en **Elegir archivo** y seleccione el archivo del plug-in.
5. Haga clic en **Cargar**.
   Si un plug-in es válido, se muestra un mensaje de ejecución exitosa después de instalar el plug-in. Si el hardware no está presente, se registra un mensaje de LC que indica que el plug-in no se inició. Si el plug-in no es válido, se mostrará un mensaje de error.

Desinstalar un plugin

1. Vaya a **Ajustes de la iDRAC** > **Ajustes** > **Plug-ins**
2. Seleccione el plug-in y haga clic en **Desinstalar**.
   Se desinstala el plug-in seleccionado.

Reinicio de un plug-in

Puede reiniciar un plug-in instalado en la iDRAC

1. Vaya a **Ajustes de la iDRAC** > **Ajustes** > **Plug-ins**
2. Haga clic en **Reiniciar**.

Habilitación o deshabilitación del plug-in

Puede habilitar o deshabilitar un plug-in.

1. Vaya a **Ajustes de la iDRAC** > **Ajustes** > **Plug-ins**
2. Seleccione el plug-in y haga clic en **Habilitar** o **Deshabilitar**.

Vista de los detalles del plug-in

Puede ver los detalles de los plug-ins instalados.

1. Vaya a **Ajustes de la iDRAC** > **Ajustes** > **Plug-ins**
2. Seleccione el plug-in y haga clic en **Detalles**.
   Se muestran los detalles del plug-in.

7

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 la iDRAC, consulte Licencias de la iDRAC.

Puede configurar iDRAC con los siguientes elementos:

- Interfaz web del iDRAC
- RACADM
- IPMITool (consulte la **Guía del usuario de Baseboard Management Controller Management Utilities**)

NOTA: Cuando haya alguna tarea o trabajo en progreso, no reinicie o apague, ni realice un ciclo de encendido/apagado de CA en el host o la iDRAC en ningún modo (de forma manual o con las teclas "Ctrl + Alt + Supr", u otras opciones que se proporcionen a través de las interfaces de la iDRAC). El sistema (host e iDRAC) siempre se debe reiniciar o apagar de forma adecuada cuando no hay tareas ni trabajos en ejecución en el iDRAC o host. Apagarlo de forma incorrecta o interrumpir una operación, puede causar resultados impredecibles, como daños en el firmware, generación de archivos principales, RSOD, YSOD, eventos de error en LCL, etc.

Para configurar iDRAC:

1. Inicio de sesión en la 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, establezca el primer dispositivo de inicio.
15. Establezca el paso del sistema operativo a iDRAC, en caso de ser necesario.

Temas:

- Configuración del primer dispositivo de inicio
- Activación o desactivación del paso del sistema operativo a iDRAC
- Obtención de certificados
- Configuración de varios iDRAC mediante RACADM
- Desactivación del acceso para modificar los valores de configuración de iDRAC en el sistema host

Visualización de la información de iDRAC

Puede ver las propiedades básicas de iDRAC.

Visualización de la información de iDRAC mediante la interfaz web

En la interfaz web de la iDRAC, vaya a **Ajustes de la iDRAC** > **Visión general** para visualizar la siguiente información relacionada con la iDRAC. Para obtener más información acerca de las propiedades, consulte la **Ayuda en línea de la iDRAC**.

Detalles de iDRAC

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

iDRAC Service Module

- Status

Vista Conexión

- Estado
- ID de conexión del conmutador
- ID de conexión del puerto del conmutador

Configuración de red actual

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

Ajuste IPv4 actual

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

Configuración IPv6 actual

- IPv6 habilitada
- 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 RACADM de Integrated Dell Remote Access Controller.

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 los ajustes de red mediante RACADM local

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

```
racadm get iDRAC.Nic
```

Para usar DHCP con el fin de obtener una dirección IP, utilice el siguiente comando para escribir el objeto `DHCPEnable` y habilitar esta característica.

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

En el siguiente ejemplo se muestra cómo se puede utilizar el comando para configurar las propiedades de 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 deshabilita incluso si DHCP está habilitado.

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.

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.

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 la iDRAC y las interfaces de línea de comandos de RACADM.

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 acerca de estos objetos, consulte la **Guía de referencia de la interfaz de línea de comandos RACADM para la iDRAC**, disponible en la página Manuales de la iDRAC.

Configuración de la selección de Conjunto de Cifrado mediante la interfaz web de la 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.
- Las herramientas y procedimientos para validar la configuración del conjunto de cifrado resultante a fin de 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.

NOTA: Sin importar la versión de TLS configurada en el iDRAC, el navegador Firefox en RHEL permite iniciar la IU de la iDRAC.

NOTA: Para obtener la lista de cifrados para un puerto específico, ejecute la herramienta nmap.

Para agregar cadenas personalizadas de cifrado:

1. En la interfaz web de la iDRAC, vaya a **Configuración de la 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 la página OpenSSL.
   - No se soporta TLS 1.3.

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.

Modo FIPS (INTERFAZ)

FIPS es un estándar de seguridad del sistema que deben usar las agencias y los contratistas del Gobierno de los Estados Unidos. La iDRAC admite la activación del modo FIPS.

iDRAC se certificará oficialmente para soportar el modo FIPS en el futuro.

Diferencia entre el modo FIPS soportado y el validado por FIPS

El software que se validó tras completar el programa de validación del módulo criptográfico se denomina validado por FIPS. Debido al tiempo que tarda en completarse la validación de FIPS, no todas las versiones de iDRAC se validan. Para obtener más información sobre el estado más reciente de la validación FIPS para iDRAC, consulte la página del Programa de validación del módulo criptográfico en el sitio web del NIST.

Deshabilitación del modo FIPS

Para deshabilitar el modo FIPS, debe restablecer el iDRAC a los valores predeterminados de fábrica.

Habilitación del modo FIPS

PRECAUCIÓN: Si habilita el Modo FIPS, se restablecerá la iDRAC a los valores predeterminados de fábrica. Si desea restaurar los ajustes, respalde el perfil de configuración del servidor (SCP) antes de habilitar el modo FIPS y restaure el SCP después de reiniciar iDRAC.

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 de 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 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 RACADM de Integrated Dell Remote Access Controller.

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.
      - Después de 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: Para un Key Management Server de KeySecure, durante la creación de una solicitud de certificado SSL, debe incluir al menos una de las direcciones IP o el nombre de DNS del servidor de administración de claves en el campo **Nombre alternativo de sujeto**. Asegúrese de que el formato de la dirección IP sea IP:xxx.xxx.xxx.xxx.

Funcionalidades de iLKM

La administración de claves locales de iDRAC (iLKM) es una solución de seguridad muy similar a la administración segura de claves empresariales (SEKM). Esta solución es ideal para los usuarios que no planean utilizar SEKM, pero que desean proteger los dispositivos mediante iDRAC. Sin embargo, los clientes pueden migrar a SEKM en cualquier momento. Para obtener más información, consulte la documentación técnica Habilitar iLKM en servidores Dell PowerEdge

.

Cuando se utiliza iLKM, iDRAC actúa como administrador de claves y genera claves de autenticación que se utilizan para asegurar los dispositivos de almacenamiento. Para utilizar iLKM como sistema de administración de claves, vaya a **Ajustes de iDRAC** > **Servicios** > **Administración de claves de iDRAC** y seleccione iLKM en el menú desplegable.

NOTA: iLKM necesita una combinación de la licencia de SEKM y la de iDRAC Enterprise, o la licencia de SEKM y la de iDRAC Datacenter.

Proporcione una frase de contraseña y un ID de clave para habilitar iLKM. Las longitudes de la frase de contraseña y el ID de clave deben tener un máximo de 255 caracteres.

NOTA:

- iLKM se puede ver y configurar a través de la IU de iDRAC, RACADM y las interfaces de Redfish.
- Es posible habilitar o deshabilitar la seguridad en la SED NVMe soportada cuando iDRAC está en el modo de seguridad iLKM.
- No es posible habilitar o deshabilitar iLKM, ni restablecer la clave de esta solución en el modo de bloqueo de sistema.
- Actualmente, iLKM solo es compatible con las SED NVMe de conexión directa que soportan el protocolo TCG Opal 2.0 y versiones posteriores.
- iLKM proporciona la opción de restablecer la clave, en la que debe proporcionar la frase de contraseña y el ID de clave para la autenticación.

Asegurar automáticamente las unidades con capacidad de seguridad

- Opción para solicitar a iDRAC que asegure de forma automática SED NVMe no conectado a PERC y SED SAS detrás de un HBA SAS habilitado para la seguridad. Las unidades se aseguran de forma automática en un reinicio del host o de conexión en caliente de la unidad.
- La opción no habilita de forma automática la seguridad en controladoras como PERC y HBA SAS.
- La opción está habilitada por defecto: se puede deshabilitar mediante el comando RACADM.
- Deshabilite la opción de seguridad automática antes de replanificar una unidad con la opción de borrado criptográfico (u opción de reversión de PSID) si iDRAC ya no necesita asegurar la unidad.

NOTA: Las unidades NVMe de conexión directa pueden ser unidades con capacidad de cifrado y unidades sin capacidad de cifrado. Los registros SEKM 044 se generan para las unidades que no soportan cifrado, ya que se verifica el estado del plug-in para ambas unidades NVMe de conexión directa durante la operación de seguridad automática.

NOTA: Las operaciones de reversión basadas en PSID solo se puede realizar en las unidades bloqueadas o externas. Las operaciones de reversión basadas en PSID no se pueden realizar en las unidades que están conectadas a la controladora PERC.

NOTA: No ejecute un ciclo de encendido en el sistema host inmediatamente después de habilitar la opción **Asegurar automáticamente las unidades con capacidad de seguridad**. Esto puede interrumpir la habilitación de seguridad en las unidades y puede ponerlas en un estado de seguridad indefinido.

Transición de iLKM a SEKM

Debe proporcionar la frase de contraseña de iLKM para autenticar la transición junto con los detalles de configuración de SEKM. Si la autenticación se realiza correctamente, SEKM se activa en el iDRAC y se elimina el ID de clave anterior de la iLKM. Para realizar la transición de iLKM a SEKM, realice lo siguiente:

1. Configure el certificado CSA.
2. Configure los ajustes del SEKM.
3. Ejecute la transición de iLKM a SEKM.

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 el 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 se deshabilita SEKM, las claves generadas por iDRAC en KMS no se utilizan y permanecen en KMS. Esta función es para permitir que la iDRAC elimine esas claves cuando el SEKM está deshabilitado. La iDRAC proporciona una nueva opción "-purgeKMSKeys" para el comando heredado existente "racadm sekm disable" que le permitirá purgar claves en KMS cuando el SEKM está deshabilitado en la 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 configuró previamente con una política de creación de claves. El atributo KeyCreationPolicy es de solo lectura y se establece en el valor "Key per iDRAC".
   - El atributo iDRAC de solo lectura 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 para SEKM**: iDRAC proporciona las siguientes dos opciones en la interfaz de usuario para regenerar la clave de la solución SEKM, ya sea iDRAC o PERC. Se recomienda regenerar la clave de iDRAC, ya que esto regenera las claves de todos los dispositivos habilitados y aptos para SEKM seguro.
   - **Regeneración de claves de la iDRAC para SEKM [Rekey on iDRAC.Embedded.1 FQDD]**: cuando se realiza `racadm sekm rekey iDRAC.Embedded.1`, todos los dispositivos habilitados y aptos para el SEKM seguro vuelven a generar una nueva clave de KMS y esta es una clave común para todos los dispositivos habilitados para el SEKM. La operación de regeneración de claves de la iDRAC también se puede realizar desde la interfaz de usuario de la iDRAC: **Configuración de la iDRAC** > **Servicios** > **Configuración del SEKM** > **Regenerar clave**. Después de realizar esta operación, el cambio en la clave se puede validar mediante la lectura de los atributos KeyIdentifierN y KeyIdentifierNMinusOne.
   - **Regeneración de claves de PERC para SEKM (Regenerar claves en controladora [por ejemplo, RAID.Slot.1-1] FQDD)**: cuando se ejecuta `racadm sekm rekey <controller FQDD>`, la controladora habilitada para SEKM correspondiente vuelve a generar la clave común de iDRAC actualmente activa que se creó a partir de KMS. La operación de regeneración de claves de la controladora de almacenamiento también se puede realizar desde la interfaz de usuario de la iDRAC: **Almacenamiento** > **Controladoras** > **<FQDD de controladora>** > **Acciones** > **Editar** > **Seguridad** > **Seguridad (cifrado)** > **Regenerar clave**.

     NOTA: Cuando se ejecuta Regenerar clave en PERC mientras las claves de iDRAC y la controladora se encuentran sincronizadas, es posible que se produzca una **falla en el trabajo de configuración**, o bien que el trabajo de configuración se realice correctamente, pero que la clave no cambie cuando se ejecute el trabajo. Puede utilizar la opción Restablecer clave de iDRAC para solucionar este problema.

5. **Regeneración de claves para SEKM solo desde Redfish**: se soportan las siguientes dos opciones de regeneración de claves de SEKM con Redfish:
   - **Regeneración de claves de iDRAC para SEKM programada**: envía una nueva solicitud de generación de claves desde iDRAC para el cambio automático de las claves de SEKM en función de un intervalo de recurrencia configurado por el usuario.
   - **Sincronización periódica de la iDRAC para el SEKM con Key Management Server (KMS)**: permite el cambio automático de las claves del SEKM en función del intervalo de recurrencia configurado en el servidor de KMS. La iDRAC sondea cualquier clave nueva generada por el servidor de KMS.

Para obtener información detallada sobre todas las características de SEKM soportadas y el flujo de trabajo de implementación, consulte la documentación técnica Habilitar OpenManage Secure Enterprise Key Manager (SEKM) en servidores Dell PowerEdge

NOTA: Cuando se habilita SEKM en PERC, se genera un registro CTL136. Sin embargo, en PERC 12, no se genera el registro CTL136 mientras se realiza la regeneración de claves. Esto se debe a que la controladora no crea una solicitud de clave, ya que las claves se proporcionan como parte del comando de regeneración de clave.

Habilitación o deshabilitación del redireccionamiento de HTTPS

Si no desea el redireccionamiento automático de HTTP a HTTPS debido a un problema de advertencia de certificado con el certificado iDRAC predeterminado o como un ajuste temporal para fines de depuración, puede configurar iDRAC de modo que se deshabilite el redireccionamiento desde el puerto http (el valor predeterminado es 80) al puerto https (el valor predeterminado es 443). Está activada de manera predeterminada. Debe cerrar sesión e iniciar sesión en iDRAC para que este ajuste surta efecto. Cuando deshabilita esta característica, se muestra un mensaje de advertencia.

Debe poseer privilegio de configuración del iDRAC para habilitar o deshabilitar el redireccionamiento de HTTPS.

Se registra un evento en el archivo de registro de Lifecycle Controller cuando esta característica está habilitada o deshabilitada.

Para deshabilitar el redireccionamiento de HTTP a HTTPS:

```
racadm set iDRAC.Webserver.HttpsRedirection Disabled
```

Para habilitar el redireccionamiento de HTTP a HTTPS:

```
racadm set iDRAC.Webserver.HttpsRedirection Enabled
```

Para ver el estado del redireccionamiento 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 SO/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 los 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 de forma simultánea. La segunda sesión 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 VNC inicia un protocolo de enlace RFB directamente y no se necesita un protocolo de enlace 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 de iDRAC

Para configurar los ajustes del servidor VNC:

1. En la interfaz web de la iDRAC, vaya a **Configuración** > **Consola virtual**.
   Aparece la página **Consola virtual**.
2. En la sección **Servidor de VNC**, habilite el servidor de VNC, especifique la contraseña y el número de puerto, y habilite o deshabilite el cifrado SSL.
   Para obtener información acerca de los campos, consulte la **Ayuda en línea de iDRAC7**.
3. Haga clic en **Aplicar**.
   El servidor de 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 RACADM de Integrated Dell Remote Access Controller.

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 soporte incorporado de cifrado SSL.

Para configurar la aplicación de túnel SSL:

1. Configure el túnel SSL para aceptar la conexión en `<localhost>:<localport number>`. Por ejemplo, 127.0.0.1:5930.
2. Configure el túnel SSL para conectarse a `<iDRAC IP address>:<VNC server port Number>`. Por ejemplo, 192.168.0.120:5901.
3. Inicie la aplicación de túnel.
   Para establecer la conexión con el servidor VNC del iDRAC en el canal de cifrado SSL, conecte el visor VNC al host local (dirección IP local de vínculo) y el número de puerto local (127.0.0.1: <número de puerto local>).

Configuración del visor VNC sin cifrado SSL

En general, todos los visores VNC compatibles con el búfer de trama remoto (RFB) se conectan al servidor VNC utilizando la dirección IP y el número de puerto de iDRAC configurados para el servidor VNC. Si la opción de cifrado SSL está deshabilitada durante la configuración de los valores del servidor VNC en iDRAC, para conectarse al visor VNC, realice lo siguiente:

En el cuadro de diálogo **Visor de VNC**, ingrese la dirección IP de iDRAC y el 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, ingrese `192.168.0.120:5901`.

Configuración de zona horaria y NTP

Es posible configurar la zona horaria en iDRAC y sincronizar la hora de iDRAC mediante Network Time Protocol (NTP) en lugar de las horas de BIOS o del sistema host. Después de actualizar la configuración del servidor NTP, cierre sesión en todas las sesiones actuales y, a continuación, inicie sesión en la iDRAC.

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

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

Cuando habilite o deshabilite la configuración del servidor NTP, cierre sesión en todas las sesiones actuales y, a continuación, inicie sesión en la iDRAC.

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

1. Vaya a **Ajustes de la iDRAC** > **Ajustes** > **Ajustes de zona horaria y NTP**.
   Se mostrará la página **Zona horaria y NTP**.
2. Para configurar la zona horaria, en la lista desplegable **Zona horaria**, seleccione la zona horaria necesaria 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 RACADM de Integrated Dell Remote Access Controller.

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 arranque o para todos los reinicios posteriores. Si configura el dispositivo para que se use en todos los arranques posteriores, permanecerá como el primer dispositivo de inicio en el orden de arranque del BIOS hasta que se cambie de nuevo en la interfaz web de iDRAC o en la secuencia de arranque 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
- Lifecycle Controller
- Administrador de inicio del BIOS
- Ruta de acceso dispositivo UEFI
- HTTP de UEFI
- Archivo de red virtual 1
- Archivo de red virtual 2

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 arranque mediante la interfaz web

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

1. Vaya a **Configuración** > **Ajustes del sistema** > **Ajustes de hardware** > **Primer dispositivo de arranque**.
   Se mostrará la ventana **Primer dispositivo de arranque**.
2. Seleccione el primer dispositivo de arranque necesario de la lista desplegable y haga clic en **Aplicar**.
   El sistema arranca desde el dispositivo seleccionado para reinicios posteriores.
3. Para iniciar desde el dispositivo seleccionado solo una vez en el próximo arranque, seleccione **Arrancar una vez**. A continuación, el sistema arranca desde el primer dispositivo de arranque 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 arranque mediante RACADM

- Para establecer el primer dispositivo de inicio, utilice el objeto `iDRAC.ServerBoot.FirstBootDevice` object.
- Para activar el inicio único de un dispositivo, utilice el objeto `iDRAC.ServerBoot.BootOnce`.

Para obtener más información acerca de estos objetos, consulte Guía de la CLI RACADM de Integrated Dell Remote Access Controller.

Configuración del primer dispositivo de arranque mediante la consola virtual

Puede seleccionar el dispositivo de arranque, 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 arranque. Boot-Once es compatible con todos los dispositivos enumerados en Configuración del primer dispositivo de arranque .

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

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

Activación o desactivación del paso del sistema operativo a iDRAC

En los servidores que tienen tarjetas Open Compute Project (OCP) o LAN incorporada en la placa base (LOM), puede activar la función de paso del sistema operativo a la 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 la guía del usuario del iDRAC Service Module disponible en la página iDRAC Service Module.

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.

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 (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 o Redfish y si se cambia la configuración de red en este archivo, debe esperar 15 segundos para activar la función de paso del sistema operativo a la 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 USB tipo C.

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.

Sistemas operativos admitidos para la NIC de USB

Para obtener una lista de los sistemas operativos soportados para la NIC USB, consulte la nota de la versión correspondiente en Versiones y notas de la versión de iDRAC.

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:

- Si deshabilita la NIC USB en iDRAC mientras iSM se ejecuta en el SO, el estado del módulo de servicio de iSM cambiará a En ejecución (funcionalidad limitada).
- Si instala iSM en el SO mientras la NIC USB está deshabilitada en iDRAC, iSM activará automáticamente la NIC USB en iDRAC para finalizar la instalación. Si es necesario, deshabilite la NIC USB después de completar la instalación.

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 habilitar la NIC USB, debe instalar el archivo VIB.

Para instalar el archivo VIB:

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

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

La salida 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. En el símbolo del sistema de ESXi, ejecute el comando: `esxcfg-vmknic -l`.
   La salida muestra la entrada usb0.

Habilitación o deshabilitación del paso del sistema operativo a iDRAC mediante RACADM

Para habilitar o deshabilitar el paso del sistema operativo al iDRAC mediante RACADM, utilice los objetos del grupo `iDRAC.OS-BMC`.

Para obtener más información, consulte el Registro de atributos de Integrated Dell Remote Access Controller disponible en la página Manuales de iDRAC.

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 USB tipo C.

   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 **Back** (Atrás), haga clic en **Finish** (Terminar), y posteriormente, haga clic en **Yes** (Sí).
   Los detalles se guardan.

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 la iDRAC** > **Conectividad** > **Red** > **Paso del sistema operativo a la 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 del host se establece mediante la LOM o OCP.
   - **NIC de USB**: el vínculo de paso del sistema operativo al iDRAC entre el iDRAC y el sistema operativo del host se establece mediante el bus USB interno.

   NOTA: Si establece el modo de paso en LOM, asegúrese de lo siguiente:
   - El sistema operativo y la iDRAC se encuentran en la misma subred.
   - La selección de NIC en la Configuración de red está establecida en 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 funciona solamente en el modo LOM compartido con etiquetado de VLAN configurado en el host.

   NOTA:
   - Cuando el modo de paso está establecido en LOM, no es posible iniciar iDRAC desde el sistema operativo del host después de un arranque en frío.
   - El paso de LOM se elimina mediante la función de 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 de NIC de USB en el panel frontal cuando se utiliza un cable USB tipo C.

   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 "::"

   NOTA: Cuando modifica la dirección IP estática de la NIC de USB, se ajusta automáticamente el rango de direcciones DHCP para que se alinee con la nueva IP estática. Por ejemplo, si configura la IP estática en 169.254.1.1, la dirección DHCP se actualiza a 169.254.1.2. Este cambio es compatible con el administrador de red, Wicked, que acepta la nueva dirección DHCP.
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.

Obtención de certificados

En la siguiente tabla, se enumeran los tipos de certificados según el tipo de inicio de sesión.

Tabla 15. Tipos de certificado según el tipo de inicio de sesión

Tipo de inicio de sesión	Tipo de certificado	Cómo obtenerlo
Single Sign On mediante Active Directory	Certificado de CA de confianza	Genere una CSR y haga que se firme desde una autoridad de certificación. **NOTA:** Los certificados SHA-2 también están soportados.

Tabla 15. Tipos de certificado según el tipo de inicio de sesión (continuación)

Tipo de inicio de sesión	Tipo de certificado	Cómo obtenerlo
Inicio de sesión mediante tarjeta inteligente como usuario local o de Active Directory	• Certificado de usuario • Certificado de CA de confianza	• Certificado de usuario: exporte el certificado de usuario de la tarjeta inteligente como un archivo codificado en Base64 mediante el software de administración de tarjetas proporcionado por el proveedor de la tarjeta inteligente. • Certificado de CA de confianza: este certificado lo emite una CA. **NOTA:** Los certificados SHA-2 también están soportados.
Inicio de sesión de usuario de Active Directory	Certificado de CA de confianza	Este certificado lo emite una CA de confianza. **NOTA:** Los certificados SHA-2 también están soportados.
Inicio de sesión de usuario local	Certificado SSL	Genere una CSR y haga que se firme desde una CA de confianza **NOTA:** La iDRAC se envía con un certificado de servidor SSL autofirmado predeterminado. El servidor web de la iDRAC, los medios virtuales y la consola virtual utilizan este certificado. **NOTA:** Los certificados SHA-2 también están soportados.

Certificados de servidor SSL

La CMC incluye un servidor web configurado para usar el protocolo de seguridad SSL estándar del sector para transferir datos cifrados en la red. Una opción de cifrado SSL se proporciona para deshabilitar los cifrados débiles. Basado en la tecnología de cifrado asimétrico, SSL se acepta ampliamente para el suministro de comunicaciones autenticadas y cifradas entre los clientes y servidores para impedir los espías en una red.

Un sistema habilitado para SSL puede realizar las siguientes tareas:

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

NOTA: Si el cifrado SSL se configura en 256 bits o más, y 168 bits o más, es posible que los ajustes de criptografía para el entorno de máquinas virtuales (JVM, IcedTea) necesiten la instalación de Unlimited Strength Java Cryptography Extension Policy Files para permitir el uso de los plug-in de la iDRAC, como vConsole, con este nivel de cifrado. Para obtener información sobre cómo instalar los archivos de políticas, consulte la documentación de Java.

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

Para cargar el certificado de CA desde la interfaz de usuario de iDRAC, vaya a **Ajustes de iDRAC** > **Servicios** > **Servidor web** > **Solicitud de firma de certificado SSL/TLS**. También puede ver los detalles del certificado en otras interfaces.

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 pueden acceder a la 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 son de confianza. Si un certificado de firma personalizado se carga cuando un certificado SSL personalizado ya se encuentra en uso, el certificado SSL personalizado se deshabilita y se utiliza un certificado SSL por única vez, generado automáticamente y firmado con el certificado de firma personalizado. Es posible descargar el certificado de firma personalizado (sin la clave privada). Además, se puede eliminar un certificado de firma personalizado existente. Después de eliminar el certificado de firma personalizado, la iDRAC se restablece y genera automáticamente un nuevo certificado SSL autofirmado. Si se vuelve a generar un certificado autofirmado, se debe volver a establecer la confianza entre la iDRAC y la estación de trabajo de administración. Los certificados SSL generados automáticamente son autofirmados y tienen una fecha de caducidad de siete años y un día, y una fecha de inicio de un día en el pasado (para diferentes configuraciones de zonas horarias en estaciones de administración e iDRAC).

El certificado SSL del servidor web de la iDRAC admite los caracteres de asterisco (*) como parte del componente ubicado más a la izquierda del nombre común al generar una solicitud de firma de certificado (CSR). Por ejemplo, *.qa.com o *.empresa.qa.com. Esto se denomina certificado comodín. Si se genera una CSR comodín fuera de la iDRAC, podrá contar con un solo certificado SSL comodín firmado que se puede cargar para varias iDRAC, y todas las iDRAC son de confianza para todos los navegadores compatibles. Si se conecta a la interfaz web de la iDRAC mediante un navegador compatible que admite un certificado comodín, la iDRAC es de confianza para el navegador. Mientras inicia los visores, las iDRAC son de confianza para los clientes de los visores.

Puede habilitar la función “Notificación de vencimiento del certificado” y también puede configurar el intervalo de notificación y la frecuencia de notificación. La iDRAC proporciona una notificación cerca del vencimiento del certificado.

NOTA: Los certificados autofirmados predeterminados se actualizan automáticamente en el reinicio de iDRAC. Por lo tanto, los certificados autofirmados no se consideran para el vencimiento del certificado.

Puede activar las opciones Notificación de vencimiento del certificado e Intervalo de notificación en **Ajustes de iDRAC** > **Servicios** > **Servidor web** > **Ajustes**. Además, puede ver la advertencia de seguridad en la parte inferior de la página de inicio de sesión de iDRAC acerca del vencimiento del certificado.

Generación de una nueva solicitud de firma de certificado

Una CSR es una solicitud digital que se envía a una autoridad de certificación CA para obtener un certificado de servidor SSL. Los certificados de servidor SSL permiten a los clientes del servidor confiar en la identidad del servidor y negociar una sesión cifrada con el servidor.

Una vez que la CA recibe una CSR, revisa y verifica la información que contiene. Si el solicitante cumple los estándares de seguridad de la CA, esta emite un certificado de 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.

Una vez que la CA aprueba la CSR y emite el certificado del servidor SSL, se puede cargar en iDRAC. La información utilizada para generar la CSR, almacenada en el firmware de iDRAC, debe coincidir con la información contenida en el certificado del servidor SSL, es decir, el certificado debe haberse generado utilizando la CSR creada por iDRAC.

Generación de CSR mediante RACADM

Para generar una CSR mediante RACADM, use el comando `set` con los objetos en el grupo `iDRAC.Security` y, a continuación, use el comando `sslcsrgen` para generar la CSR.

Para obtener más información, consulte Guía de la CLI RACADM de Integrated Dell Remote Access Controller.

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.

Inscripción automática de certificados

En iDRAC, la característica de inscripción automática de certificados (ACE) permite realizar la instalación y la renovación automáticas de los certificados que utiliza el servidor web. Cuando se habilita esta función, el certificado del servidor web existente se reemplaza por un nuevo certificado. Ingrese los detalles de la solicitud de firma de certificado (CSR) antes de habilitar ACE.

NOTA:
- ACE es una característica con licencia y requiere una licencia Datacenter.
- Se requiere la configuración de un servicio de inscripción de dispositivos de red (NDES) válido para emitir el certificado del servidor.

La hora de iDRAC se debe sincronizar con el NDES o la autoridad de certificación.

NOTA: Si la hora no está sincronizada, es posible que iDRAC reciba certificados no válidos o vencidos durante el proceso de inscripción y renovación.

A continuación, se indican los parámetros de configuración de ACE:

- Habilitar y deshabilitar.
- URL/ACME (entorno automatizado de administración de certificados) del servidor SCEP
- Contraseña de comprobación

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

A continuación, se presentan los estados disponibles de ACE:

- Inscrito: se habilitó ACE. El certificado se monitorea y se puede emitir un nuevo certificado tras su vencimiento.
- En proceso de inscripción: es un estado intermedio después de que se habilita ACE.
- Error: se produjo un problema con el servidor de NDES.
- Ninguno: valor predeterminado.

NOTA: Cuando se habilita ACE, se reinicia el servidor web y se cierran todas las sesiones web existentes.

NOTA: Para ver los mensajes de operación correcta o de falla, consulte los registros de Lifecycle.

Carga del certificado de servidor

Después de generar una CSR, puede cargar el certificado del servidor SSL firmado en el firmware de la iDRAC. La iDRAC se debe restablecer para aplicar el certificado. La iDRAC solo acepta certificados de servidor web X509 codificados en Base 64. Los certificados SHA-2 también están soportados.

PRECAUCIÓN: Durante el restablecimiento, iDRAC no estará disponible durante unos minutos.

Carga de un certificado de servidor mediante RACADM

Para cargar el certificado del servidor SSL, utilice el comando `sslcertupload`. Para obtener más información, consulte Guía de la CLI RACADM de Integrated Dell Remote Access Controller.

Si la CSR se genera fuera de iDRAC con una clave privada disponible, para cargar el certificado en iDRAC, realice lo siguiente:

1. Envíe la CSR a una CA raíz conocida. La CA firma la CSR y esta 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 carga en iDRAC. Aparece un mensaje en el que se le solicita que restablezca iDRAC.
4. Ejecute el comando racadm `racreset` para restablecer iDRAC.
   Se restablecerá 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 de certificado de servidor mediante interfaz web

Para cargar el certificado de servidor SSL:

1. En la interfaz web de iDRAC, vaya a **Configuración de iDRAC** > **Servicios** > **Servidor web** > **Solicitud de firma de certificado SSL/TLS**, seleccione **Cargar certificado de servidor** y haga clic en **Siguiente**.
   Aparecerá la página **Carga del certificado**.
2. En **Ruta de 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 restablecerá 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 del servidor SSL que se está utilizando actualmente en iDRAC.

Visualización del certificado de servidor mediante RACADM

Para ver el certificado del servidor SSL, utilice el comando `sslcertview`.

Para obtener más información, consulte Guía de la CLI RACADM de Integrated Dell Remote Access Controller.

Visualización de certificado de servidor mediante 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.

Carga del certificado de firma personalizado

Puede cargar un certificado de firma personalizado para firmar el certificado SSL. Los certificados SHA-2 también están soportados.

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 **Ajustes de iDRAC** > **Servicios** > **Servidor web** > **Certificado de firma personalizado SSL/TLS**.
   Aparecerá la página **SSL**.
2. En **Certificado de firma personalizado SSL/TLS**, haga clic en **Cargar certificado de firma**.
   Aparecerá la página **Cargar certificado de firma del certificado SSL personalizado**.
3. Haga clic en **Elegir archivo** y seleccione el archivo de certificado de firma del certificado SSL personalizado.
   Solo se admite el certificado que cumple con las normas de criptografía de claves públicas N.º 12 (PKCS N.º 12).
4. Si el certificado está protegido con contraseña, introduzca la contraseña en el campo **Contraseña de PKCS N.º 12**.
5. Haga clic en **Aplicar**.
   El certificado se ha cargado en iDRAC.
6. Aparecerá un mensaje emergente solicitándole que reinicie iDRAC de inmediato o más adelante. Haga clic en **Reiniciar iDRAC** o en **Reiniciar iDRAC más adelante**, según sea necesario.
   Después de que se reinicie iDRAC, se aplicará el nuevo certificado. iDRAC no estará disponible por algunos minutos durante el reinicio.
   NOTA: Debe reiniciar iDRAC para aplicar el nuevo certificado. Hasta que no se reinicie iDRAC, estará activo el certificado existente.

Carga del certificado de firma del certificado SSL personalizado mediante RACADM

Para cargar el certificado de firma del certificado SSL personalizado mediante RACADM, utilice el comando `sslcertupload` y, luego, use el comando `racreset` para restablecer iDRAC.

Para obtener más información, consulte Guía de la CLI RACADM de Integrated Dell Remote Access Controller.

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 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 RACADM de Integrated Dell Remote Access Controller.

Descarga del certificado de firma personalizado

Para descargar el certificado de firma personalizado mediante la interfaz web de iDRAC:

1. Vaya a **Ajustes de iDRAC** > **Conectividad** > **SSL**.
   Aparecerá la página **SSL**.
2. En **Certificado de firma de certificado SSL personalizado**, seleccione **Descargar certificado de firma de certificado SSL personalizado** y haga clic en **Siguiente**.
   Aparecerá un mensaje emergente que le permitirá guardar el certificado de firma personalizado en la ubicación que desee.

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 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 RACADM de Integrated Dell Remote Access Controller.

Descarga del certificado de firma personalizado

Para descargar el certificado de firma personalizado mediante la interfaz web de iDRAC:

1. Vaya a **Ajustes de iDRAC** > **Conectividad** > **SSL**.
   Aparecerá la página **SSL**.
2. En **Certificado de firma de certificado SSL personalizado**, seleccione **Descargar certificado de firma de certificado SSL personalizado** y haga clic en **Siguiente**.
   Aparecerá un mensaje emergente que le permitirá guardar el certificado de firma personalizado en la ubicación que desee.

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 única de iDRAC, como la dirección IP estática, que debe modificar antes de importar el archivo a otras 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 Página Manuales de Dell.

Para configurar varias iDRAC mediante el archivo de configuración:

1. Consulte la instancia de 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 configuración de un grupo (especificadas por el nombre y el índice del grupo) y todas las propiedades de configuración de un usuario.

2. Modifique el archivo de configuración mediante un editor de texto, si es 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 la iDRAC de objetivo, utilice el siguiente comando para modificar los ajustes:

   ```
   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 deshabilitar el acceso para modificar los ajustes de configuración de iDRAC a través de RACADM local o la utilidad de configuración de iDRAC. Sin embargo, puede ver estos ajustes de configuración. Para hacerlo, realice estos pasos:

1. En la interfaz Web de iDRAC, vaya a **Configuración de iDRAC** > **Servicios** > **Ajustes 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 el acceso está deshabilitado, no puede utilizar Server Administrator, iDRAC Service Module ni IPMITool para realizar configuraciones de iDRAC. Sin embargo, puede usar IPMI a través de LAN.

8

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.

9

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.

Temas:

Visualización de la condición y las propiedades de Managed System

Cuando inicia sesión en la interfaz web de iDRAC, la página **Resumen del sistema** le permite ver el estado del sistema administrado, la información básica de iDRAC, obtener una vista previa de la consola virtual, agregar y ver notas de trabajo e iniciar rápidamente tareas como encender o apagar, realizar un ciclo de apagado y encendido, ver registros, actualizar y revertir el firmware, encender o apagar el LED del panel frontal, y restablecer iDRAC.

Para acceder a la página **Resumen del sistema**, diríjase a **Sistema** > **Descripción general** > **Resumen**. Aparecerá 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**.

Visualización del inventario del sistema

Podrá ver información sobre los componentes de hardware y firmware instalados en el sistema administrado. Para ver el inventario del sistema en la interfaz web de iDRAC, vaya a **Sistema** > **Inventario**. Para obtener información acerca de las propiedades que se muestran, consulte **Ayuda en línea de la iDRAC**.

En la sección **Inventario de hardware**, se muestra información sobre los siguientes componentes disponibles en el sistema administrado:

- iDRAC
- OEM
- Controladora RAID
- Baterías
- CPU
- GPU
- DIMM
- HDD
- Planos posteriores
- Tarjetas de interfaz de red (integradas e incorporadas)
- Tarjeta de video
- Unidades de suministro de energía (PSU)
- Ventiladores
- HBA de Fibre Channel
- USB
- Dispositivos SSD PCIe

NOTA: En Inventario de hardware para cualquier GPU, los datos de BuildDate, GPUGUID y OEMInfo de entrada de GPU solo se soportan y completan en dispositivos NVIDIA. Los datos de OEMInfo solo se completan si el dispositivo NVIDIA proporciona algún dato para ese campo.

En la siguiente tabla, se enumeran los atributos y los valores esperados en la página **Inventario de hardware** en la interfaz de usuario de iDRAC cuando la tarjeta Pensando DPU no soporta HII.

Tabla 16. Atributos y valores esperados

Atributos	Valor esperado
CurrentMACAddress	Vacía
BusNumber	Zero
Ancho del bus de datos	Vacía
PCIDeviceID	Vacía
PCISubDeviceID	Vacía
PCISubVendorID	Vacía
PCIVendorID	Vacía
SlotLength	Vacía
Tipo de ranura	Vacía
LastSystemInventoryTime	1970-01-01T00:00:00
LastUpdateTime	1970-01-01T00:00:00
FCoEOffloadMode	Deshabilitado
iScsiOffloadMode	Deshabilitado

Tabla 16. Atributos y valores esperados (continuación)

Atributos	Valor esperado
NicMode	Deshabilitado
MaxBandwidth	0
MinBandwidth	0

NOTA: El inventario por etapas se actualiza solo después del arranque del host. Los inventarios, como las ranuras PCIe y los dispositivos PCIe en el inventario de hardware, forman parte del inventario por etapas que se genera durante el arranque del host (después de CSIOR). Incluso la conexión o extracción en caliente de las unidades no cambia los datos de inventario, a menos que se reinicie el host.

En la página **Dispositivo de red** > **Estado de la partición** de la IU, los valores de ID del dispositivo de PCI, Ancho de banda mínimo y Ancho de banda máximo están vacíos.

En la página **Dispositivo de red** > **Ajustes y funcionalidades**, el valor de Protocolos de arranque soportados está vacío.

En la sección **Inventario de firmware**, se muestra la versión de firmware de los siguientes componentes:

- BIOS
- Lifecycle Controller
- iDRAC
- Paquete de controladores del sistema operativo
- FPGA
- Controladoras PERC
- Discos físicos
- Fuente de alimentación
- NIC
- Fibre Channel
- Backplane
- Carcasa
- Unidades SSD PCIe
- TPM
- iSM

NOTA: Los componentes que carecen de funcionalidad de reversión a través de iDRAC no muestran su fecha de lanzamiento en el inventario de software. Cuando se actualiza un componente desde el sistema operativo del HOST, es posible que no se completen el contenido de reversión ni los detalles de la fecha de lanzamiento.

NOTA: Después de realizar una actualización de firmware del sistema operativo dentro de banda en un gabinete externo (JBOD), realice un reinicio en frío (ciclo de apagado y encendido) del servidor para actualizar la información del gabinete y el inventario del sistema en iDRAC.

NOTA: El inventario de firmware puede tardar mucho o no aparecer en algunos casos. Utilice el comando de radadm `getremoteservicestatus` antes de ejecutar el inventario de firmware.

NOTA:

- El inventario de software solo muestra los últimos 4 bytes de la versión del firmware y la información de la fecha de lanzamiento. Por ejemplo, si la versión del firmware es FLVDL06, el inventario de firmware muestra DL06.
- En el caso de las unidades SATA, la versión de firmware siempre se compone de cuatro caracteres. Si cualquier unidad SATA tiene una versión de firmware superior a cuatro caracteres, el inventario de software muestra los últimos cuatro caracteres de la versión de firmware y la página de almacenamiento, y el inventario de hardware muestra la versión completa.
- Cuando se revisa el inventario del software mediante la interfaz de Redfish, se muestra la información de la fecha de lanzamiento solo para los componentes que soportan la reversión.

NOTA:

- La versión del firmware del paquete de GPU se muestra como 00.00.00.00:
  - Hasta que se realiza la actualización del firmware mediante el DUP.
  - Después de que se realiza el borrado del sistema en el sistema.

- Si hay una falla de comunicación entre la placa base de la GPU e iDRAC, es posible que la versión del paquete de GPU no se muestre en el inventario de firmware. Para resolver el problema de comunicación, realice el ciclo de CA. La versión del firmware se muestra como 00.00.00.00 cuando se restaura la comunicación.
- Si algún dispositivo (por ejemplo: TPM) está en estado Apagado, el inventario de software muestra la versión como **No disponible** o **0**. Y si la aplicación no está instalada, entonces se muestra la versión como **No instalada**.
- El sistema muestra la fecha y hora iniciales predeterminadas del sistema como **Fecha y hora de instalación** en la página **Inventario del sistema** hasta que se instala una nueva versión de firmware del dispositivo mediante el DUP. Además, la fecha y hora del BIOS e iDRAC se deben sincronizar para los componentes cuyos detalles de inventario se obtienen del BIOS (por ejemplo: BIOS, TPM).
- La fecha de instalación no cambia si la versión actualizada es la misma que la versión instalada.
- En ocasiones, el campo **LastUpdateTime** de cualquier componente en el inventario de hardware de iDRAC se muestra con una fecha futura/pasada. Esto puede suceder cuando la hora del BIOS o HOST se establece en una fecha incorrecta. Para solucionar este problema, corrija la fecha del BIOS o HOST.

Si reemplaza algún componente de hardware o actualiza las versiones de firmware, habilite y ejecute la opción **Recopilar inventario del sistema al reiniciar** (CSIOR) para recopilar el inventario del sistema en el reinicio. Después de unos minutos, inicie sesión en iDRAC y vaya a la página **Inventario del sistema** para ver los detalles. Es posible que haya una demora hasta de 5 minutos para que la información esté disponible, según el hardware instalado en el servidor.

NOTA: La opción CSR está activada de forma predeterminada.

NOTA: Es posible que los cambios en la configuración y las actualizaciones de firmware que se realizan dentro del sistema operativo no se reflejen correctamente en el inventario hasta que realice un reinicio del servidor.

Haga clic en **Exportar** para exportar el inventario de hardware en formato XML y guárdelo en la ubicación que desee.

Visualización de los componentes del sistema

Los siguientes componentes de la interfaz de usuario de iDRAC lo ayudan a monitorear el estado de un sistema administrado:

- **Baterías**: proporciona información sobre las baterías del CMOS de la tarjeta madre y el RAID de almacenamiento en la placa base (ROMB).

  NOTA: La configuración de la batería ROMB de almacenamiento solo está disponible si el sistema tiene una ROMB con una batería.

- **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 dobles de memoria en línea (DIMM) presentes en un sistema administrado.
- **Intrusión**: proporciona información sobre el chasis.
- **Alimentación** (disponible solo para servidores en rack y torre): proporciona información sobre las fuentes de alimentación y el estado de redundancia de la fuente de alimentación.

  NOTA: Si solo existe un suministro de energía en el sistema, la redundancia del mismo estará **desactivada**.

- **Voltaje**: indica el estado y la lectura de los sensores de voltaje en varios componentes del sistema.
- **Enfriamiento**: proporciona detalles sobre los ventiladores y las temperaturas del hardware. Los cuatro tipos de ventiladores son de doble rotor incluido (Fan1A, Fan1B), rotor simple incluido (Fan1A, Fan1B), doble rotor no incluido (Fan1, Fan2) y un solo rotor no incluido (Fan1, Fan2).
- **Accelerator**: proporciona los detalles de las GPU y los aceleradores de procesamiento.
- **Ranuras PCIe**: proporciona detalles sobre todos los dispositivos PCIe, incluidos los dispositivos SSD PCIe (NVMe).
- **Dispositivos de red**: proporciona detalles sobre todos los dispositivos de red, incluidas las DPU.

En la siguiente tabla, se enumeran los componentes del sistema que se pueden monitorear:

NOTA: La página **Resumen del sistema** muestra datos solo de los sensores presentes en su sistema.

Tabla 17. Componentes del sistema monitoreados desde la interfaz de usuario de iDRAC

Componentes del sistema	Ruta de navegación en iDRAC
Baterías	**Sistema** > **Visión general** > **Baterías**
Enfriamiento	**Sistema** > **Visión general** > **Enfriamiento**
CPU	**Sistema** > **Visión general** > **CPU**
Memoria	**Sistema** > **Visión general** > **Memoria**
Intrusión	**Sistema** > **Visión general** > **Intrusión**
Alimentación	**Sistema** > **Visión general** > **Alimentación**
Soportes extraíbles	**Sistema** > **Visión general** > **Medios extraíbles**
Voltajes	**Sistema** > **Visión general** > **Voltajes**
Dispositivos de red	**Sistema** > **Visión general** > **Dispositivos de red**
Aceleradores	**Sistema** > **Visión general** > **Aceleradores**
Ranuras PCIe	**Sistema** > **Descripción general** > **Ranuras PCIe**

Utilice el comando `racadm getsensorinfo` para obtener los detalles de cada uno de estos componentes.

NOTA: Para obtener información actualizada sobre las propiedades soportadas y sus valores, consulte la **Ayuda en línea de iDRAC**.

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

En los servidores Dell PowerEdge, 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 proporciona valores de computación, memoria y utilización de recursos de I/O como un índice de CUPS. La iDRAC monitorea este índice de CUPS para la utilización general del sistema y también monitorea el índice instantáneo de utilización de la CPU, la memoria e I/O.

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 soportados 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. Esta es una medida del consumo de ancho de banda de memoria y no de la cantidad de utilización de memoria. La iDRAC la agrega durante un minuto, por lo que puede o no coincidir con la utilización de memoria que muestran otras herramientas del sistema operativo, como **top** en Linux. La utilización del ancho de banda de la memoria que 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 necesarios son:

- Se necesita el privilegio de inicio de sesión para monitorear los datos de rendimiento.
- Se necesita el privilegio de configuración para configurar umbrales de advertencia y restablecer picos históricos.
- Se necesita el privilegio de inicio de sesión y una licencia Enterprise para leer los datos estáticos históricos.

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 RACADM de Integrated Dell Remote Access Controller.

Monitoreo del índice de rendimiento de CPU, memoria y módulos de entrada y salida mediante la interfaz web

Para monitorear el índice de rendimiento de CPU, memoria y módulos de I/O, en la interfaz web de la iDRAC, consulte **Sistema** > **Rendimiento**.

- Sección **Rendimiento del sistema**: muestra la lectura actual y la lectura de aviso para el índice de utilización de I/O, memoria y CPU y el índice CUPS de nivel de sistema en una vista gráfica.
- Sección **Datos históricos de rendimiento del sistema**:
  - Proporciona las estadísticas para CPU, memoria, utilización de E/S e índice CUPS de nivel del sistema. Si el sistema del host está apagado, el gráfico muestra la línea de apagado por debajo del 0 %.
  - Puede restablecer la utilización máxima de un sensor en particular. Haga clic en **Restablecer valores máximos históricos**. Debe tener el privilegio de configuración para restablecer el valor máximo.
- Sección **Métricas de rendimiento**:
  - Muestra el estado y la lectura actual
  - Muestra o especifica el límite de utilización del umbral de precaución. Debe tener el privilegio de configuración del servidor para establecer los valores de umbral.

Para obtener información acerca de las propiedades que se muestran, consulte la **Ayuda en línea de iDRAC**.

Lectura de inventarios de firmware y hardware

NOTA: Asegúrese de esperar unos segundos cuando utilice el comando `getremoteservicesstatus`hasta un máximo de cinco minutos.

1. Utilice el método/URI/comando `getremoteservicesstatus` para comprobar si el estado de Lifecycle Controller (LC) es Listo. Asegúrese de que el sistema se haya **ENCENDIDO** al menos una vez y que **Recopilar el inventario del sistema al reiniciar (CSIOR)** se haya ejecutado al menos una vez para obtener los detalles adecuados. Según los requisitos de algunos componentes, como el almacenamiento y la red, es posible que también deba comprobar si el sistema está **Fuera de POST** y el estado en **Tiempo real (RT)**.
2. El tiempo de espera máximo para que LC esté listo debe ser de cinco minutos. Asegúrese de que el sistema tenga el siguiente estado para que el estado de LC sea Listo:

- Fuera de POST
- El trabajo aún no se ejecuta
- No está en la GUI de LC
- El host está bloqueado en POST

3. Una vez que el estado de LC sea Listo, utilice el método/URI/comando `getinventory`.

Ejecución y verificación del estado de configuración del sistema/componente

NOTA: Asegúrese de esperar unos segundos cuando utilice el comando `getremoteservicesstatus`hasta un máximo de cinco minutos.

1. Verifique el inventario de firmware (siga el procedimiento mencionado anteriormente).
2. Para evitar posibles fallas posteriores, asegúrese de que el componente requerido esté presente en el sistema.
3. Después de las verificaciones iniciales, utilice el método/URI/comando `getremoteservicesstatus` para comprobar si el estado de LC es "Listo". Según los requisitos de algunos componentes, como el almacenamiento y la red, es posible que sea necesario verificar otros estados, por ejemplo, si el sistema está **Fuera de POST** y el estado en **Tiempo real (RT)**.
4. Una vez que LC esté listo, utilice las configuraciones del sistema/componente y cree el trabajo.
5. Si es necesario reiniciar el host para la configuración, cree un trabajo de reinicio o reinicie el host. Es posible que se requiera un reinicio en frío para un ajuste de configuración específico.
6. La persona que llama debe verificar el estado del trabajo que se debe completar: **Ejecución correcta/Error**. Vea los eventos del registro de Lifecycle y el estado de la cola de trabajos, y compruebe los resultados de configuración para obtener más detalles sobre las fallas.
7. Solo después de que la acción **Recopilar el inventario del sistema al reiniciar (CSIOR)** en el host se realice de manera correcta (si es necesaria), el trabajo se marcará como completado si no hubo fallas. Esto es aplicable si es necesario reiniciar el host.
8. Una vez que finalice el trabajo, espere 30 segundos, utilice el método/URI/comando `getremoteservicesstatus` para comprobar si el estado de LC es "Listo", con los otros estados requeridos, y lea los valores esperados.

Ejecución y verificación del estado de la actualización del firmware

NOTA: Asegúrese de esperar unos segundos cuando utilice el comando `getremoteservicesstatus`hasta un máximo de cinco minutos.

1. Verifique el inventario de firmware (siga el procedimiento mencionado anteriormente).
2. Para evitar posibles fallas posteriores, verifique que el componente que se actualizará esté presente en el sistema o si se seleccionó el Dell Update Package (DUP) soportado adecuado para cargar.
3. Después de las verificaciones iniciales, utilice el método/URI/comando `getremoteservicesstatus` para comprobar si el estado de LC es "Listo".
4. Una vez que LC esté listo, utilice el método/URI/comando `firmwareupdate` y aplique el DUP correcto para iniciar la actualización.
5. Si es necesario reiniciar el host para la actualización, cree un trabajo de reinicio o reinicie el host. En el caso de las actualizaciones de alimentación, OSM y PERC, se requiere un reinicio en frío.
6. Verifique el estado del trabajo: **Ejecución correcta/Error**. Vea los eventos del registro de Lifecycle y el estado de la cola de trabajos, y compruebe los resultados de configuración para obtener más detalles sobre las fallas.
7. Solo después de que la acción **Recopilar el inventario del sistema al reiniciar (CSIOR)** en el host se realice de manera correcta (si es necesaria), el trabajo se marcará como completado si no hubo fallas, incluso si se trata de varias actualizaciones de catálogo. Por lo tanto, se recomienda que la persona que llama no tenga un tiempo de espera propio o que este sea superior a este tiempo de espera.
8. Si la actualización se bloquea durante más de seis horas (es decir, el módulo de trabajo no obtiene el estado del módulo de actualización durante seis horas), el trabajo puede caducar y fallar.
9. Los tiempos de espera de actualización se basan en la recomendación del equipo del dispositivo que se lee en el momento de la ejecución.
10. Una vez que el trabajo se marca como completado, y si los nuevos cambios que acaba de aplicar no se informan en el inventario, espere 30 segundos y, a continuación, vuelva a revisar el inventario.

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/iDRAC.Embedded.1/Oem/Dell/DellAttributes/
System.Embedded.1
```

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.

A continuación, se muestran las propiedades de la GPU y los detalles de las licencias:

Tabla 18. Propiedades de la GPU y detalles de las licencias

Propiedades del GPU	Licencia
Inventario	
Número de pieza de la placa	Todas las licencias
Información de OEM	Todas las licencias
Número de serie	Todas las licencias

Tabla 18. Propiedades de la GPU y detalles de las licencias (continuación)

Propiedades del GPU	Licencia
Nombre de marketing	Todas las licencias
Número de pieza de la GPU	Todas las licencias
Fecha de compilación.	Todas las licencias
Versión de firmware	Todas las licencias
GPU GUID	Todas las licencias
PCI vendorid	Todas las licencias
PCI deviceid	Todas las licencias
PCI Subvendorid	Todas las licencias
PCI Subdeviceid	Todas las licencias
Estado de GPU	Todas las licencias
Estado de la GPU	Todas las licencias
Métricas térmicas	
Temperatura de la GPU principal	Todas las licencias
Temperatura de la GPU secundaria	Todas las licencias
Temperatura de la placa	Todas las licencias
Temperatura de la memoria	Todas las licencias
Temperatura mínima de ralentización de hardware de GPU	Enterprise
Temperatura de apagado de GPU	Enterprise
Temperatura máxima de funcionamiento de la memoria	Enterprise
Temperatura máxima de funcionamiento de la GPU	Enterprise
Estado de alerta térmica	Enterprise
Estado de interrupción de alimentación	Enterprise
Métricas de alimentación	
Consumo de energía	Todas las licencias
Estado de la fuente de alimentación	Enterprise
Estado de la fuente de alimentación de la placa	Enterprise

NOTA:

- No se muestran las propiedades de la GPU para las tarjetas GPU integradas y el estado se marca como **Desconocido**.
- La temperatura de funcionamiento puede ser diferente en el caso de los sistemas basados en AMD.
- La cantidad de entradas de la GPU por ranura PCIe que se muestra en el host puede diferir de la cantidad que se muestra en la iDRAC.
- Cuando se necesita un ciclo de encendido y apagado de CA manual después de realizar cualquier actualización de firmware de componentes o paquetes para las GPU o los FPGA de la placa de distribución de alimentación (PDB), se muestra el evento SUP0545 en los registros de Lyfecycle Controller (LC). Después de este evento, asegúrese de realizar un ciclo de apagado y encendido de CA manual o virtual para evitar cualquier comportamiento inesperado en el servidor.
- Después de una actualización de firmware de la GPU que incluya actualizaciones de firmware de componentes o de paquetes de firmware, asegúrese de realizar un ciclo de encendido y apagado de CA o uno de CA virtual para completar la actualización. Esto evita cualquier comportamiento inesperado en iDRAC relacionado con las GPU.
- En el modo persistente, durante el reinicio mediante sistema operativo, es posible que los valores límite de alimentación de la GPU no sean precisos.

- La característica Límite de alimentación de la GPU no está disponible en las configuraciones de GPU que no sean A2.

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 que se recuperan 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.

Con el reinicio activo y el modo persistente desactivado, podemos ver el siguiente comportamiento:

- El consumo de energía se muestra como N/A.
- El límite de alimentación se muestra con valores de límite de inventario más antiguos.

El sistema host debe tener el controlador de la GPU NVIDIA instalado y en ejecución para que estén disponibles varias funciones de la GPU. Algunas de las características de la GPU que están disponibles son: consumo de energía, límite de alimentación actual, limitación y límite de alimentación de la GPU, temperatura objetivo de la GPU, temperatura mínima de ralentización de la GPU, temperatura de apagado de la GPU, temperatura máxima de funcionamiento de la memoria, temperatura máxima de funcionamiento de la GPU, utilización de la GPU, etc. Estos valores se muestran como **N/A** cuando el controlador de la GPU de NVIDIA no está instalado. Las funciones de la GPU dependientes del controlador que está cargado y en ejecución no se limitan a esta lista.

En Linux, cuando no se utiliza la tarjeta, el controlador usa la tarjeta y se descarga para ahorrar energía. En estos casos, no están disponibles las siguientes funciones: consumo de energía, límite de alimentación actual, limitación y límite de alimentación de la GPU, temperatura objetivo de la GPU, temperatura mínima de ralentización de la GPU, temperatura de apagado de la GPU, temperatura máxima de funcionamiento de la memoria, temperatura máxima de funcionamiento de la GPU y utilización de la GPU, entre otras funciones. 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 las características de telemetría, consulte Transmisión de telemetría.

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 una operación iDRAC `racrest` para resolver este problema.

Monitoreo de aceleradores de procesamiento

Los dispositivos aceleradores con aceleradores de procesamiento de clase PCIe necesitan un monitoreo en tiempo real de la temperatura y del sensor, ya que generan mucho calor cuando están en uso.

Realice los siguientes pasos para obtener información de inventario de **aceleradores de procesamiento**:

1. Apague el servidor.
2. Instale los aceleradores en la tarjeta elevadora.
3. Encienda el servidor.
4. Espere hasta que se complete la prueba POST.
5. Inicie sesión en la interfaz de usuario de iDRAC.
6. Vaya a **Sistema** > **Visión general** > **Aceleradores**. Puede ver las secciones GPU y Aceleradores de procesamiento.
7. Amplíe el acelerador específico para ver la siguiente información del sensor:
   - Consumo de energía
   - Detalles de temperatura

NOTA: Los sensores lógicos de temperatura no se muestran en las interfaces de iDRAC. Solo se muestran los sensores físicos de temperatura.

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

NOTA: Los sensores de consumo de energía están disponibles solo para los aceleradores soportados y únicamente con una licencia Datacenter.

NOTA: Es posible que las interfaces de iDRAC no muestren la información de los sensores térmicos y de alimentación que dependen del sistema operativo del host (SO). En este caso, instale los controladores de GPU (paquete ROCm) en el sistema operativo del host.

NOTA:

- Se recomienda realizar la actualización de firmware de la GPU CEC A100 antes de actualizar el firmware de los aceleradores.
- No realice la actualización de firmware de la GPU CEC y de los aceleradores de forma simultánea para evitar fallas de actualizaciones. Realice un ciclo de apagado y encendido de CA o CA virtual después de las fallas de actualización del firmware. Si lo hace, se evitan más fallas a partir de una actualización única causadas por una falla de actualización anterior.
- La actualización de firmware para FPGA de placa base HGX A100 de 8 GPU puede tardar entre 60 y 90 minutos.
- Las actualizaciones de DUP CEC y FPGA de placa base HGX A100 de 8 GPU no se deben activar simultáneamente. Se recomienda seguir estos pasos:
  1. Actualice el firmware de CEC.
  2. Realice un ciclo de CA virtual o manual.
  3. Actualice el firmware de FPGA.
  4. Realice otro ciclo de CA virtual o manual.
- Para actualizar FPGA de PDB desde el sistema operativo, inicie un reinicio en frío. Después de la actualización, se realiza un ciclo de CA virtual.

NOTA: Ocasionalmente, los aceleradores envían valores 0 para el consumo de energía. Por lo tanto, PLDM también utiliza valores 0 y muestra lo mismo en la interfaz de usuario. Sin embargo, los valores se corrigen automáticamente en lecturas posteriores.

NOTA: Los dispositivos PCIe dependen de los controladores y el firmware de dispositivo para responder a las solicitudes de iDRAC. Estos dispositivos registran mensajes de LC HWC9053 (una pérdida de comunicación con el dispositivo) cuando los controladores y el firmware necesarios no están cargados o cuando el servidor se encuentra en el entorno previo al sistema operativo (shell de la UEFI y página Lifecycle Controller).

Comprobación del sistema para el cumplimiento de aire fresco

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

NOTA: Es posible que algunos servidores o ciertas configuraciones de un servidor no soporten aire fresco. Consulte el manual del servidor específico para obtener detalles relacionados con el cumplimiento de aire fresco o comuníquese con Dell para obtener más detalles.

Para comprobar el cumplimiento de aire fresco en el sistema:

1. En la interfaz web de la iDRAC, consulte **Sistema** > **Descripción general** > **Refrigeración** > **Descripción general de temperatura**.
   Se muestra la página **Descripción general de temperatura**.
2. Consulte la sección **Aire fresco** que indica si el servidor cumple los requisitos de aire fresco o no.

Visualización de datos históricos de temperatura

Puede supervisar el porcentaje de tiempo que el sistema ha funcionado a temperatura ambiente, por encima del umbral de temperatura de aire fresco que normalmente se admite. 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. Puede realizar un seguimiento de la temperatura supervisada correspondiente a los últimos siete años y almacenar los resultados.

NOTA: Puede realizar un seguimiento del historial de temperaturas de entrada incluso para los sistemas que no cumplen con la admisión de - aire fresco. Sin embargo, los límites del umbral y las advertencias relacionadas con el aire fresco que se generan se basan en límites compatibles con aire fresco. Los límites son de 42 °C para precaución y de 47 °C en el caso de estado crítico. Estos valores corresponden a los límites de aire fresco de 40 °C y 45 °C, con un margen de 2 °C para precisión.

Se rastrean dos bandas de temperatura fijas que están asociadas a los límites de aire fresco:

- Banda de precaución: consta de la duración en la que un sistema ha funcionado por encima del umbral de precaución del sensor de temperatura (42 °C). El sistema puede funcionar en la banda de precaución el 10 % del tiempo durante 12 meses.
- Banda crítica: consta de la duración en la que un sistema ha funcionado por encima del umbral crítico del sensor de temperatura (47 °C). El sistema puede funcionar en la banda crítica durante el 1 % del tiempo durante 12 meses, lo cual también aumenta el tiempo en la banda de precaución.

Los datos recopilados se representan en formato gráfico para el seguimiento de los niveles del 10 % y el 1 %. Los datos de la temperatura registrada solo se pueden borrar antes del envío desde la fábrica.

Se genera un evento si el sistema continúa funcionando por encima del umbral de temperatura normalmente admitido para un tiempo de funcionamiento especificado. Si la temperatura promedio durante el tiempo de funcionamiento especificado es mayor o igual que el nivel de precaución (> = 8 %) o el nivel crítico (> = 0,8 %), se asienta un evento en el registro de Lifecycle y se genera la correspondiente captura SNMP. Los eventos son los siguientes:

- Evento de precaución cuando la temperatura fue mayor que el umbral de precaución durante un 8 % o más en los últimos 12 meses.
- Evento crítico cuando la temperatura fue mayor que el umbral de precaución durante un 10 % o más en los últimos 12 meses.
- Evento de precaución cuando la temperatura fue mayor que el umbral crítico durante un 0,8 % o más en los últimos 12 meses.
- Evento crítico cuando la temperatura fue mayor que el umbral crítico durante un 1 % o más en los últimos 12 meses.

También puede configurar la iDRAC para generar eventos adicionales. Para obtener más información, consulte la sección Configuración de eventos de periodicidad de alertas.

Visualización de datos históricos de temperatura mediante RACADM

Para visualizar datos históricos mediante RACADM, use el comando `inlettemphistory`:

Para obtener más información, consulte Guía de la CLI RACADM de Integrated Dell Remote Access Controller.

NOTA: Es posible que no coincidan los valores de temperatura de entrada en la interfaz de usuario de iDRAC y RACADM. Para comparar los datos entre estas interfaces, tenga en cuenta lo siguiente:

- Opciones de la **interfaz de usuario de iDRAC** en el menú desplegable y sus valores:
  - Último día: Datos por hora mostrados sobre las últimas 24 horas.
  - Último mes: Datos diarios mostrados sobre los últimos 30 días.
  - Último año: Datos mensuales mostrados sobre los últimos 12 meses.
- Valores de **RACADM**: Muestra valores exactos para hora, día, mes y año de los comandos RACADM respectivos.

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 tarjeta madre** que proporciona una representación gráfica de la temperatura almacenada (valores promedio y pico) correspondientes al último día, a los últimos 30 días y al último año.

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

   NOTA: Después de una actualización del firmware de iDRAC o un restablecimiento de iDRAC, es posible que algunos datos de temperatura no aparezcan 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.

Configuración del umbral de advertencia para la temperatura de entrada

Puede modificar los valores de umbral de aviso mínimo y máximo para el sensor de temperatura de entrada de la tarjeta madre. Si se realiza la acción de restablecer los valores predeterminados, los umbrales de temperatura se establecen en los valores predeterminados. Debe tener el privilegio de usuario Configurar a fin de establecer los valores de umbral de advertencia para el sensor de temperatura de entrada.

NOTA: La diferencia entre la **advertencia superior** y la **Lectura** de la **Temperatura de entrada de la tarjeta madre** debe ser superior a 2 grados para evitar cualquier advertencia de estado.

NOTA: Cada vez que reinicia el sistema o actualiza el firmware de la iDRAC, se muestran los registros LC que proporcionan información sobre el límite de umbral establecido 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 precaución 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 las interfaces de red disponibles en el sistema operativo del 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 la *Guía de la CLI de RACADM de la iDRAC*.

Visualización de las interfaces de red disponibles en el sistema operativo del host mediante la interfaz web

Para ver las interfaces de red disponibles en el sistema operativo del host mediante la interfaz web:

1. Vaya a **Sistema** > **Sistema operativo del host** > **Interfaces de red**.
   La página **Interfaces de red** muestra todas las interfaces de red que están disponibles en el sistema operativo del host.
2. Para ver la lista de interfaces de red asociadas con el 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 la IP del sistema operativo se mostrarán en la sección **Interfaces de red para el sistema operativo del host**.
3. En la columna **FQDD** del dispositivo, haga clic en el enlace del dispositivo de red.

   Se muestra la página del dispositivo correspondiente en la sección **Hardware** > **Dispositivos de red**, en la que puede ver los detalles del dispositivo. Para obtener información acerca de las propiedades, consulte la **Ayuda en línea de la iDRAC**.
4. Haga clic en el icono + para mostrar más detalles.

   De forma similar, se puede ver la información de interfaces de red para el sistema operativo del host asociado con un dispositivo de red desde la página **Hardware** > **Dispositivos de red**. Haga clic en **Ver interfaces de red del sistema operativo del host**.

   NOTA: Para el sistema operativo del host ESXi en iDRAC Service Module 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 o finalización de sesiones de iDRAC

Puede ver la cantidad de usuarios que están conectados actualmente a iDRAC y finalizar las sesiones de usuario.

Finalización de sesiones de iDRAC mediante RACADM

Debe tener privilegios de administrador para finalizar sesiones de iDRAC mediante RACADM.

Para ver las sesiones de usuario actuales, utilice el comando `getssninfo`.

Para finalizar una sesión de usuario, utilice el comando `closessn`.

Para obtener más información, consulte Guía de la CLI RACADM de Integrated Dell Remote Access Controller.

Finalización de sesiones de iDRAC mediante la interfaz web

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

Para ver y finalizar las sesiones de iDRAC:

1. En la interfaz web de la iDRAC, vaya a **Configuración de la iDRAC** > **Usuarios** > **Sesiones**.
   La página **Sesiones** muestra el ID de sesión, el nombre de usuario, la dirección IP y el tipo de sesión. Para obtener más información acerca de las propiedades, consulte la **Ayuda en línea de la iDRAC**.
2. Para finalizar la sesión, en la columna **Finalizar**, haga clic en el icono de papelera de una sesión.

10

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
- Remote Services

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 19. Modos de comunicación: resumen

Modos de comunicación	Protocolo compatible	Comandos admitidos	Requisito previo
Interfaz web del iDRAC	Protocolo de Internet (https)	N/D	Servidor web
Comunicación en serie mediante un cable DB9 de módem nulo	Protocolo de comunicación en serie	RACADM e IPMI	Parte del firmware de iDRAC y la comunicación en serie RAC o IPMI serial está habilitada
Comunicación en serie IPMI en la LAN	Protocolo de bus SSH de administración de plataforma inteligente	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]	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 Dell Lifecycle Controller* disponible en Manuales de iDRAC..			

Temas:

- Configuración de un terminal en serie en RHEL
- Esquemas de criptografía SSH compatibles

Comunicación con iDRAC a través de una conexión serie mediante un cable DB9

Puede utilizar cualquiera de los métodos de comunicación para realizar tareas de administración del sistema a través de una conexión serie a servidores tipo bastidor y torre:

- Comunicación en serie RAC
- Comunicación en serie IPMI: modo básico de conexión directa y modo de terminal de conexión directa.

NOTA: Cuando USB DB9 está conectado al sistema, la **Velocidad en baudios** (**Ajustes de la iDRAC** > **Conectividad** > **Serie**) se configura automáticamente en función de si **Serie RAC** está habilitado o deshabilitado. Si **Serie RAC** está habilitado, **Serie RAC > Velocidad en baudios** está configurado para USB DB9. Si **Serie RAC** está deshabilitado (IPMI está habilitado), **Serie IPMI > Velocidad en baudios** está configurado para USB DB9.

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 IU 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 en la conexión serie:

NOTA: Esto es aplicable solo para los servidores iDRAC en torre y rack.

1. Encienda o reinicie el sistema.
2. Presione F2.
3. Vaya a **Configuración del BIOS del sistema** > **Comunicación en serie**.
4. Seleccione **Conector serial externo** para el **Dispositivo de acceso remoto**.
5. Haga clic en **Back** (Atrás), haga clic en **Finish** (Terminar), y posteriormente, haga clic en **Yes** (Sí).
6. Presione Esc para salir de **Configuración del sistema**.

Activación de la conexión serie RAC

Después de configurar la conexión serie en el BIOS, active la serie RAC en iDRAC.

NOTA: Esto es aplicable solo para los servidores iDRAC en torre y rack.

Activación de la conexión serie RAC mediante RACADM

Para habilitar la conexión serie RAC mediante RACADM, utilice el comando `set` con el objeto en el grupo `iDRAC.Serial`

Activación de la conexión serie RAC mediante la interfaz web

Para habilitar la conexión serie RAC:

1. En la interfaz web de la iDRAC, vaya a **Ajustes de la iDRAC** > **Red** > **Serie**.
   Se muestra la página **Serie**.
2. En **Serie RAC**, seleccione **Habilitado** y especifique los valores para los atributos.
3. Haga clic en **Aplicar**.
   Se configuran los ajustes de serie de RAC.

Activación de los modos básicos y de terminal de la conexión serie básica IPMI

Para habilitar el enrutamiento en serie IPMI del BIOS a iDRAC, configure la comunicación en serie IPMI en cualquiera de los siguientes modos en iDRAC:

NOTA: Esto es aplicable solo para los servidores iDRAC en torre y rack.

- 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 deshabilitar la interfaz en serie RAC para habilitar la serie IPMI.

Para configurar los ajustes de la serie IPMI:

1. En la interfaz web de la iDRAC, vaya a **Ajustes de la iDRAC** > **Conectividad** > **Serie**.
2. En **Serie de IPMI**, especifique los valores para los atributos. Para obtener información acerca de las opciones, consulte la **Ayuda en línea de la iDRAC**.
3. Haga clic en **Aplicar**.

Activación del modo de comunicación en serie de IPMI mediante RACADM

Para configurar el modo IPMI, deshabilite la interfaz en serie RAC y, a continuación, habilite el modo 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 a la configuración adecuada mediante el comando.

```
racadm set iDRAC.Serial.Enable 0
```

2. Establezca la velocidad en baudios de la serie 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 IPMI mediante el comando.

```
racadm set iDRAC.IPMISerial.FlowContro 1
```

4. Establezca el nivel de privilegio mínimo del canal en serie 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 de serie (conector de serie externo) esté configurado correctamente en el dispositivo de acceso remoto en el programa de configuración del BIOS a fin de configurar el BIOS para la conexión en serie.

Para obtener más información sobre estas propiedades, consulte la especificación de IPMI 2.0.

Configuración adicional para el modo de terminal de la comunicación en serie IPMI

En esta sección, se proporcionan ajustes de configuración adicionales para el modo de terminal de comunicación en serie IPMI.

Configuración de valores adicionales para el modo de terminal de comunicación en serie IPMI mediante RACADM

Para configurar los ajustes 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 RACADM de Integrated Dell Remote Access Controller.

Configuración de valores adicionales para el modo de terminal de comunicación en serie IPMI mediante la interfaz web

Para establecer los ajustes del modo de terminal:

1. En la interfaz web de la iDRAC, vaya a **Ajustes de la iDRAC** > **Conectividad** > **Serie**.
Se muestra la página **Serie**.

2. Habilite la serie IPMI
3. Haga clic en **Ajustes del modo de terminal.**
   Se mostrará la página **Ajustes del modo de terminal**.
4. Especifique los siguientes valores:
   - Edición de línea
   - Control de eliminación
   - Control del eco
   - Control del protocolo de enlace
   - Nueva secuencia de línea
   - Introducir nueva secuencia de línea

   Para obtener información acerca de las opciones, consulte la **Ayuda en línea de la iDRAC**.
5. Haga clic en **Aplicar**.
   Se configuran los ajustes del modo de terminal.
6. Asegúrese de que el MUX de serie (conector de serie externo) esté configurado correctamente en el dispositivo de acceso remoto en el programa de configuración del BIOS a fin de configurar el BIOS para la conexión en serie.

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

iDRAC soporta secuencias de teclas Escape que permiten alternar entre la comunicación de la interfaz en serie RAC y la consola en serie en servidores en rack y torre.

Cambio de una comunicación en serie RAC a consola de comunicación en serie

Para cambiar al modo de consola en serie cuando se encuentre en el modo de comunicación de interfaz en serie de RAC, presione Esc+Mayús, Q.

En el modo de terminal, para cambiar la conexión al modo de consola en serie, presione Esc+Mayús, Q.

Para volver al modo de terminal, cuando esté conectado en el modo de consola en serie, presione Esc+Mayús, 9.

Cambio de una consola de comunicación en serie a la comunicación en serie RAC

Para cambiar al modo de comunicación de interfaz en serie RAC cuando se encuentre en el modo de consola en serie, presione Esc+Mayús, 9.

La secuencia de teclas lo dirige al símbolo del sistema `iDRAC Login` (si la iDRAC está establecida en el modo de conexión en serie RAC) o al modo de conexión en serie donde se pueden emitir comandos de terminal si la iDRAC está establecida en el modo de terminal de conexión directa en serie IPMI.

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 de forma remota a los sistemas operativos sin tiempo de espera.
- Diagnosticar los sistemas host en los servicios de administración de emergencias (EMS) o en la consola de administrador especial (SAC) para el shell de Windows o Linux.
- Ver el progreso de un servidor durante la POST y volver a configurar el programa de configuración del BIOS.

Para configurar el modo de comunicación de SOL:

1. Configure el BIOS para la conexión serie.

2. Configure iDRAC para usar SOL.
3. Activar un protocolo compatible (SSH, IPMItool).

Configuración del BIOS para la conexión serie

NOTA: Esto es aplicable solo para los servidores iDRAC en torre y rack.

1. Encienda o reinicie el sistema.
2. Presione F2.
3. Vaya a **Configuración del BIOS del sistema** > **Comunicación en serie**.
4. Especifique los siguientes valores:
   - Comunicaciones en serie: activada con redirección de consola
   - Dirección del puerto serial: COM2.

     NOTA: Puede establecer el campo **comunicación en serie** en **activado con redirección serial a través de com1** si **el dispositivo serial2** en el campo **dirección del puerto serial** también está establecido en com1.

   - Conector serial externo: dispositivo serial 2
   - Velocidad en baudios a prueba de errores: 115200
   - Tipo de terminal remoto: VT100/VT220
   - Redirección después del inicio: habilitada
5. Haga clic en **Atrás** y, luego, en **Finalizat**.
6. Haga clic en **Yes** para guardar los cambios.
7. Presione <Esc> para salir de **Configuración del sistema**.

   NOTA: El BIOS envía los datos en serie de la pantalla en formato 25 x 80. La ventana SSH que se utiliza para invocar el comando `console com2` se debe configurar en 25 x 80. A continuación, la pantalla redirigida aparece 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 los ajustes de SOL en iDRAC mediante la interfaz web, RACADM o la utilidad de configuración de iDRAC.

Configuración de iDRAC para usar SOL mediante RACADM

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

1. Active la comunicación en serie IPMI en la LAN mediante el comando.

```
racadm set iDRAC.IPMISol.Enable 1
```

2. Actualice el nivel de privilegio mínimo de IPMI SOL mediante el comando.

```
racadm set iDRAC.IPMISol.MinPrivilege <level>
```

Parámetro	Nivel de privilegio
<level> = 2	Usuario
<level> = 3	Operador
<level> = 4	Administrador

NOTA: Para activar IPMI SOL, debe tener el privilegio mínimo definido en IMPI SOL. Para obtener más información, consulte la especificación de IPMI 2.0.

3. Actualice la velocidad en baudios de IPMI SOL mediante el comando.

```
racadm set iDRAC.IPMISol.BaudRate <baud_rate>
```

NOTA: Para redirigir la consola 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. Habilite SOL para cada usuario mediante el comando.

```
racadm set iDRAC.Users.<id>.SolEnable 2
```

Parámetro	Descripción
<id>	ID único 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.

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 la iDRAC, vaya a **Ajustes de la iDRAC** > **Conectividad** > **Comunicación en serie por LAN**.
   Se muestra la página **Comunicación en serie por LAN**.
2. Habilite SOL, especifique los valores y haga clic en **Aplicar**.
   Se configuran los ajustes de IPMI SOL.
3. Para configurar el intervalo de acumulación de caracteres y el umbral de envío de caracteres, seleccione **Ajustes avanzados**.
   Aparecerá la página **Ajustes de comunicación en serie por LAN**.
4. Especifique los valores para los atributos y haga clic en **Aplicar**.

   Se configuraron los ajustes avanzados de IPMI SOL. Estos valores ayudan a mejorar el rendimiento.

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

Activación del protocolo compatible

Los protocolos compatibles son IPMI y SSH.

Activación del protocolo admitido mediante RACADM

Para habilitar SSH, ejecute el siguiente comando.

SSH

```
racadm set iDRAC.SSH.Enable 1
```

Para cambiar el puerto SSH, ejecute el siguiente comando:

```
racadm set iDRAC.SSH.Port <port number>
```

Puede utilizar herramientas como:

- IPMItool para usar el protocolo IPMI

- Putty/OpenSSH para utilizar el protocolo SSH

Activación del protocolo admitido mediante la interfaz web

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

Para activar IPMI, vaya a **Configuración de la 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.

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 la iDRAC. Es posible analizar comandos de SMCLP remoto a través de esta interfaz.

SSH ha mejorado la seguridad. La iDRAC solo admite SSH versión 2 con autenticación de contraseña y está habilitada de manera predeterminada. La iDRAC admite hasta dos o cuatro sesiones de SSH a la vez.

NOTA: Mientras se establece una conexión SSH, se muestra un mensaje de seguridad `Further Authentication required` incluso cuando 2FA está deshabilitada.

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 la iDRAC, realice los siguientes pasos:

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 la 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 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 com2`
   - `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.

   Para ver el historial de la interfaz de SOL, habilite la captura de datos en serie. Escribe todos los datos en serie recibidos del host en la memoria de iDRAC en una ventana gradual de 512 KB. Para ello, se requiere la licencia de Datacenter.

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

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 administración 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 com2` 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:
   - Cuando se accede al sistema administrado a través de PuTTY durante la prueba POST, si la opción de las teclas de función y teclado en PuTTY está establecida en:
     - VT100+: F2 pasa, pero F12 no puede pasar.
     - ESC[n~: F12 pasa, pero F2 no puede pasar.

- 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.

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 SOL, finalice la sesión SOL desde la consola de línea de comandos de iDRAC.

Para salir de la redirección de SOL, presione Intro, Esc, T.
La sesión de SOL se cierra.

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 la iDRAC** > **Conectividad** > **Comunicación en serie en la LAN**.

Comunicación con iDRAC mediante IPMI en la LAN

Debe configurar IPMI en la LAN para que iDRAC habilite o deshabilite los comandos de IPMI a través de canales LAN a cualquier sistema externo. Si IPMI en la LAN no está configurada, los sistemas externos no pueden comunicarse con el servidor iDRAC mediante los comandos de IPMI.

NOTA: IPMI también soporta el protocolo de direcciones IPv6 para sistemas operativos basados en Linux.

Configuración de IPMI en la LAN mediante la utilidad de configuración de iDRAC

Para configurar IPMI en la LAN:

1. En la **Utilidad de configuración de iDRAC**, vaya a **Red**.
   Se muestra la página **Red de configuración de iDRAC**.
2. Para **Ajustes 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 **Back** (Atrás), haga clic en **Finish** (Terminar), y posteriormente, haga clic en **Yes** (Sí).
   Se configuran los ajustes de IPMI en la LAN.

Configuración de IPMI en la LAN mediante RACADM

1. Habilite la IPMI en la LAN.

```
racadm set iDRAC.IPMILan.Enable 1
```

NOTA: Estos ajustes determinan 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 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 LAN de IPMI, si es necesario.

```
racadm set iDRAC.IPMILan.EncryptionKey <key>
```

Parámetro	Descripción
<key>	Clave de cifrado de 20 caracteres en un formato hexadecimal válido.

NOTA: La IPMI de iDRAC soporta el protocolo RMCP+. Para obtener más información, consulte las especificaciones de IPMI 2.0. en **intel.com**.

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 **Ajustes de iDRAC** > **Conectividad**.
   Aparecerá la página **Red**.
2. En **Configuración de IPMI**, especifique los valores para los atributos y haga clic en **Aplicar**.

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

   Se configuran los ajustes de IPMI en la LAN.

Activación o desactivación de RACADM remoto

Puede habilitar o deshabilitar RACADM remoto mediante la interfaz Web iDRAC o RACADM. Puede ejecutar hasta cinco sesiones remotas de RACADM en paralelo.

NOTA: RACADM está habilitada de manera predeterminada.

Habilitación o deshabilitación de RACADM remoto mediante RACADM

NOTA: Se recomienda ejecutar estos comandos mediante RACADM local o RACADM de firmware.

Para deshabilitar RACADM remoto:

- Para deshabilitar RACADM remoto:

```
racadm set iDRAC.Racadm.Enable 0
```

- Para habilitar RACADM remoto:

```
racadm set iDRAC.Racadm.Enable 1
```

Activación o desactivación de RACADM remoto mediante la interfaz web

1. En la interfaz web de la iDRAC, vaya a **Ajustes de la iDRAC** > **Servicios**.
2. En **RACADM remoto**, seleccione la opción deseada y haga clic en **Aplicar**.
   El RACADM remoto se habilita o deshabilita según la selección.

Desactivación de RACADM local

El protocolo RACADM local está habilitado de manera predeterminada. Para desactivarlo, consulte Desactivación del acceso para modificar los valores de configuración de la iDRAC en el sistema host.

Configuración de Linux para la consola en serie durante el arranque en RHEL

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 la posible condición de error de varios componentes intentando acceder al puerto serial.

Activación del inicio de sesión en la consola virtual después del inicio

En el archivo **/etc/inittab**, agregue una nueva línea para configurar `agetty` en el puerto serial COM2:

```
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
```

En el siguiente ejemplo, se muestra un archivo de ejemplo 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 nueva línea con el nombre del tty serial para COM2:

```
ttyS1
```

En el siguiente ejemplo, se muestra un archivo de ejemplo con la nueva línea.

NOTA: Utilice la secuencia de clave de interrupción (~B) para ejecutar los comandos de teclado de Linux **Magic SysRq** en la consola en serie mediante 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 de un terminal en serie en RHEL

Para configurar un terminal en serie en RHEL, 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 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` mediante 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 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 iDRAC mediante el protocolo SSH, se soportan varios esquemas de criptografía que se enumeran en la siguiente tabla.

Tabla 20. Esquemas de criptografía SSH

Tipo de esquema	Algoritmos
Criptografía asimétrica	
Clave pública	• curve25519-sha256 • curve25519-sha256@libssh.org • ssh-rsa • ecdsa-sha2-nistp256 • diffie-hellman-group16-sha512 • diffie-hellman-group18-sha512 • diffie-hellman-group14-sha256
Criptografía simétrica	
Intercambio de claves	• rsa-sha2-512

Tabla 20. Esquemas de criptografía SSH (continuación)

Tipo de esquema	Algoritmos
	• rsa-sha2-256 • ssh-rsa • ecdsa-sha2-nistp256 • ssh-ed25519 • ecdh-sha2-nistp256 • ecdh-sha2-nistp384 • ecdh-sha2-nistp521 • diffie-hellman-group-exchange-sha256
Cifrado	• chacha20-poly1305@openssh.com • aes128-ctr • aes192-ctr • aes256-ctr • aes128-gcm@openssh.com • aes256-gcm@openssh.com
MAC	• umac-64@openssh.com • umac-128-etm@openssh.com • hmac-sha2-256-etm@openssh.com • hmac-sha2-512-etm@openssh.com • umac-128@openssh.com • hmac-sha2-256 • hmac-sha2-512
Compression	Ninguna

NOTA: Si activa OpenSSH 7.0 o versiones posteriores, la compatibilidad con clave pública de DSA se desactiva. A fin de garantizar una mejor seguridad para iDRAC, Dell recomienda no activar la compatibilidad con clave pública de DSA.

Uso de la autentificación de clave pública para SSH

iDRAC soporta la Autenticación de clave pública (PKA) mediante SSH. Esta es una función con licencia. Cuando la PKA mediante SSH se configura y utiliza correctamente, debe ingresar el nombre de usuario durante el inicio de sesión en iDRAC. Esto es útil para configurar scripts automatizados que realicen diversas funciones. Las claves cargadas deben estar en formato RFC 4716 o OpenSSH. De lo contrario, debe convertir las claves en ese formato.

En cualquier caso, se debe generar un par de claves públicas y privadas en la estación de administración. La clave pública se carga al usuario local de iDRAC y el cliente SSH utiliza la clave privada 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:

- Aplicación **Generador de claves PuTTY** para clientes que ejecutan Windows
- CLI **ssh-keygen** para clientes que ejecutan Linux.

PRECAUCIÓN: Este privilegio está reservado para los usuarios que son miembros del grupo de usuarios administrador en iDRAC. Sin embargo, este privilegio se puede asignar a los usuarios en el grupo de usuarios "personalizado". Un usuario con este privilegio puede modificar la configuración de cualquier usuario. Esto incluye la creación o eliminación de cualquier usuario, la administración de la clave SSH para usuarios, etc. Por estos motivos, asigne este privilegio cuidadosamente.

PRECAUCIÓN: La capacidad de cargar, ver o eliminar claves SSH se basa en el privilegio de usuario "Configurar usuarios". Este privilegio permite que los usuarios configuren la clave SSH de otro usuario. Debe otorgar este privilegio con cuidado.

Generación de claves públicas para Linux

Para usar la aplicación **ssh-keygen** a fin de crear la clave básica, abra una ventana de terminal y, en el indicador del shell, ingrese `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 que se generan desde la estación de administración de Linux mediante ssh-keygen tienen un formato distinto de 4716. Convierta las claves al formato 4716 mediante `ssh-keygen -e -f /root/.ssh/id_rsa.pub > std_rsa.pub`. No cambie los permisos del archivo de clave. La conversión se debe realizar con permisos predeterminados.

NOTA: iDRAC no soporta el reenvío de claves mediante ssh-agent.

Generación de claves públicas para Windows

Para utilizar la aplicación **Generador de claves PuTTY** a fin de 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. La cantidad de bits debe estar entre 2048 y 4096 bits.
3. Haga clic en **Generar** y mueva el mouse en la ventana, tal como se indica.
   Se generan las claves.
4. Puede modificar el campo de comentario clave.
5. Ingrese una frase de contraseña para proteger la clave.
6. Guarde la clave pública y la clave privada.

Carga de claves SSH

Puede cargar hasta cuatro claves públicas **por usuario** para usarlas en una interfaz SSH. Antes de agregar las claves públicas, asegúrese de ver las claves si están configuradas, de modo que no se sobrescriba accidentalmente una clave.

Cuando agregue nuevas claves públicas, asegúrese de que las claves existentes no estén en el índice donde se agrega la nueva clave. La iDRAC no realiza comprobaciones para asegurarse de que las claves anteriores se eliminen antes de que se agreguen claves nuevas. Cuando se agrega una nueva clave, se puede utilizar si la interfaz SSH está habilitada.

Carga de claves SSH mediante la interfaz web

Para cargar las claves SSH:

1. En la interfaz web de iDRAC, vaya a **Configuración de iDRAC** > **Usuarios** > **Usuarios locales**.
   Se muestra la página **Usuarios locales**.
2. En la columna **ID del usuario**, haga clic en un número de ID de usuario.
   Aparece la página **Menú principal de usuarios**.
3. En **Configuraciones de clave SSH**, seleccione **Cargar claves SSH** y haga clic en **Siguiente**.
   Se muestra la página **Cargar claves SSH**.
4. Cargue las claves SSH de una de las siguientes maneras:
   - Cargue el archivo de clave.
   - Copie el 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 descargar la clave SSH, ejecute el siguiente comando:

NOTA: No puede 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 de usuario 2 de iDRAC en el primer espacio de claves mediante un archivo, ejecute el siguiente comando:

```
$ racadm sshpkauth -i 2 -k 1 -f pkkey.key
```

NOTA: La opción `-f` no se admite en RACADM SSH/serie.

Eliminación de claves SSH

Antes de eliminar las claves públicas, asegúrese de ver si las claves si están configuradas, de modo que no se elimine accidentalmente una clave.

Eliminación de claves SSH mediante RACADM

Para borrar la clave SSH, ejecute el siguiente comando:

- 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`

Eliminación de claves SSH mediante la interfaz web

Para eliminar las claves SSH:

1. En la interfaz web, vaya a **Ajustes de iDRAC** > **Usuarios**.
   Se muestra la página **Usuarios locales**.
2. En la columna **ID**, seleccione un número de ID de usuario y haga clic en **Editar**.
   Se muestra la página **Editar usuario**.
3. En **Ajustes de la clave SSH**, seleccione una clave SSH y haga clic en **Edit**.
   La página **Clave SSH** muestra los detalles de **Editar desde**.
4. Seleccione **Eliminar** para las claves que desea eliminar y haga clic en **Aplicar**.
   Se eliminan las claves seleccionadas.

Visualización de claves SSH

Puede ver las claves que se cargan en iDRAC.

Visualización de claves SSH mediante la interfaz web

Para ver las claves SSH:

1. En la interfaz web, vaya a **Ajustes de iDRAC** > **Usuarios**.
   Se muestra la página **Usuarios locales**.
2. En la columna **ID del usuario**, haga clic en un número de ID de usuario.
   Aparece la página **Menú principal de usuarios**.
3. En **Configuraciones de clave SSH**, seleccione **Ver/eliminar claves SSH** y haga clic en **Siguiente**.
   Se muestra la página **Ver/eliminar claves SSH** con los detalles de la clave.

11

Funciones de usuario y cuentas de usuario

Puede crear funciones de usuario con privilegios específicos mediante la iDRAC para administrar el sistema y mantener su seguridad. De manera predeterminada, la iDRAC está configurada con una función de administrador local. En la etiqueta del sistema se proporciona el nombre de usuario y la contraseña predeterminados de la iDRAC. Para obtener más información, consulte la documentación de su servidor.

Como administrador, puede crear funciones de usuario con los privilegios asociados. Puede crear cuentas de usuario y asignar las funciones recién creadas o las funciones existentes **Administrador**, **Operador**, **Solo lectura** en la iDRAC. 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.

Temas:

Funciones y privilegios de usuario de iDRAC

Las funciones predeterminadas de la iDRAC son **Administrador**, **Operador** y **Solo lectura**. Estas funciones tienen privilegios de usuario específicos.

En la siguiente tabla, se muestran los nombres de las funciones predeterminadas de la iDRAC:

Tabla 21. Funciones de iDRAC

Funciones	Privilegios
Administrador	Iniciar sesión en la iDRAC, Configurar iDRAC, Configurar usuarios, Borrar registros, Configurar sistema, Acceder a consola virtual, Acceder a medios virtuales, Probar alertas y Ejecutar comandos de depuración.
Operador	Iniciar sesión en la iDRAC, Configurar iDRAC, Borrar registros, Configurar sistema, Acceder a medios virtuales, Probar alertas y Ejecutar comandos de depuración.
ReadOnly	Inicio de sesión en la iDRAC.

En la siguiente tabla se describen los privilegios de usuario:

Tabla 22. Privilegios del usuario del iDRAC

Privilegios	Descripción
Iniciar sesión en la iDRAC	Permite a los usuarios iniciar sesión en la iDRAC.
Configurar la iDRAC.	Permite a los usuarios configurar la 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 y SCP, entre otros.
NOTA: La función de administrador reemplaza todos los privilegios de otros componentes, como la contraseña de configuración del BIOS.	
Configurar usuarios.	Permite a los usuarios crear cuentas de usuario.
Borrar registros	Permite a los usuarios borrar solo los registros de eventos del sistema (SEL).

Tabla 22. Privilegios del usuario del iDRAC (continuación)

Privilegios	Descripción
Configurar sistema	Permite a los usuarios realizar un ciclo de apagado y encendido del sistema host.
Acceder a la consola virtual	Permite a los usuarios ejecutar la consola virtual.
Acceder a los medios virtuales	Permite a los usuarios ejecutar y utilizar los medios virtuales.
Probar alertas	Permite a los usuarios probar alertas por correo electrónico, excepciones de SNMP y otras notificaciones de alerta configuradas.
Ejecutar comandos de depuración	Permite a los usuarios ejecutar comandos de diagnóstico.

Caracteres recomendados para nombres de usuario y contraseñas

En esta sección, se 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 cuando cree nombres de usuario y contraseñas:

Tabla 23. Caracteres recomendados para los nombres de usuario

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

Tabla 24. Caracteres recomendados para las contraseñas

Caracteres	Versiones de iDRAC10	Longitud
• Entre 0 y 9 • A-Z • a-z • ' - ! " # $ % & ( ) * , . / : ; ? @ [\ ] ^ _ ` { | } ~ + < = >	1.10.17.00 y posterior	1-127

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 las contraseñas para los recursos compartidos de red están determinados por el tipo de recurso compartido de red. La iDRAC admite caracteres válidos para las credenciales del recurso compartido de red según lo definido por el tipo de recurso compartido, excepto <, > y , (coma).

NOTA: Para mejorar la seguridad, se recomienda utilizar contraseñas complejas de ocho caracteres o más, que incluyan letras minúsculas, mayúsculas, números y caracteres especiales. También se recomienda cambiar periódicamente las contraseñas, si es posible.

Creación de funciones de usuario

Puede crear funciones de usuario con los privilegios necesarios para poder delegar las tareas a los usuarios de manera eficiente. Solo los usuarios con la función de Administrador pueden crear funciones de usuario.

1. Vaya a **Configuración de la iDRAC** > **Usuarios** > **Usuarios locales** > **Roles de usuario**.

2. Haga clic en **+Agregar**.
   Se muestra el cuadro de diálogo **Agregar función nueva**.
3. Seleccione el **ID de usuario**.
4. Ingrese el **Nombre de función de usuario**.
5. Seleccione los **Privilegios del usuario**.
6. Haga clic en **Save**.
   La función de usuario aparece en la lista **Funciones de usuario**.

Configuración de usuarios locales

Puede configurar hasta 32 usuarios locales en la iDRAC con funciones de usuario específicas. Antes de crear un usuario de la iDRAC, compruebe si existen usuarios actuales. Puede establecer los nombres de usuario, las contraseñas y los roles con los privilegios para estos usuarios. Los nombres de usuario y las contraseñas se pueden cambiar usando cualquiera de las interfaces seguras de la iDRAC (es decir, la interfaz web, RACADM o Redfish).

Crear usuarios locales mediante la interfaz de usuario de la iDRAC

Puede agregar usuarios y asignar funciones específicas a los usuarios en función de las tareas que se les asignan.

NOTA: Solo podrá crear usuarios si la función de usuario asignada tiene el privilegio **Configurar usuarios**.

1. En la interfaz de usuario de la iDRAC, vaya a **Ajustes de la iDRAC** > **Usuarios locales** > **Visión general**.
   Se enumeran los usuarios locales.
2. Haga clic en **+Agregar**.
   Aparece el cuadro de diálogo **Agregar usuario nuevo**.
3. Seleccione el **ID**.
4. Ingrese los campos **Nombre de usuario**, **Contraseña** y **Confirmar contraseña**.
5. Seleccione la **Función de usuario**
   Se muestran los **Privilegios de usuario** correspondientes.
6. Haga clic en **Save**.
   Y el nombre del usuario aparecerá en la lista.

Configuración de los usuarios locales mediante RACADM

NOTA: Debe iniciar sesión como usuario **raíz** para ejecutar comandos de RACADM en un sistema Linux remoto.

Puede configurar uno o varios usuarios de iDRAC mediante RACADM.

Para configurar varios usuarios de iDRAC con ajustes de configuración idénticos, siga estos procedimientos:

- Utilice los ejemplos de RACADM de esta sección como guía para crear un archivo por lotes de comandos de RACADM y, a continuación, ejecutar 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 habilitar y deshabilitar con el tiempo. Como resultado, 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 (1-16):

```
racadm get iDRAC.Users.<index>.UserName
```

Se muestran varios parámetros e ID de objeto 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 habilitar la autenticación SNMP v3 de un usuario, utilice los objetos **SNMPv3AuthenticationType**, **SNMPv3Enable**, **SNMPv3PrivacyType**. Para obtener más información, consulte Guía de la CLI RACADM de Integrated Dell Remote Access Controller.

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.

Adición de un usuario de iDRAC mediante RACADM

1. Configure 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. Configure los privilegios de usuario.

   Para obtener más información, consulte Guía de la CLI RACADM de Integrated Dell Remote Access Controller.

4. Habilite el usuario.

   ```
   racadm set idrac.users.<index>.enable 1
   ```

Para verificar, utilice el siguiente comando:

```
racadm get idrac.users.<index>
```

Para obtener más información, consulte Guía de la CLI RACADM de Integrated Dell Remote Access Controller.

Habilitación de un usuario de iDRAC con permisos

Para habilitar a un usuario con permisos administrativos específicos (autoridad basada en funciones):

1. Busque un índice de usuarios disponible.

   ```
   racadm get iDRAC.Users <index>
   ```

2. Escriba los siguientes comandos con el nuevo nombre de usuario y contraseña.

   ```
   racadm set iDRAC.Users.<index>.Privilege <user privilege bit mask value>
   ```

NOTA: El valor de privilegio predeterminado es 0, esto indica que el usuario no tiene habilitado privilegios. Para obtener una lista de los valores de máscara de bits válidos para privilegios específicos del usuario, consulte Guía de la CLI RACADM de Integrated Dell Remote Access Controller.

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: Se admite StartTLS en el puerto 389. De manera predeterminada, LDAPS está configurado en el puerto 636. El protocolo de conexión se puede volver a configurar en StartTLS mediante el comando `racadm set iDRAC.ActiveDirectory.Connection StartTLS` de RACADM o Redfish.

Requisitos a fin de usar la autenticación de Active Directory para iDRAC

Para utilizar la función de autenticación de Active Directory de iDRAC, asegúrese de:

- Implementar una infraestructura de Active Directory. Consultar el sitio web de Microsoft para obtener más información.
- PKI integrada en la infraestructura de Active Directory. La iDRAC utiliza el mecanismo estándar de infraestructura de clave pública (PKI) para autenticarse de manera segura en Active Directory. Consultar el sitio web de Microsoft para obtener más información.
- Se habilitó la capa de conectores seguros (SSL) en todas las controladoras de dominio a las que se conecta iDRAC para autenticarse en todas las controladoras de dominio.

Habilitación de SSL en la controladora de dominio

Cuando iDRAC autentica usuarios con una controladora de dominio de Active Directory, inicia una sesión SSL con la controladora de dominio. En este momento, la controladora de dominio debe publicar un certificado firmado por la autoridad de certificación (CA), cuyo certificado raíz también se carga en iDRAC. Para que iDRAC se autentique en **cualquier** controladora de dominio, ya sea la controladora de dominio raíz o secundaria, esa controladora de dominio debe tener un certificado habilitado para SSL firmado por la CA del dominio.

Si utiliza la CA raíz de Microsoft Enterprise para asignar **automáticamente** todas las controladoras de dominio a un certificado SSL, debe:

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 de firmware de iDRAC

Instalación del certificado SSL para cada controladora de dominio

Para instalar el certificado SSL en cada controladora:

1. Haga clic en **Inicio** > **Herramientas administrativas** > **Política de seguridad de dominio**.
2. Expanda la carpeta **Políticas de clave pública**, haga clic con el botón secundario en **Configuración automática de solicitud de certificado** y, a continuación, haga clic en **Solicitud automática de certificado**.
   Se muestra el **Asistente de configuración automática de solicitud de certificado**.
3. Haga clic en **Siguiente** y seleccione **Controladora de dominio**.
4. Haga clic en **Siguiente** y, a continuación, en **Finalizar**. El certificado SSL está instalado.

Exportación del 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 Microsoft Enterprise CA.
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/quitar complemento**, haga clic en **Agregar**.
6. En la ventana **Complemento independiente**, seleccione **Certificados** y haga clic en **Agregar**.
7. Seleccione **Computadora** y haga clic en **Siguiente**.
8. Seleccione **Computadora local**, haga clic en **Finalizar** y, a continuación, en **Aceptar**.
9. En la ventana **Consola 1**, vaya a la carpeta **Certificados Personal Certificados**.
10. Localice el certificado de CA raíz y haga clic con el botón derecho del mouse sobre ese elemento. Seleccione **Todas las tareas** y haga clic en **Exportar...**.
11. En el **Asistente para exportar certificados**, haga clic en **Siguiente** y seleccione **No, no exportar clave privada**.
12. Haga clic en **Siguiente** y seleccione **X.509 (.cer) codificado en Base64** como formato.
13. Haga clic en **Siguiente** para guardar el certificado en el directorio del sistema.
14. Cargue el certificado que guardó 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 autenticación soportados de Active Directory

Puede utilizar Active Directory a fin de definir el acceso de usuario de iDRAC mediante dos métodos:

- Solución **Esquema estándar**, que utiliza los objetos de grupo predeterminados de Active Directory de Microsoft solamente.
- Solución **Esquema extendido**, que tiene objetos de Active Directory personalizados. Todos los objetos de control de acceso se mantienen en Active Directory. Proporciona la máxima flexibilidad para configurar el acceso de los usuarios en diferentes iDRAC con distintos niveles de privilegios.

Visión general de Active Directory con esquema estándar

Como se muestra en la siguiente figura, el uso del esquema estándar para la integración de Active Directory necesita la configuración tanto en Active Directory como en iDRAC.

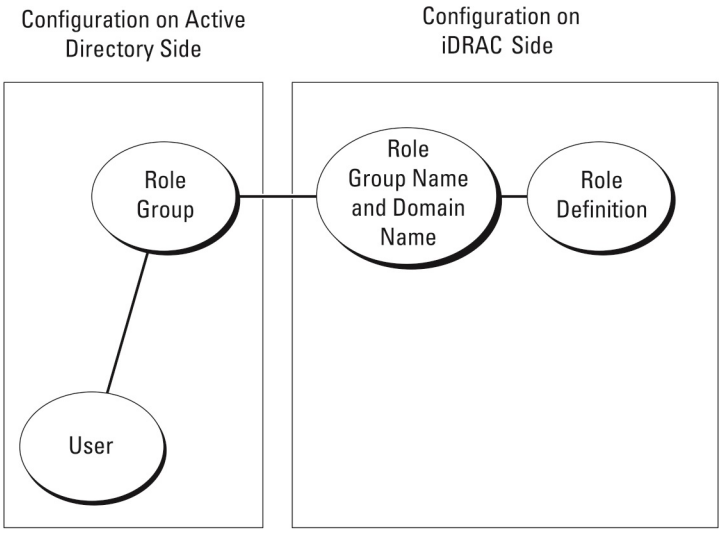


Ilustración 1. Configuración de iDRAC con el esquema estándar de Active Directory

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 otorgar este acceso de usuario a un iDRAC específico, se deben configurar en el iDRAC específico 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 25. Privilegios predeterminados del grupo de funciones

Grupos de funciones	Nivel de privilegio predeterminado	Permisos concedidos	Máscara de bits
Grupo de funciones 1	Ninguna	Iniciar sesión en iDRAC, Configurar iDRAC, Configurar usuarios, Borrar registros, Ejecutar comandos de control del servidor, Acceder a la consola virtual, Acceder a los medios virtuales, Probar alertas, Ejecutar comandos de diagnóstico.	0x000001ff
Grupo de funciones 2	Ninguna	Iniciar sesión en iDRAC, Configurar iDRAC, Ejecutar comandos de control del servidor, Acceder a la consola virtual, Acceder a los medios virtuales, Probar alertas, Ejecutar comandos de diagnóstico.	0x0000001f3
Grupo de funciones 3	Ninguna	Iniciar sesión en la iDRAC	0x00000001
Grupo de funciones 4	Ninguna	Sin permisos asignados	0x00000000
Grupo de funciones 5	Ninguna	Sin permisos asignados	0x00000000

NOTA: Los valores de la máscara de bits se utilizan solo cuando se establece el esquema estándar con RACADM.

Situaciones de dominio único frente a dominio múltiple

Si todos los usuarios de inicio de sesión y los grupos de funciones, incluidos los grupos anidados, se encuentran en el mismo dominio, solo se deben configurar las direcciones de los controladores de dominio en iDRAC. En esta situación de dominio único, se soporta cualquier tipo de grupo.

Si todos los usuarios de inicio de sesión y los grupos de funciones, o cualquiera de los grupos anidados, pertenecen a varios dominios, las direcciones de servidor de catálogo global se deben configurar en iDRAC. En esta situación de varios dominios, todos los grupos de funciones y los grupos anidados, si los hay, deben ser del tipo 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.
- Los ajustes de red de iDRAC están configurados o, en la interfaz web de iDRAC, vaya a **Ajustes de iDRAC > Conectividad > Red > Ajustes comunes** para establecer los ajustes 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 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 intenta conectarse a cada una de las direcciones configuradas una por una hasta que se establece una conexión correctamente. Si la opción esquema estándar está seleccionada, se trata de las direcciones de las controladoras de dominio donde se ubican las cuentas de usuario y los grupos de roles.
- El servidor de catálogo global solo es necesario para el esquema estándar cuando las cuentas de usuario y los grupos de roles se encuentran en dominios diferentes. En el caso de varios dominios, solamente 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 está habilitada la validación de certificados, especifique las direcciones de servidor de la controladora de dominio y el FQDN del catálogo global. Asegúrese de que el DNS esté configurado correctamente en **Overview (Descripción general)** > **iDRAC Settings (Configuración de la 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.

Configuración de Active Directory con esquema estándar mediante la interfaz web de iDRAC

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

1. Los caracteres permitidos en los nombres de usuario y las contraseñas para los recursos compartidos de red están determinados por el tipo de recurso compartido de red. La iDRAC admite caracteres válidos para las credenciales del recurso compartido de red según lo definido por el tipo de recurso compartido, excepto <, > y , (coma).
   Aparecerá la página **Servicios de directorio**.
2. Seleccione la opción **Active Directory de Microsoft** y, a continuación, haga clic en **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 la configuración y administración de Active Directory**.
4. También tiene la opción de habilitar la validación de certificados y cargar el certificado digital de CA firmado que se usa durante el inicio de conexiones SSL cuando se comunica con un servidor de Active Directory (AD). Para ello, se deben especificar las controladoras de dominio y el FQDN del catálogo global. Esto se realiza en los siguientes pasos. Y, por lo tanto, el DNS debe configurarse correctamente en los ajustes de red.
5. Haga clic en **Siguiente**.

   Aparece la página **Paso 2 de 4 de la configuración y administración de Active Directory**.

6. Habilite 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 en iDRAC.

   NOTA: Si está habilitada la validación de certificados, especifique las direcciones de servidor de la controladora de dominio y el FQDN del catálogo global. Asegúrese de que el DNS esté configurado correctamente en **Ajustes de la iDRAC** > **Red**.

7. Haga clic en **Siguiente**. Aparece la página **Paso 3 de 4 de la configuración y administración de Active Directory**.
8. Seleccione **Esquema estándar** y haga clic en Siguiente.

Aparece la página **Paso 4a de 4 de la configuración y administración de Active Directory**.

9. Ingrese la ubicación de los servidores del catálogo global de Active Directory y especifique los grupos de privilegios que se usan para autorizar a los usuarios.
10. Haga clic en un **Grupo de funciones** a fin de configurar la política de autorización de control para los usuarios en el modo de esquema estándar.
    Aparece la página **Paso 4b de 4 de la configuración y administración de Active Directory**.
11. Especifique los privilegios y haga clic en **Aplicar**.

    Se aplican los ajustes y se muestra la página **Paso 4a de 4 de la configuración y administración de Active Directory**.

12. Haga clic en **Finish**. Se configuran los ajustes de Active Directory para el esquema estándar.

Visión general de Active Directory con esquema extendido

El uso de la solución de esquema extendido necesita Active Directory con esquema extendido.

Prácticas recomendadas para el esquema extendido

El esquema extendido utiliza objetos de asociación de Dell para unir iDRAC y permisos. Esto le permite utilizar iDRAC en función de los permisos generales otorgados. La lista de control de acceso (ACL) predeterminada de los objetos de asociación de Dell permite que los administradores de dominio y autónomos administren los permisos y el alcance de los objetos de iDRAC.

De manera predeterminada, los objetos de asociación de Dell no heredan todos los permisos de los objetos primarios de Active Directory. Si habilita la herencia para el objeto de asociación de Dell, los permisos heredados para ese objeto de asociación se otorgan a los usuarios y grupos seleccionados. Esto puede dar lugar a que se proporcionen privilegios no deseados a iDRAC.

Para utilizar el esquema extendido de manera segura, Dell recomienda no habilitar 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 existen en una base de datos distribuida de **atributos** y **clases**. El esquema de Active Directory incluye las reglas que determinan el tipo de datos que se pueden agregar o incluir en la base de datos. La clase de usuario es un ejemplo de una **clase** que se almacena en la base de datos. Algunos ejemplos de atributos de la clase de usuario pueden ser el nombre, el apellido y el número de teléfono del usuario, entre otros. Puede ampliar la base de datos de Active Directory agregando sus propios **atributos** y **clases** únicos para requisitos específicos. Dell amplió el esquema a fin de incluir los cambios necesarios para soportar la autenticación y la autorización de administración remotas mediante Active Directory.

Cada **atributo** o **clase** que se agrega a un esquema de Active Directory se debe definir con un ID único. Para mantener identificadores únicos en todo el sector, Microsoft mantiene una base de datos de identificadores de objetos de Active Directory (OID) para que, cuando las empresas agreguen extensiones al esquema, se pueda garantizar que son únicos y que no entran en conflicto entre sí. Para extender el esquema en Active Directory de Microsoft, Dell recibió OID únicos, extensiones de nombre únicas e ID de atributo vinculados de manera única 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 LinkID de RAC es: `12070 to 12079`

Visión general de las extensiones de esquema de iDRAC

Dell extendió el esquema para incluir una propiedad de **Asociación**, **Dispositivo** y **Privilegio**. La propiedad de **Asociación** se utiliza para vincular a los usuarios o grupos con un conjunto específico de privilegios a uno o más dispositivos iDRAC. Este modelo proporciona al administrador la máxima flexibilidad sobre las diferentes combinaciones de usuarios, privilegios de iDRAC y dispositivos de iDRAC en la red sin mucha complejidad.

Para cada dispositivo iDRAC físico en la red que desee integrar en Active Directory para la autenticación y autorización, cree al menos un objeto de asociación y un objeto de dispositivo iDRAC. Puede crear varios objetos de asociación, y cada objeto de asociación se puede vincular a tantos usuarios, grupos de usuarios u objetos de dispositivo iDRAC como sea necesario. Los usuarios y los grupos de usuarios de iDRAC pueden ser miembros de cualquier dominio de la empresa.

Sin embargo, cada objeto de asociación se puede vincular (o puede vincular usuarios, grupos de usuarios u objetos de dispositivo iDRAC) a un solo objeto de privilegio. Este ejemplo permite que un administrador controle los privilegios de cada usuario en dispositivos iDRAC específicos.

El objeto de dispositivo iDRAC es el vínculo al firmware de iDRAC para consultar a Active Directory con fines de autenticación y autorización. Cuando se agrega iDRAC a la red, el administrador debe configurar iDRAC y su objeto de dispositivo con su nombre de Active Directory para que los usuarios puedan ejecutar la autenticación y la autorización con Active Directory. Además, el administrador debe agregar iDRAC a, al menos, un objeto de asociación para que los usuarios puedan realizar la autenticación.

En la siguiente figura, se ilustra que el objeto de asociación proporciona la conexión necesaria para todo el proceso de autenticación y autorización.

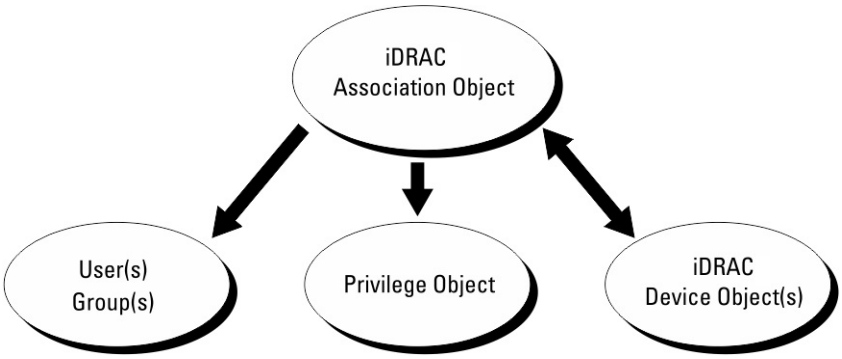


Ilustración 2. Configuración típica de objetos de Active Directory

Puede crear tantos o tan pocos objetos de asociación como sea necesario. Sin embargo, debe crear al menos un objeto de asociación y debe tener un objeto de dispositivo de iDRAC para cada dispositivo de iDRAC en la red que desea integrar en Active Directory para la autenticación y autorización con iDRAC.

El objeto de asociación permite la misma cantidad o tan pocos usuarios o grupos, como también los objetos de dispositivo de iDRAC. Sin embargo, el objeto de asociación solo incluye un objeto de privilegio por objeto de asociación. El objeto de asociación conecta a los usuarios que tienen privilegios en los dispositivos iDRAC.

La extensión de Dell para el complemento MMC de ADUC solo permite asociar el objeto de privilegio y los objetos de iDRAC del mismo dominio con el objeto de asociación. La extensión de Dell no permite que un grupo o un objeto de iDRAC de otros dominios se agreguen como un producto miembro del objeto de asociación.

Cuando se agregan grupos universal desde dominios separados, se crea un objeto de asociación con alcance universal. Los objetos de asociación predeterminados que crea la utilidad Dell Schema Extender son grupos locales de dominio y no funcionan con los grupos universal de otros dominios.

Los usuarios, los grupos de usuarios o los grupos de usuarios anidados de cualquier dominio se pueden agregar al objeto de asociación. Las soluciones de esquema extendido soportan cualquier tipo de grupo de usuarios y cualquier grupo de usuarios anidado en varios dominios permitidos por Active Directory de Microsoft.

Acumulación de privilegios mediante el esquema extendido

El mecanismo de autenticación de esquema extendido soporta la acumulación de privilegios de diferentes objetos de privilegio asociados con el mismo usuario a través de diferentes objetos de asociación. En otras palabras, la autenticación de esquema extendido acumula privilegios para permitir al usuario el superconjunto de todos los privilegios asignados correspondientes a los diferentes objetos de privilegio asociados con el mismo usuario.

En la siguiente figura, se proporciona un ejemplo de acumulación de privilegios mediante el esquema extendido.

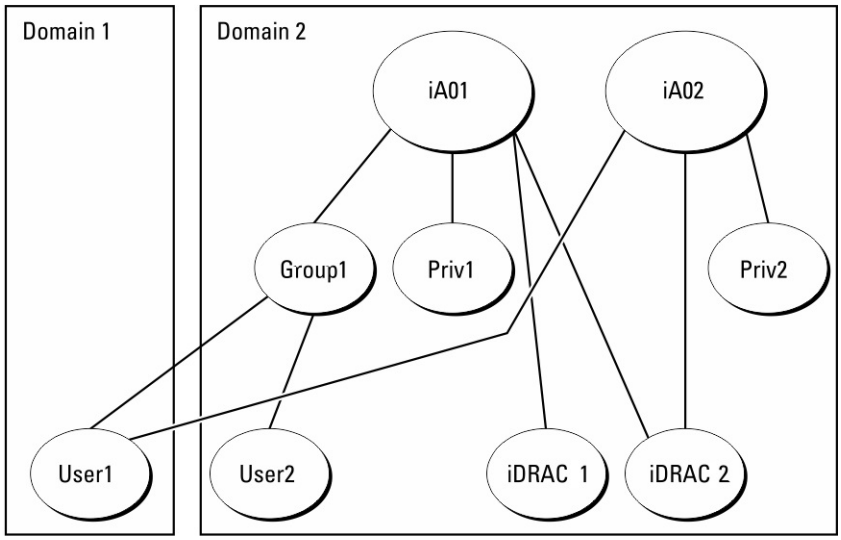


Ilustración 3. Acumulación de privilegios para un usuario

En la figura, se muestran dos objetos de asociación: A01 y A02. El usuario1 está asociado a iDRAC2 a través de ambos objetos de asociación.

La autenticación de esquema extendido acumula privilegios para permitir al usuario el máximo conjunto de privilegios posibles considerando los privilegios asignados de los diferentes objetos de privilegio asociados al mismo usuario.

En este ejemplo, el usuario1 tiene privilegios Priv1 y Priv2 en iDRAC2. El usuario1 tiene privilegios de Priv1 solo en iDRAC1. El usuario2 tiene privilegios de Priv1 tanto en iDRAC1 como en iDRAC2. Además, esta figura muestra que el usuario1 puede estar en un dominio diferente y puede ser miembro de un grupo.

Configuración del esquema extendido de Active Directory

Para configurar Active Directory y acceder a iDRAC:

1. Amplíe el esquema de Active Directory.
2. Amplíe el complemento Usuarios y equipos de Active Directory.
3. Agregue los usuarios de iDRAC y sus privilegios a 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 al esquema de Active Directory una unidad organizacional de Dell, clases y atributos de esquema, y ejemplos de privilegios y objetos de asociación. Antes de extender el esquema, asegúrese de que tiene privilegios de Administrador de esquema en el Maestro de esquema FSMO-Role-Owner del bosque de dominio.

NOTA: La extensión del esquema para este producto es diferente a la de las generaciones anteriores. El esquema anterior no funciona con este producto.

NOTA: La extensión del nuevo esquema no tiene ningún impacto en las versiones anteriores del producto.

Puede extender el esquema utilizando uno de los siguientes métodos:

- Utilidad Dell Schema Extender
- Archivo de script LDIF

Si utiliza el archivo de script LDIF, la unidad organizacional de Dell no se agrega al esquema.

Los archivos LDIF y Dell Schema Extender se encuentran en el DVD **Herramientas y documentación de Dell Systems Management** en los siguientes directorios respectivos:

- DVDdrive `:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\LDIF_Files`

- <DVDdrive>: `\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\Schema Extender`

Para usar los archivos LDIF, consulte las instrucciones en el archivo léame que se incluye en el directorio **LDIF_Files**.

Puede copiar y ejecutar Schema Extender o los archivos LDIF desde cualquier ubicación.

Uso de Dell Schema Extender

PRECAUCIÓN: Dell Schema Extender utiliza el archivo SchemaExtenderOem.ini. Para asegurarse de que la utilidad Dell Schema Extender funcione correctamente, no modifique el nombre de este archivo.

1. En la pantalla **Bienvenida**, haga clic en **Siguiente.**
2. Lea y comprenda la información de precaución y haga clic en **Siguiente**.
3. Seleccione **Usar las credenciales de inicio de sesión actuales** o ingrese un nombre de usuario y una contraseña con derechos de administrador de esquema.
4. Haga clic en **Siguiente** para ejecutar Dell Schema Extender.
5. Haga clic en **Finish**.

   El esquema se extiende. Para verificar la extensión del esquema, use la MMC y el complemento de esquema de Active Directory para verificar que clases y atributos exista. Consulte la documentación de Microsoft para obtener más detalles acerca del uso de MMC y el complemento de esquema de Active Directory.

Clases y atributos

Tabla 26. 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 27. Clase DelliDRACdevice

OID	1.2.840.113556.1.8000.1280.1.7.1.1
Descripción	Representa el dispositivo Dell iDRAC. La iDRAC debe configurarse como delliDRACDevice en Active Directory. Esta configuración permite a la iDRAC enviar consultas del protocolo ligero de acceso a directorios (LDAP) a Active Directory.
Tipo de clase	Clase estructural
SuperClasses	dellProduct
Atributos	dellSchemaVersion dellRacType

Tabla 28. 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 29. Clase dellRAC4Privileges

OID	1.2.840.113556.1.8000.1280.1.1.1.3
Descripción	Define los privilegios (derechos de autorización) de iDRAC
Tipo de clase	Clase auxiliar
SuperClasses	Ninguna opción
Atributos	• dellIsLoginUser • dellIsCardConfigAdmin • dellIsUserConfigAdmin • dellIsLogClearAdmin • dellIsServerResetUser • dellIsConsoleRedirectUser • dellIsVirtualMediaUser • dellIsTestAlertUser • dellIsDebugCommandAdmin

Tabla 30. Clase dellPrivileges

OID	1.2.840.113556.1.8000.1280.1.1.1.4
Descripción	Se utiliza como clase de contenedor de los privilegios de Dell (derechos de autorización).
Tipo de clase	Clase estructural
SuperClasses	Usuario
Atributos	dellRAC4Privileges

Tabla 31. Clase dellProduct

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

Tabla 32. 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 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 objetos dellRacDevice y DelliDRACDevice que pertenecen a esta función. Este atributo es el vínculo de avance para el vínculo de retroceso dellAssociationMembers. Identificación de vínculo: 12070	• 1.2.840.113556.1.8000.1280.1.1.2.2 • Nombre distintivo (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSO
dellIsLoginUser: TRUE si el usuario tiene derechos de inicio de sesión en el dispositivo.	• 1.2.840.113556.1.8000.1280.1.1.2.3 • Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
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)	TRUE

Tabla 32. 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
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)	TRUE
dellIsLogClearAdmin: TRUE si el usuario tiene derechos de borrado de registros en el dispositivo.	• 1.2.840.113556.1.8000.1280.1.1.2.6 • Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsServerResetUser: TRUE si el usuario tiene derechos de restablecimiento del servidor en el dispositivo.	• 1.2.840.113556.1.8000.1280.1.1.2.7 • Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
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)	TRUE
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)	TRUE
dellIsTestAlertUser: TRUE si el usuario tiene derechos de usuario de alerta 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)	TRUE
dellIsDebugCommandAdmin: TRUE si el usuario tiene derechos de administrador de comandos de depuración en el dispositivo.	• 1.2.840.113556.1.8000.1280.1.1.2.11 • Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellSchemaVersion: la versión actual del esquema se utiliza para actualizar el esquema.	• 1.2.840.113556.1.8000.1280.1.1.2.12 • Case Ignore String (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellRacType: este atributo es el tipo de RAC actual para el objeto delliDRACDevice y el vínculo hacia atrás para el vínculo de avance dellAssociationObjectMembers.	• 1.2.840.113556.1.8000.1280.1.1.2.13 • Case Ignore String (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellAssociationMembers: lista de dellAssociationObjectMembers que pertenecen a este producto. Este atributo es el vínculo de retroceso para el 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 la extensión para el complemento de usuarios y equipos de Active Directory

Cuando extiende el esquema en Active Directory, también debe extender el complemento Usuarios y equipos de Active Directory para que el administrador pueda gestionar dispositivos iDRAC, usuarios y grupos de usuarios, asociaciones iDRAC y privilegios iDRAC.

Cuando instala Systems Management Software mediante el uso del DVD **Herramientas y documentación de Dell Systems Management**, puede extender el complemento si selecciona la opción **Complemento de usuario y equipos de Active Directory** durante la instalación. Consulte la Guía de instalación rápida del Dell OpenManage Software para obtener instrucciones adicionales sobre cómo instalar Systems Management Software. Para los sistemas operativos Windows de 64 bits, el instalador del complemento se encuentra en:

<DVDdrive>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_SnapIn64

Para obtener más información sobre el complemento Usuarios y equipos de Active Directory, consulte la documentación de Microsoft.

Adición de usuarios de iDRAC y privilegios en Active Directory

Mediante el complemento Usuarios y equipos de Active Directory ampliado de Dell, puede añadir usuarios y privilegios de iDRAC creando objetos de dispositivo, asociación y privilegio. Para agregar cada objeto, realice lo siguiente:

- Cree un objeto de dispositivo iDRAC
- Cree un objeto de privilegio
- Cree un objeto de asociación
- Agregue objetos a un objeto de asociación

Creación de un objeto de dispositivo iDRAC

Para crear un objeto de dispositivo iDRAC:

1. En la ventana de MMC **Raíz de la consola**, haga clic con el botón secundario en un contenedor.
2. Seleccione **Nuevo** > **objeto de administración remota de Dell Avanzado**.
   Se abre la ventana **Nuevo objeto**.
3. Introduzca un nombre para el nuevo objeto. El nombre debe ser idéntico al nombre de iDRAC que ingrese durante la configuración de 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** > **objeto de administración remota de Dell Avanzado**.
   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 pestaña **Privilegios de administración remota** y asigne los privilegios para el usuario o grupo.

Cómo crear un objeto de asociación

Para crear un objeto de asociación:

NOTA: El objeto de asociación de iDRAC se deriva del grupo y su alcance se establece en Dominio local.

1. En la ventana **Raíz de consola** (MMC), haga clic con el botón derecho del mouse en un contenedor.
2. Seleccione **Nuevo** > **objeto de administración remota de Dell Avanzado**.
   Se abre la ventana **Nuevo certificado**.
3. Ingrese un nombre para el objeto nuevo y seleccione **Objeto de asociación**.
4. Seleccione el ámbito para el **Objeto de asociación**.
5. Proporcione privilegio de acceso a Usuarios autentificados para acceder al objeto de asociación creado.

Otorgamiento de privilegios de acceso de usuarios para objetos de asociación

Para proporcionar privilegios de acceso a usuarios autentificados a fin de acceder al objeto de asociación creado:

1. Vaya a **Herramientas administrativas** > **Editar ADSI**. Aparece la ventana **Editar ADSI**.
2. En el panel derecho, desplácese hasta el objeto de asociación creado, haga clic con el botón secundario y seleccione **Propiedades**.
3. En el panel **Acción**, haga clic en **Agregar**.

4. Escriba `Authenticated Users`, haga clic en **Verificar nombres** y haga clic en **Aceptar**. Los usuarios autenticados se agregan a la lista de **Grupos y nombres de usuario**.
5. Haga clic en **Aceptar**.

Agregación de objetos a un objeto de asociación

En la ventana **Propiedades del objeto de asociación**, puede asociar usuarios o grupos de usuarios, objetos de privilegio y dispositivos iDRAC o grupos de dispositivos iDRAC.

Puede añadir grupos de usuarios y dispositivos iDRAC.

Adición de privilegios

Para agregar un privilegio:

Haga clic en la pestaña **Objeto de privilegio** para agregar el objeto de privilegio a la asociación que define los privilegios del usuario o del grupo de usuarios cuando se autentica un dispositivo iDRAC. Solo se puede agregar un objeto de privilegio a un objeto de asociación.

1. Seleccione la pestaña **Objeto de privilegios** y haga clic en **Agregar**.
2. Ingrese el nombre del objeto con privilegio y haga clic en **Aceptar**.
3. Haga clic en la pestaña **Objeto de privilegio** para agregar el objeto de privilegio a la asociación que define los privilegios del usuario o del grupo de usuarios cuando se autentica un dispositivo iDRAC. Solo se puede agregar un objeto de privilegio a un objeto de asociación.

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. Ingrese el nombre del usuario o grupo de usuarios y haga clic en **Aceptar**.

Adición de dispositivos iDRAC o grupos de dispositivos iDRAC

Para agregar dispositivos iDRAC o grupos de dispositivos iDRAC:

1. Seleccione la pestaña **Productos** y haga clic en **Agregar**.
2. Ingrese los dispositivos iDRAC o el nombre del grupo de dispositivos iDRAC y haga clic en **Aceptar**.
3. En la ventana **Propiedades**, haga clic en **Aplicar** y, a continuación, en **Aceptar**.
4. Haga clic en la pestaña **Productos** para agregar un dispositivo iDRAC conectado a la red que está disponible para los usuarios o grupos de usuarios definidos. Puede agregar varios dispositivos iDRAC a un objeto de asociación.

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 intenta conectarse a cada una de las direcciones configuradas una por una hasta que se establece una conexión correctamente. Con el esquema extendido, estas son las direcciones FQDN o IP de las controladoras de dominio donde se encuentra este dispositivo iDRAC.
- Para desactivar la validación del certificado durante el protocolo de enlace de SSL, utilice el siguiente comando:

  ```
  racadm set iDRAC.ActiveDirectory.CertValidationEnable 0
  ```

  En este caso, no tiene que cargar un certificado de CA.
- Para aplicar la validación de certificado durante el protocolo de enlace SSL (opcional):

  ```
  racadm set iDRAC.ActiveDirectory.CertValidationEnable 1
  ```

  En este caso, deberá cargar un certificado de la entidad emisora con el siguiente comando:

  ```
  racadm sslcertupload -t 0x2 -f <ADS root CA certificate>
  ```

  NOTA: Si está habilitada la validación de certificados, especifique las direcciones de servidor de la controladora de dominio y el FQDN. Asegúrese de que el DNS esté configurado correctamente en **Configuración de la iDRAC** > **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.

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 la iDRAC, vaya a **Ajustes de la iDRAC** > **Usuarios** > **Servicios de directorio** > **Active Directory de Microsoft**. Haga clic en **Editar**
   Aparece la página **Paso 1 de 4 de la configuración y administración de Active Directory**.
2. También tiene la opción de habilitar la validación de certificados y cargar el certificado digital de CA firmado que se usa durante el inicio de conexiones SSL cuando se comunica con un servidor de Active Directory (AD).
3. Haga clic en **Siguiente**.
   Aparece la página **Paso 2 de 4 de la configuración y administración de Active Directory**.
4. Especifique la información de ubicación acerca de los servidores de Active Directory (AD) y las cuentas de usuario. Además, especifique el tiempo que iDRAC debe esperar las respuestas de AD durante el proceso de inicio de sesión.

NOTA:

- Si está habilitada la validación de certificados, especifique las direcciones de servidor de la controladora de dominio y el FQDN. Asegúrese de que el DNS esté configurado correctamente en **Ajustes de la iDRAC** > **Red**
- Si el usuario y los objetos de iDRAC se encuentran en dominios diferentes, no seleccione la opción **Dominio de usuario en inicio de sesión**. En su lugar, seleccione la opción **Especificar un dominio** e ingrese el nombre de dominio en el que el objeto de iDRAC está disponible.

5. Haga clic en **Siguiente**. Aparece la página **Paso 3 de 4 de la configuración y administración de Active Directory**.
6. Seleccione **Esquema extendido** y haga clic en **Siguiente**.
   Aparece la página **Paso 4 de 4 de la configuración y administración de Active Directory**.
7. Ingrese el nombre y la ubicación del objeto del dispositivo iDRAC en Active Directory (AD) y haga clic en **Finalizar**.
   Se configuran los ajustes de Active Directory para el modo de esquema extendido.

Prueba de los ajustes de Active Directory

Puede probar los ajustes de Active Directory para verificar si la configuración es correcta o diagnosticar el problema con un inicio de sesión fallido de Active Directory.

Prueba de los ajustes de Active Directory mediante una interfaz web de iDRAC

Para probar la configuración de Active Directory:

1. En la interfaz web de la iDRAC, vaya a **Ajustes de la iDRAC** > **Usuarios** > **Servicios de directorio** > **Active Directory de Microsoft** y haga clic en **Probar**.
   Se muestra la página **Probar los ajustes de Active Directory**.
2. Haga clic en **Test**.
3. Ingrese el nombre (por ejemplo, **username@domain.com**) y la contraseña del usuario de prueba, y haga clic en **Iniciar prueba**.
   Aparecen los resultados detallados de la prueba y el registro de esta.

   Si hay una falla en algún paso, examine los detalles en el registro de prueba para identificar el problema y una posible solución.

   NOTA: Al realizar la prueba de los ajustes de Active Directory con la opción Habilitar la validación de certificados seleccionada, la iDRAC necesita que el FQDN (y no una dirección IP) identifique el servidor de Active Directory. Si al servidor de Active Directory lo identifica una dirección IP, fallará la validación del certificado, porque la iDRAC no puede comunicarse con el servidor Active Directory.

Configuración de usuarios LDAP genéricos

iDRAC proporciona una solución genérica para soportar la autenticación basada en el protocolo ligero de acceso a directorios (LDAP). Esta característica no requiere ninguna extensión de esquema en los servicios de directorio.

Para que la implementación de LDAP de iDRAC sea genérica, se utiliza la relación en común entre los diferentes servicios de directorio para agrupar usuarios y, luego, asignar la relación entre usuarios y grupos. La acción específica del servicio de directorio es el esquema. Por ejemplo, pueden tener nombres de atributo diferentes para el grupo, el usuario y el enlace entre el usuario y el grupo. Estas acciones se pueden configurar en iDRAC.

NOTA: Se admite StartTLS en el puerto 389. De manera predeterminada, LDAPS está configurado en el puerto 636. El protocolo de conexión se puede volver a configurar en StartTLS mediante el comando `racadm set iDRAC.LDAP.Connection StartTLS` de RACADM o Redfish.

NOTA: Las funciones de autentificación de dos factores (TFA) basada en tarjeta inteligente y Single Sign On (SSO) no están soportadas en el servicio de directorio de LDAP genérico.

Configuración del servicio directorio LDAP genérico mediante RACADM

Para configurar el servicio de directorio LDAP, utilice los objetos en los grupos `iDRAC.LDAP` y `iDRAC.LDAPRole`.

Para obtener más información, consulte Guía de la CLI RACADM de Integrated Dell Remote Access Controller.

Configuración de Directory Service de LDAP genérico mediante la interfaz web de iDRAC

Para configurar el servicio de directorio 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 **Ajustes de la iDRAC** > **Usuarios** > **Servicios de directorio** > **Servicio de directorio de LDAP genérico** y haga clic en **Editar**.
   En la página **Configuración y administración de LDAP genérico: Paso 1 de 3**, se muestran los ajustes actuales del LDAP genérico.
2. También tiene la opción de activar la validación de certificados y cargar el certificado digital que se usa durante el inicio de conexiones SSL cuando se comunica con un servidor LDAP genérico.
3. Haga clic en **Siguiente**.
   Aparece la página **Configuración y administración de LDAP genérico: Paso 2 de 3**.
4. Active la autenticación de LDAP genérico y especifique la información de ubicación sobre los servidores LDAP genéricos y las cuentas de usuario.

   NOTA: Si la validación del certificado está activada, especifique el FQDN del servidor LDAP y asegúrese de que DNS esté configurado correctamente en **Ajustes de iDRAC** > **Red**.

   NOTA: En esta versión, no se admite el grupo anidado. El firmware busca el miembro directo del grupo para que coincida con el DN del usuario. Además, soporta un solo dominio. No soporta el dominio cruzado.

5. Haga clic en **Siguiente**.
   Aparece la página **Configuración y administración de LDAP genérico: Paso 3a de 3**.
6. Haga clic en **Grupo de funciones**.
   Aparece la página **Configuración y administración de LDAP genérico: Paso 3b de 3**.
7. Especifique el nombre distintivo del grupo, los privilegios asociados con el grupo y haga clic en **Aplicar**.

   NOTA: Si utiliza Novell eDirectory y si ha utilizado estos caracteres (# [hash], " [comillas dobles], ; [punto y coma], > [mayor que], , [coma] o < [menor que]) para el nombre de DN del grupo, se deben eliminar.

   Los ajustes del grupo de funciones se guardan. En la página **Configuración y administración de LDAP genérico: Paso 3a de 3**, se muestran los ajustes del grupo de funciones.
8. Si desea configurar grupos de funciones adicionales, repita los pasos 7 y 8.
9. Haga clic en **Finish**. El servicio de directorio LDAP genérico está configurado.

Probar los ajustes del servicio de directorio LDAP

Puede probar los ajustes del servicio de directorio LDAP para verificar si la configuración es correcta o diagnosticar el problema con un inicio de sesión fallido de LDAP.

Prueba de la configuración del servicio de directorio de LDAP mediante una interfaz web de iDRAC

Para probar la configuración del servicio de directorio LDAP:

1. En la interfaz web de iDRAC, vaya a **Ajustes de iDRAC** > **Usuarios** > **Servicios de directorio** > **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 **Test**.
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.

12

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. Cuando habilita el modo de bloqueo del sistema, se bloquea la actualización de firmware de las tarjetas I/O de otros fabricantes mediante las herramientas del proveedor.

El modo de bloqueo del sistema solo está disponible para los clientes con licencia de la empresa.

NOTA: El bloqueo mejorado para NIC solo incluye el bloqueo del firmware a fin de evitar las actualizaciones de firmware. 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
- Perfil de configuración del sistema (SCP)
- 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 una 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 el modo de bloqueo, pero la configuración de recursos compartidos de archivos remotos no se encuentra habilitada.

NOTA: Las interfaces como OMSA, SysCfg y USC solo pueden comprobar la configuración, no pueden modificarla.

NOTA: Cuando se habilita el modo de bloqueo, los usuarios no pueden configurar ningún ajuste de alerta. Sin embargo, pueden activar un correo electrónico de prueba.

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, existe una opción de control de arranque disponible en el menú de vConsole, que no surte efecto cuando iDRAC se encuentra en el modo de bloqueo.

Tabla 33. Elementos afectados por el modo de bloqueo

Deshabilitado	Permanece funcional
• Eliminación de licencias • Actualizaciones de DUP • Importación de SCP • Restablecer a los valores predeterminados • 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 tarjeta madre • Ejecución de diagnósticos • Operaciones modulares (FlexAddress o dirección asignada de forma remota)

Tabla 33. Elementos afectados por el modo de bloqueo

Deshabilitado	Permanece funcional

• BIOS (la configuración de F2 es de solo lectura)
• Selección de tarjetas de red.
• iLKM/SEKM
	• Todas las herramientas de proveedores que tengan acceso directo al dispositivo (esto excluye las NIC seleccionadas)
	• 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-N1
	• Configuración del ISM (habilitación de la BMC en el sistema operativo, comando ping al guardián, nombre del sistema operativo, versión del sistema operativo)

NOTA: Cuando se habilita el modo de bloqueo, la opción de inicio de sesión de OpenID Connect no se muestra en la página de inicio de sesión de iDRAC.

13

Configuración de iDRAC para inicio de sesión único o 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:

Requisitos para el inicio de sesión único de Active Directory o el inicio de sesión mediante tarjeta inteligente

Los requisitos para los SSO o con tarjeta inteligente basados en Active Directory son los siguientes:

- Sincronice la hora de la iDRAC con la hora de la controladora de dominio de Active Directory. De lo contrario, la autenticación Kerberos en la iDRAC genera un error. Puede utilizar la zona horaria y la función de NTP para sincronizar la hora. Para ello, consulte Configuración de zona horaria y NTP.
- Registre iDRAC como una computadora en el dominio raíz de Active Directory.

  NOTA: La iDRAC no soporta usuarios con tarjetas inteligentes de verificación de identidad personal (PIV) o tarjeta de acceso común (CAC) en un dominio secundario o subdominio de un bosque o recopilación de dominios. Para superar esta limitación, se recomienda implementar todos los usuarios de tarjetas inteligentes en el dominio raíz en lugar de los dominios secundarios del bosque.

- Genere un archivo keytab con la herramienta ktpass.
- A fin de habilitar Single Sign On en el esquema extendido, asegúrese de que la opción **Confiar en este usuario para la delegación a cualquier servicio (solo Kerberos)** esté seleccionada en la pestaña **Delegación** del usuario de keytab. Esta pestaña solo está disponible después de crear el archivo de keytab mediante la utilidad ktpass.
- Configure el navegador para habilitar el SSO.
- Cree los objetos de Active Directory y proporcione los privilegios necesarios.
- Para el SSO, configure la zona de búsqueda inversa en los servidores DNS en la subred donde reside iDRAC.

  NOTA: Si el nombre de host no coincide con la búsqueda inversa de DNS, la autenticación de Kerberos falla.

- Configure el navegador para activar el inicio de sesión SSO. Para obtener más información, consulte Single Sign-On.

  NOTA: Google Chrome y Safari no soportan Active Directory para el 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 la 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. Proporcione un **Nombre de dominio de DNS** válido.
6. Verifique que la configuración de DNS de 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 SSO en iDRAC para usuarios de Active Directory

Antes de configurar iDRAC para el SSO de Active Directory, asegúrese de haber completado todos los requisitos.

Puede configurar iDRAC para el 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.

Generar el 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, lo que permite establecer 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 con la herramienta ktpass:

1. Ejecute la utilidad **ktpass** en la controladora de dominio (servidor de Active Directory) donde desea asignar iDRAC a una cuenta de usuario en Active Directory.
2. Utilice el siguiente comando ktpass 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 archivo keytab.

NOTA: Si encuentra algún problema con el usuario de iDRAC para el cual creó el archivo keytab, cree un usuario y un archivo keytab nuevo. Si se vuelve a ejecutar el mismo archivo keytab que se creó inicialmente, este no se configura correctamente.

Configuración del SSO en iDRAC para usuarios de Active Directory mediante la interfaz web

Para configurar iDRAC en un acceso de SSO de Active Directory:

NOTA: Para obtener información acerca de las opciones, consulte la **Ayuda en línea de la 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. Durante la configuración de Active Directory para configurar una cuenta de usuario basada en el esquema estándar o el esquema extendido, realice los dos pasos adicionales siguientes a fin de configurar el SSO:
   - Cargue el archivo keytab en la página **Paso 1 de 4 de la configuración y administración de Active Directory**.
   - Seleccione la opción **Habilitar Single Sign On** en la página **Paso 2 de 4 de la configuración y administración de Active Directory**.

Configuración del SSO en iDRAC para usuarios de Active Directory mediante RACADM

Para habilitar el SSO, complete los pasos a fin de configurar Active Directory y ejecute el siguiente comando:

```
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.

Habilitación o deshabilitación del inicio de sesión mediante tarjeta inteligente

Antes de habilitar o deshabilitar el inicio de sesión mediante tarjeta inteligente para iDRAC, asegúrese de que:

- Configuró los permisos de iDRAC.
- Se completó la configuración de usuario local de iDRAC o la configuración de usuario de Active Directory con los certificados correspondientes.

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.

Habilitación o deshabilitación del inicio de sesión mediante tarjeta inteligente con la interfaz web

Para habilitar o deshabilitar la función de inicio de sesión mediante tarjeta inteligente:

1. En la interfaz web de iDRAC, vaya a **Ajustes de iDRAC** > **Usuarios** > **Tarjeta inteligente**.
   Aparecerá la página **Tarjeta inteligente**.
2. En el menú desplegable **Configurar inicio de sesión mediante tarjeta inteligente**, seleccione **Habilitado** para habilitar el inicio de sesión mediante tarjeta inteligente o seleccione **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 cualquier intento posterior de inicio de sesión con la interfaz web de iDRAC.

Habilitación o deshabilitación del inicio de sesión con tarjeta inteligente mediante RACADM

Para habilitar el inicio de sesión mediante tarjeta inteligente, utilice el comando con objetos en el grupo `setiDRAC.SmartCard`.

Para obtener más información, consulte la *Guía de CLI de RACADM de Integrated Dell Remote Access Controller*.

Habilitación o deshabilitación del inicio de sesión con tarjeta inteligente mediante la utilidad de configuración de iDRAC

Para habilitar o deshabilitar 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 Ajustes de iDRAC**.
2. Seleccione **Habilitado** para habilitar la sesión mediante tarjeta inteligente. De lo contrario, seleccione **Desactivado**. Para obtener más información acerca de estas opciones, consulte la **Ayuda en línea de la utilidad de configuración de iDRAC**.
3. Haga clic en **Atrás**, en **Terminar** y, a continuación, en **Sí**.
   La característica de inicio de sesión mediante tarjeta inteligente se habilita o deshabilita según la selección.

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 completado los requisitos necesarios.

Para configurar iDRAC para el inicio de sesión con tarjeta inteligente:

1. En la interfaz web de iDRAC, mientras configura Active Directory para configurar una cuenta de usuario basada en el esquema estándar o el esquema extendido, en la página **Paso 1 de 4 de la configuración y administración de Active Directory**:
   - Habilite la validación de certificados.
   - Cargue un certificado de confianza firmado por la CA.
   - Cargar el archivo Keytab.

2. Habilite el inicio de sesión mediante tarjeta inteligente. Para obtener información acerca de las opciones, consulte la **Ayuda en línea de la iDRAC**.

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

Para configurar el usuario local de iDRAC para el 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. Habilite 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 exporte en formato Base64. Los certificados SHA-2 también están soportados.

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 RACADM de Integrated Dell Remote Access Controller.

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 la tarjeta inteligente

Antes de cargar el certificado de CA, asegúrese de contar con un certificado firmado por una CA.

Carga del certificado de CA de confianza para tarjeta inteligente mediante la interfaz web

Para cargar un certificado de CA de confianza para el inicio de sesión mediante tarjeta inteligente:

1. En la interfaz web de iDRAC, vaya a **Ajustes de iDRAC** > **Red** > **Autenticación de usuarios** > **Usuarios locales**.
   Se muestra la página **Usuarios**.
2. En la columna **ID del usuario**, haga clic en un número de ID de usuario.
   Aparece la página **Menú principal de usuarios**.
3. En **Ajustes de la tarjeta inteligente**, seleccione **Cargar certificado de CA de confianza** y haga clic en **Siguiente**.
   Se muestra 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 una tarjeta inteligente mediante RACADM

Para cargar un certificado de CA de confianza para el inicio de sesión con tarjeta inteligente, utilice el objeto **usercertupload**. Para obtener más información, consulte la *Guía de CLI de RACADM de Integrated Dell Remote Access Controller*.

Inicio de sesión mediante la tarjeta inteligente

NOTA: El inicio de sesión mediante tarjeta inteligente es soportado en Edge/Chrome y Firefox.

NOTA: El inicio de sesión mediante tarjeta inteligente solo es soportado en la versión 1.2 de TLS.

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.

14

Configuración de iDRAC para enviar alertas

Es posible configurar alertas y acciones para determinados sucesos que se producen en el sistema administrado. Un suceso se produce cuando el estado de un componente del sistema es mayor que la condición definida previamente. Si un evento coincide con un filtro de eventos, y este filtro se configuró para que genere una alerta (correo electrónico, captura SNMP, alerta IPMI, registros del sistema remoto, evento de Redfish o eventos de WS), se envía una alerta a uno o más destinos configurados. Si el mismo filtro de sucesos 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.

NOTA: En caso de que una actualización requiera el restablecimiento/reinicio de la iDRAC, o si se reinicia la iDRAC, se recomienda verificar si la iDRAC está completamente lista; para ello, espere unos segundos hasta un máximo de cinco minutos antes de usar cualquier otro comando.

Temas:

Habilitación o deshabilitación de alertas

Para enviar una alerta a destinos configurados o realizar una acción de evento, debe habilitar la opción de alerta global. Esta propiedad reemplaza las acciones de eventos o alertas individuales configuradas.

Habilitación o deshabilitación de las alertas mediante la interfaz web

Para habilitar o deshabilitar la generación de alertas:

1. En la interfaz web de iDRAC, vaya a **Configuración** > **Configuración del sistema** > **Configuración de alertas**.
   Se muestra la página **Alertas**.
2. En la sección **Alertas**:
   - Seleccione **Habilitar** para habilitar la generación de alertas o realizar una acción de evento.
   - Seleccione **Deshabilitar** para deshabilitar la generación de alertas o una acción de evento.
3. Haga clic en **Aplicar** para guardar el ajuste.

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.
   Todas las alertas configuradas se muestran en **Resumen de configuración de alertas**.

NOTA: Debe seleccionar al menos un tipo de categoría, gravedad y destino para aplicar la configuración.

NOTA: Después de configurar las alertas mediante la pestaña **Alertas rápidas**, y cuando el usuario ingresa a la pestaña **Configuración de alertas**, las alertas configuradas no se encuentran habilitadas en las categorías de alerta correspondientes. Para habilitar las categorías de alerta correspondientes:

1. Seleccione una de las otras pestañas de categoría (**Estado del sistema**, **Auditoría**, **Actualizaciones** y **Configuración**) en la página **Configuración de alertas**.
2. Revierta a la categoría que se usó originalmente para la configuración de alertas.

Activación o desactivación de alertas mediante RACADM

Use el siguiente comando:

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

n=0: deshabilitado

n=1: habilitado

Habilitación o deshabilitación de alertas mediante la utilidad de configuración de iDRAC

Para habilitar o deshabilitar la generación de alertas o acciones de eventos:

1. En la utilidad de configuración de iDRAC, vaya a **Alertas**.
   Se muestra la página **Alertas de Ajustes de iDRAC**.
2. En **Eventos de plataforma**, seleccione **Habilitado** para habilitar la generación de alertas o la acción de eventos. De lo contrario, seleccione **Desactivado**. Para obtener más información acerca de estas opciones, consulte la **Ayuda en línea de la utilidad de configuración de iDRAC**.
3. Haga clic en **Atrás**, en **Terminar** y, a continuación, en **Sí**.
   Se configuran los ajustes de alertas.

Configuración de alertas de eventos

Puede establecer alertas de eventos, como alertas por correo electrónico, alertas IPMI, capturas SNMP, registros del sistema remoto, registros del sistema operativo y eventos de WS para que se envíen a los destinos configurados.

Configuración de alertas de eventos mediante la interfaz web

Para configurar una alerta de eventos 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**.
   Se guarda el ajuste.
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 monitorean los componentes del sistema, consulte la **Guía de referencia de mensajes de errores y eventos de Dell** en iDRACmanuals

Configuración de alertas de eventos mediante RACADM

Para configurar la alerta de evento, utilice el comando **eventfilters**. Para obtener más información, consulte Guía de la CLI RACADM de Integrated Dell Remote Access Controller.

Configuración de eventos de periodicidad de alertas

Puede 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 la 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 hay periodicidad del evento.

NOTA: Debe tener el privilegio Configurar iDRAC para establecer el valor de recurrencia de la alerta.

Configuración de eventos 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 RACADM de Integrated Dell Remote Access Controller.

Configuración de sucesos de periodicidad de alertas mediante la interfaz web de iDRAC

Para establecer el valor de periodicidad de las alertas:

1. En la interfaz web de iDRAC, vaya a **Configuración** > **Ajustes del sistema** > **Periodicidad de la alerta**.
2. En la columna **Periodicidad**, ingrese el valor de frecuencia de alertas para los tipos de categoría, alerta y gravedad necesarios.
   Para obtener más información, consulte la **Ayuda en línea de iDRAC**.
3. Haga clic en **Aplicar**.
   Se guardan los ajustes de periodicidad de alertas.

Configuración de acciones de eventos

Puede configurar acciones de eventos, como realizar un reinicio, ciclo de apagado y encendido, apagado o no realizar ninguna acción en el sistema.

Configuración de acciones de eventos mediante la interfaz web

Para configurar una acción de evento:

1. En la interfaz web de la iDRAC, vaya a **Configuración** > **Ajustes del sistema** > **Configuración de alertas y del registro del sistema remoto**.
2. En el menú desplegable **Acciones**, para cada evento, seleccione una acción:
   - Reiniciar
   - Ciclo de encendido
   - Apagado
   - Sin acción
3. Haga clic en **Aplicar**.
   Se guarda el ajuste.

Configuración de acciones de eventos mediante RACADM

Para configurar acciones del evento, utilice el comando `eventfilters`. Para obtener más información, consulte Guía de la CLI RACADM de Integrated Dell Remote Access Controller.

Configuración de los ajustes de alertas por correo electrónico, capturas SNMP o capturas IPMI

La estación de administración utiliza capturas del Protocolo simple de administración de red (SNMP) y de la Interfaz de administración de plataforma inteligente (IPMI) para recibir datos de iDRAC. Para 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 ocurrir. Por ejemplo, las capturas de eventos pueden ayudar a una estación de administración con el equilibrio de carga entre nodos o mediante la emisión de una alerta si se produce una falla de autenticación. Se soportan los formatos SNMP v1, v2 y v3.

Puede configurar los destinos de alerta IPv4 e IPv6, los ajustes del correo electrónico y los ajustes del servidor SMTP, y probar estos ajustes. También puede especificar el usuario SNMP v3 al que desea enviar las capturas SNMP.

Antes de configurar los ajustes de correo electrónico, SNMP o captura IPMI, asegúrese de lo siguiente:

- Tiene permiso de configuración de RAC.
- Ha configurado los filtros de eventos.

Configuración de destinos de alertas 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 de Dell OpenManage* disponible en la página Manuales de OpenManage..

Configuración de los destinos de alertas IP mediante la interfaz web

Para configurar los ajustes de destinos de alerta mediante la interfaz web:

1. En la interfaz web de iDRAC, vaya a **Configuración** > **Ajustes del sistema** > **Ajustes de SNMP y correo electrónico**.
2. Seleccione la opción **Estado** para habilitar un destino de alerta (dirección IPv4, dirección IPv6 o nombre de dominio completo [FQDN]) para recibir las traps.

   Puede 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. Ingrese la cadena de comunidad SNMP de iDRAC (aplicable solo para SNMPv1 y v2) y el número de puerto de alerta de 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 utilizará en una captura de alerta de Protocolo simple de administración de red (SNMP) enviada desde iDRAC. Asegúrese de que la cadena de comunidad de destino sea la misma que la cadena de comunidad de iDRAC. El valor predeterminado es Público.

5. Para probar si la dirección IP está recibiendo las capturas IPMI o SNMP, haga clic en **Enviar** en **Probar captura IPMI** y **Probar captura SNMP** respectivamente.
6. Haga clic en **Aplicar**.
   Se configuran los destinos de alerta.
7. En la sección **Formato de captura SNMP**, seleccione la versión del protocolo que se utilizará para enviar las capturas en los destinos trap: **SNMP v1**, **SNMP v2** o **SNMP v3** y haga clic en **Aplicar**.

   NOTA: La opción **Formato de captura SNMP** se aplica solo a captura de SNMP y no a captura de IPMI. Las capturas IPMI siempre se envían en formato SNMP v1 y no se basan en la opción **Formato de captura SNMP** configurada.

   Se configura el formato de captura SNMP.

Configuración de destinos de alerta de IP mediante RACADM

Para configurar los ajustes de alerta de captura:

1. Para habilitar las 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	Deshabilite la captura Habilite la captura

2. Para configurar la dirección de destino trap:

```
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 comunidad SNMP.

4. Para configurar el destino de SNMP:
   - Establezca el destino trap de SNMP para SNMPv3:

     ```
     racadm set idrac.SNMP.Alert.<index>.DestAddr <IP address>
     ```

   - Configure usuarios SNMPv3 para destinos de captura:

     ```
     racadm set idrac.SNMP.Alert.<index>.SNMPv3Username <user_name>
     ```

   - Habilite SNMPv3 para un usuario:

     ```
     racadm set idrac.users.<index>.SNMPv3Enable Enabled
     ```

5. Para probar la captura, si es necesario:

```
racadm testtrap -i <index>
```

Para obtener más información, consulte Guía de la CLI RACADM de Integrated Dell Remote Access Controller.

Configuración de los destinos de alertas IP mediante la utilidad de configuración de iDRAC

Puede configurar destinos de alerta (IPv4, IPv6 o FQDN) mediante la utilidad de configuración de iDRAC. Para hacerlo:

1. En la **utilidad de configuración de iDRAC**, vaya a **Alertas**.
   Se muestra la página **Alertas de Ajustes de iDRAC**.
2. En **Ajustes de captura**, habilite las direcciones IP para recibir las capturas e ingrese las direcciones de destino IPv4, IPv6 o FQDN. Puede especificar hasta ocho direcciones.
3. Introduzca el nombre de la cadena de comunidad.
   Para obtener información acerca de las opciones, consulte la **Ayuda en línea de la utilidad de configuración de iDRAC**.
4. Haga clic en **Atrás**, en **Terminar** y, a continuación, en **Sí**.
   Se configuran 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 la 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 SMTP (correo electrónico), proporcione los siguientes detalles:
   - Dirección IP de servidores de correo electrónico SMTP o nombre FQDN/DNS
   - Dirección personalizada del remitente: este campo contiene las siguientes opciones:
     - **Predeterminado**: el campo de dirección no se puede editar.
     - **Personalizado**: puede ingresar el ID de correo electrónico en el cual recibir las alertas de correo electrónico.
   - Prefijo personalizado del asunto del mensaje: este campo contiene las siguientes opciones:
     - **Predeterminado**: el mensaje predeterminado no se puede editar.
     - **Personalizado**: puede elegir el mensaje que desea que aparezca en la línea de **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 conexión: cuando no existe un servidor de correo electrónico en las instalaciones, puede usar servidores de correo electrónico basados en la nube o retransmisores SMTP. Para configurar un servidor de correo electrónico en la nube, puede establecer esta característica 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 es una función con licencia y no está disponible en la licencia de la iDRAC Core.
- Debe tener el privilegio Configurar iDRAC para usar esta característica.

- 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 ajustes de alertas por correo electrónico mediante RACADM

1. Para habilitar la alerta 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**	Deshabilita alertas por correo electrónico. Habilita alertas por correo electrónico.

2. Para configurar los ajustes del 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 de correo electrónico configurada, si es 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 RACADM de Integrated Dell Remote Access Controller.

Configuración de los ajustes de la dirección de correo electrónico del servidor SMTP

Debe configurar la dirección del servidor SMTP para que las alertas por correo electrónico se envíen a destinos especificados.

Configuración de los ajustes de la dirección de servidor de correo electrónico SMTP mediante la interfaz web de iDRAC

Para configurar la dirección del servidor SMTP:

1. En la interfaz web de iDRAC, vaya a **Configuración** > **Ajustes del sistema** > **Configuración de alertas** > **SNMP (configuración de correo electrónico)**.
2. Ingrese la dirección IP válida o el nombre de dominio completo (FQDN) del servidor SMTP que se utilizará en la configuración.
3. Seleccione la opción **Habilitar autenticación** y, a continuación, proporcione el nombre de usuario y la contraseña (de un usuario que tiene 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 configuran los ajustes 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 eventos de Redfish

El protocolo de eventos de Redfish se utiliza para que un servicio de cliente (suscriptor) registre el interés (suscripción) en un servidor (fuente de eventos) a fin de recibir mensajes que contengan los sucesos de Redfish (notificaciones o mensajes de eventos). Los clientes interesados en recibir los mensajes de eventos de Redfish pueden suscribirse con iDRAC y recibir eventos relacionados con el trabajo de Lifecycle Controller.

Configuración del registro de sistema remoto

Puede enviar registros de Lifecycle a un sistema remoto. Antes de hacerlo, asegúrese de lo siguiente:

- Hay conectividad de red entre iDRAC y el sistema remoto.
- El sistema remoto e iDRAC se encuentran en la misma red.

NOTA: Esta característica está disponible para las licencias iDRAC Enterprise y Datacenter.

El certificado de identidad del registro del sistema remoto se puede generar en la configuración del servidor de firma de certificados interno de la empresa. Los clientes y servidores Syslog remotos basados en TLS utilizan el mismo certificado de CA en los ajustes de configuración, el cual se obtiene desde un servidor de CA. iDRAC proporciona una interfaz de usuario para cargar este certificado de CA, agregarlo a su archivo de configuración y reiniciar el servicio Syslog remoto.

Configuración de registros de sistemas remotos mediante la interfaz web

Para configurar los ajustes del servidor de registro del sistema remoto:

1. En la interfaz web de iDRAC, vaya a **Configuración** > **Ajustes del sistema** > **Configuración de alertas** > **Registro del sistema remoto** > **Ajustes**.
2. Los siguientes ajustes están disponibles: Seleccione el ajuste requerido:
   - **Ajustes básicos**: para soluciones heredadas
   - **Ajustes seguros**: para implementaciones nuevas (cifrado del tráfico del registro del sistema remoto con TLS) Para
   - **Ninguno**: para deshabilitar las alertas del registro del sistema remoto

   Para obtener información acerca de los valores de campo de estas opciones, consulte la **Ayuda en línea de iDRAC**.
3. Haga clic en **Aplicar**.
   Se guardan los ajustes. Todos los registros que se graban en el registro de Lifecycle también se graban simultáneamente en los servidores remotos configurados.

Configuración del registro de sistema remoto mediante RACADM

Para configurar los ajustes del registro de sistema, utilice el comando `set` con los objetos en el grupo `iDRAC.SysLog`.

Para obtener más información, consulte Guía de la CLI RACADM de Integrated Dell Remote Access Controller.

Id. de mensaje de alertas

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

Tabla 34. Id. de mensaje de alertas

ID de mensaje	Descripción
AMP	Amperaje
ASR	Restablecimiento automático del sistema
BAT	Suceso de la batería
BIOS	Administración del BIOS
BOOT	Control de arranque
CBL	Cable
CPU	Procesador
CPUA	Procesador ausente
CTL	Controladora de almacenamiento
DH	Administración de certificados
DIS	Descubrimiento automático
ENC	Gabinete de almacenamiento
VENTILADOR	Suceso de ventilador
FSD	Depuración
HWC	Configuración de hardware
IPA	Cambio de IP de DRAC
ITR	Intrusión
JCP	Control de trabajos

Tabla 34. Id. de mensaje de alertas (continuación)

ID de mensaje	Descripción
LC	Lifecycle Controller
LIC	Licencias
LNK	Estado de vínculo
LOG	Registrar evento
MEM	Memoria
NDR	Controlador de NIC de SO
NIC	Configuración de NIC
OSD	Implementación de SO
OSE	Evento de SO
PCI	Dispositivo PCI
PDR	Disco físico
PR	Intercambio de piezas
PST	POST del BIOS
PSU	Fuente de alimentación
PSUA	PSU ausente
PWR	Uso de alimentación
RAC	Suceso RAC
RDU	Redundancia
RED	Descarga de firmware
RFM	SD de dirección flexible
RSI	Servicio remoto
SEC	Suceso de seguridad
SEL	Registro de sucesos del sistema
SRD	RAID de software
SSD	SSD PCIe
STOR	Almacenamiento
SUP	Trabajo de actualización del firmware
SWC	Configuración de software
SWU	Cambio de software
SYS	Información del sistema
TMP	Temperatura
TST	Alerta de prueba
UEFI	Evento de UEFI
USR	Seguimiento del usuario
VDR	Disco virtual
VLT	Voltaje
VME	Medios virtuales

Tabla 34. Id. de mensaje de alertas (continuación)

ID de mensaje	Descripción
VRM	Consola virtual
WRK	Nota de trabajo

Detección de fugas de GPU y CPU

iDRAC detecta fugas de líquido de enfriamiento en la CPU y la GPU a través de señales críticas, de advertencia y de información recibidas de los sensores IPMI del OEM correspondiente. Las fugas se notifican como registros de eventos del sistema (SEL), registros de LC, eventos de WS, correos electrónicos y capturas SNMP en función de los ajustes de alerta configurados. iDRAC realiza las acciones adecuadas según los ajustes de configuración de alertas.

De manera predeterminada, la alerta **Apagado de acción predeterminada del sistema de refrigeración líquida** está configurada para un **Apagado ordenado** si hay una fuga de líquido de GPU en el servidor. Se recomienda forzar el apagado del servidor cuando se detecta una fuga de líquido de GPU y no esperar a que se complete la operación de **Apagado ordenado**.

Si iDRAC detecta una fuga de líquido de GPU al acceder a la UI de LC o al entorno previo al arranque (BIOS o administrador de arranque), o durante el proceso de arranque, el servidor puede activar un apagado inmediato.

Configuración de detección de fuga de líquido de CPU

Configure las alertas para que se generen las notificaciones necesarias y se inicien acciones específicas en iDRAC en función de la gravedad de la fuga de la CPU.

1. Vaya a **Configuración** > **Ajustes del sistema** > **Configuración de alertas** > **Alertas** > **Configuración de alertas** > **Sistema de refrigeración líquida**.
2. Haga clic en **+** y, a continuación, seleccione las casillas de verificación **Correo electrónico**, **Captura SNMP**, **Alerta de IPMI**, **Registro del sistema remoto**, **Evento de WS**, **Registro del sistema operativo** y **Evento de Redfish** para las alertas críticas, de advertencia e informativas.
3. Seleccione las acciones (**Reiniciar, Ciclo de encendido, Apagado**) en la lista **Acciones** para las alertas críticas, de advertencia e informativas.

Configuración de detección de fuga de líquido de GPU

De manera predeterminada, la alerta **Apagado de acción predeterminada del sistema de refrigeración líquida** está configurada para un **Apagado ordenado** si hay una fuga de líquido de GPU en el servidor. Puede configurar las opciones según sus requisitos.

1. Vaya a **Configuración** > **Ajustes del sistema** > **Configuración de alertas** > **Alertas** > **Configuración de alertas** > **Apagado de acción predeterminada del sistema de refrigeración líquida**.
2. Haga clic en **+**.
   Las casillas de verificación **Gravedad** y **Captura SNMP** están seleccionadas. En la lista **Acciones**, la opción **Apagado ordenado** está seleccionada de manera predeterminada.

   NOTA: Si el servidor no puede realizar un **apagado ordenado** en un plazo de 15 minutos, se realiza un apagado forzado.

   PRECAUCIÓN: Si iDRAC se está reiniciando y el Apagado ordenado también está en curso en simultáneo, el sistema tarda más de 20 minutos en apagarse. Se recomienda forzar el apagado del servidor y no esperar a que se complete la operación de Apagado ordenado.
3. Si desea incluir más notificaciones, seleccione las casillas de verificación **Correo electrónico**, **Captura SNMP**, **Alerta IPMI**, **Registro del sistema remoto**, **Evento de WS**, **Registro del sistema operativo** y **Evento de Redfish**.
4. Si desea cambiar la acción predeterminada **Apagado ordenado**, seleccione **Sin acción** o **Apagar**.

   NOTA: Si se selecciona **Sin acción**, el sistema no se apaga cuando hay una fuga de líquido de la GPU.

15

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). Se puede acceder al registro de ciclo de vida útil mediante la interfaz web de la iDRAC y RACADM.

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 de registros de eventos de sistema

Cuando se produce un suceso del sistema en un sistema administrado, se guarda 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 eventos 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 RACADM de Integrated Dell Remote Access Controller.

Visualización del registro de eventos del sistema mediante la interfaz web

Para ver el SEL, en la interfaz web de iDRAC, vaya a **Mantenimiento** > **Registro de eventos del sistema**.

En la página **Registro de eventos del sistema**, se muestra un indicador de estado del sistema, un registro de fecha y hora, 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 **SEL** en la ubicación de su elección.

NOTA: Si utiliza Internet Explorer y hay un problema al guardar, descargue la actualización de seguridad acumulativa para Internet Explorer. Puede descargarlo desde el sitio web de soporte 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 borrar el SEL, se registra una entrada en el registro de Lifecycle Controller. La entrada de registro incluye el nombre de usuario y la dirección IP desde donde se borró el SEL.

Visualización del registro de eventos del sistema mediante la utilidad de configuración de iDRAC

Puede ver la cantidad total de registros en el registro de eventos del sistema (SEL) mediante la utilidad de configuración de iDRAC y borrar los registros. Para hacerlo, realice estos pasos:

1. En la utilidad de configuración de iDRAC, vaya a **Registro de eventos del sistema**.
   En **Registro de eventos del sistema de Ajustes de iDRAC**, se muestra el **Número total de registros**.
2. Para borrar los registros, seleccione **Sí**. De lo contrario, seleccione **No**.
3. Para ver los eventos del sistema, haga clic en **Mostrar el registro de eventos del sistema**.
4. Haga clic en **Back** (Atrás), haga clic en **Finish** (Terminar), y posteriormente, haga clic en **Yes** (Sí).

Visualización del registro de Lifecycle

Los registros de Lifecycle Controller proporcionan el historial de cambios relacionados con los componentes instalados en un sistema administrado. También es posible agregar notas de trabajo a cada entrada del registro.

Se registran los siguientes eventos y actividades:

- 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
- Virtual console
- 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: Cuando se produce un evento varias veces, se muestra un único registro de eventos en los registros de LC. También se muestra un registro adicional (L0G007) que indica la cantidad de veces que se produjo este evento. De manera predeterminada, los registros de eventos duplicados están deshabilitados en la iDRAC. Si desea que todos los eventos se muestren en los registros de LC, ejecute el comando RACADM `set idrac.logging.LCDuplicateEventEnable enabled`.

Visualización de registro de ciclo de vida útil mediante la interfaz web

Para ver los registros de ciclo de vida útil, haga clic en **Mantenimiento** > **Registro de ciclo de vida útil**. Se muestra la página **Registro de ciclo de vida útil**. Para obtener más información sobre las opciones, consulte la **Ayuda en línea de iDRAC**.

Filtrado de registros de Lifecycle

Puede filtrar las entradas del registro en función de la categoría, la gravedad, la palabra clave o el rango de fechas.

Para filtrar los registros de ciclo de vida útil:

1. En la página **Registro de ciclo de vida útil**, en la sección **Filtro de registro**, realice una o todas las siguientes acciones:
   - En la lista desplegable, seleccione el **Tipo de registro**.
   - Seleccione el nivel de gravedad en la lista desplegable **Gravedad**.
   - Ingrese una palabra clave.
   - Especifique el rango de fechas.
2. Haga clic en **Aplicar**.
   Las entradas del registro con filtro se muestran en **Resultados del registro**.

Incorporación de comentarios en los registros de Lifecycle

Para agregar comentarios a los registros de Lifecycle, realice lo siguiente:

1. En la página **Registro de ciclo de vida útil**, haga clic en el icono + para la entrada de registro necesaria.
   Se muestran los detalles del ID del mensaje.
2. Ingrese los comentarios para la entrada del registro en el cuadro **Comments**.
   Los comentarios se muestran en el cuadro **Comentario**.

Visualización del registro de ciclo de vida útil mediante RACADM

Para ver los registros de Lifecycle, utilice el comando `lclog`.

Para obtener más información, consulte la *Guía de la CLI de RACADM de la iDRAC*.

Exportación de los registros de Lifecycle Controller

Puede exportar el registro completo de Lifecycle Controller (entradas activas y archivadas) en un único archivo XML comprimido en zip a un recurso compartido de red o al sistema local. La extensión del archivo XML comprimido es `.xml.gz`. Las entradas del archivo están ordenadas secuencialmente en función de sus números de secuencia, desde el número de secuencia más bajo al más alto.

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 la *Guía de la CLI de RACADM de la iDRAC*.

Exportación de 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**: exportar los registros de Lifecycle Controller a una ubicación compartida en la red.
   - **Local**: exportar los registros de Lifecycle Controller a una ubicación en el sistema local.

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

   Para obtener información acerca de los campos, consulte la **Ayuda en línea de iDRAC**.
3. Haga clic en **Exportar** para exportar el registro a la ubicación especificada.

Evitar el desbordamiento de registros de Lifecycle

La iDRAC admite la capacidad de evitar el desbordamiento de registros de Lifecycle desde las consolas debido a la alta frecuencia de inicios de sesión desde las consolas.

- Los eventos USR0030/USR0032 se incluyen en el registro de Lifecycle para cada inicio/cierre de sesión correcto, respectivamente.
- Estos eventos se pueden agregar a un registro único nuevo, en función del ajuste de un atributo.
- Un nuevo registro de USR0036 se incluirá en el registro de Lifecycle con una agregación de los eventos de inicio y cierre de sesión que se han producido dentro de un período especificado por el atributo`LCLoggingAggregationTimeout`.

NOTA:
- De forma predeterminada, el atributo LCLogAggregation de la característica está deshabilitado.
- De manera predeterminada, el tiempo de espera se establece en 60 minutos y se aplica solo si LCLogAggregation está habilitado.

- Los eventos USR0030 y USR0032 no se incluirán en el registro de Lifecycle, pero se seguirán enviando alertas individuales si las alertas correspondientes están habilitadas (SNMP/correo electrónico/evento de Redfish/evento de WS).

Adición de notas de trabajo

Cada usuario que inicia sesión en iDRAC puede agregar notas de trabajo, y esto se almacena en el registro del ciclo de vida útil como un evento. 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 iDRAC, vaya a **Panel** > **Notas** > **Agregar nota**.
   Aparecerá la página **Notas de trabajo**.
2. En **Notas de trabajo**, ingrese el texto en el cuadro de texto en blanco.

   NOTA: Se recomienda no utilizar demasiados caracteres especiales.

3. Haga clic en **Save**.
   La nota de trabajo se agregará al registro. Para obtener más información, consulte la **Ayuda en línea de iDRAC**.

Visualización del registro de Lifecycle

Los registros de Lifecycle Controller proporcionan el historial de cambios relacionados con los componentes instalados en un sistema administrado. También es posible agregar notas de trabajo a cada entrada del registro.

Se registran los siguientes eventos y actividades:

- 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
- Virtual console
- 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: Cuando se produce un evento varias veces, se muestra un único registro de eventos en los registros de LC. También se muestra un registro adicional (L0G007) que indica la cantidad de veces que se produjo este evento. De manera predeterminada, los registros de eventos duplicados están deshabilitados en la iDRAC. Si desea que todos los eventos se muestren en los registros de LC, ejecute el comando RACADM `set idrac.logging.LCDuplicateEventEnable enabled`.

Visualización de registro de ciclo de vida útil mediante la interfaz web

Para ver los registros de ciclo de vida útil, haga clic en **Mantenimiento** > **Registro de ciclo de vida útil**. Se muestra la página **Registro de ciclo de vida útil**. Para obtener más información sobre las opciones, consulte la **Ayuda en línea de iDRAC**.

16

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:

- **Monitoreo de alimentación**: vea el estado de la alimentación, el historial de 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 energía potencial 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.
- **Opciones de recuperación de alimentación de CA**: configure las opciones de recuperación de alimentación para que el sistema se recupere en función de sus necesidades.

Temas:

Monitoreo de la alimentación

iDRAC monitorea continuamente el consumo de energía en el sistema y muestra los siguientes valores:

- Advertencia de consumo de energía y umbrales críticos.
- Valores de acumulación de energía, pico de alimentación y pico de amperaje.
- Consumo de energía durante la última hora, el último día o la última semana.
- Consumo de energía promedio, mínimo y máximo.
- Valores pico históricos, y registros de fecha y hora pico.
- Valores de capacidad máxima pico y de capacidad máxima instantánea (para servidores en torre y en rack).

NOTA: El histograma para la tendencia de consumo de energía del sistema (por hora, diariamente, semanalmente) se mantiene solo mientras iDRAC está en ejecución. Si se reinicia iDRAC, se pierden los datos de consumo de energía existentes y se reinicia el histograma.

NOTA: En el modo solo HBM, la alimentación de memoria de HBM se cuenta como parte de la alimentación del paquete; por lo tanto, la lectura de telemetría de alimentación de memoria se informa como 0 para este modo.

NOTA: Después de aplicar una actualización o restablecimiento del firmware de iDRAC, el gráfico de consumo de energía se borrará o restablecerá.

Monitoreo del índice de rendimiento de CPU, memoria y módulos de entrada y salida mediante la interfaz web

Para monitorear el índice de rendimiento de CPU, memoria y módulos de I/O, en la interfaz web de la iDRAC, consulte **Sistema** > **Rendimiento**.

- Sección **Rendimiento del sistema**: muestra la lectura actual y la lectura de aviso para el índice de utilización de I/O, memoria y CPU y el índice CUPS de nivel de sistema en una vista gráfica.
- Sección **Datos históricos de rendimiento del sistema**:
  - Proporciona las estadísticas para CPU, memoria, utilización de E/S e índice CUPS de nivel del sistema. Si el sistema del host está apagado, el gráfico muestra la línea de apagado por debajo del 0 %.
  - Puede restablecer la utilización máxima de un sensor en particular. Haga clic en **Restablecer valores máximos históricos**. Debe tener el privilegio de configuración para restablecer el valor máximo.
- Sección **Métricas de rendimiento**:
  - Muestra el estado y la lectura actual
  - Muestra o especifica el límite de utilización del umbral de precaución. Debe tener el privilegio de configuración del servidor para establecer los valores de umbral.

Para obtener información acerca de las propiedades que se muestran, consulte la **Ayuda en línea de iDRAC**.

Supervisión del índice de rendimiento de CPU, memoria y módulos de 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 RACADM de Integrated Dell Remote Access Controller.

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.

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 precaución para el consumo de energía mediante la interfaz web

1. En la interfaz web de iDRAC, vaya a **Sistema** > **Visión general** > **Lectura de alimentación y umbrales actuales**.
2. En la sección **Lectura de alimentación y umbrales actuales**, haga clic en **Editar umbral de precaución**.
   Se muestra la página **Editar umbrales de precaución**.
3. En la columna **Umbral de precaución**, ingrese el valor en **Vatios** o **BTU/h**.

   Los valores deben ser inferiores a los valores de **Umbral de fallo**. Los valores se redondean 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 **Save**. Se configuran los valores.

Realización de operaciones de control de alimentación

La iDRAC permite encender, apagar, restablecer, apagar de manera ordenada, o ejecutar un ciclo de apagado y encendido del sistema de manera remota mediante la interfaz web o RACADM.

Las operaciones de control de alimentación del servidor que se inician desde iDRAC son independientes del comportamiento del botón de encendido que se configura 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.

Realización de operaciones de control de alimentación mediante la interfaz web

Para realizar operaciones de control de alimentación:

1. En la interfaz web de iDRAC, vaya a **Configuración** > **Administración de energía** > **Control de alimentación**. Aparecen las opciones de **Control de alimentación**.
2. Seleccione la operación de alimentación necesaria:
   - Encender el sistema
   - Apagar el sistema
   - 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**.

Realización de operaciones de control de alimentación mediante RACADM

Para realizar acciones de alimentación, utilice el comando **serveraction**.

Para obtener más información, consulte Guía de la CLI RACADM de Integrated Dell Remote Access Controller.

Límites de alimentación

Puede ver los límites del umbral de alimentación que cubren el rango de consumo de energía de CA y CC que presenta un sistema con una carga de trabajo pesada al centro de datos. Esta es una función con licencia.

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 un umbral de presupuesto de energía para reducir el consumo a 525 W. Cuando se configura este presupuesto de energía, el rendimiento del sistema se ajusta dinámicamente para mantener el consumo de energía 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.

NOTA: Establecer un límite de alimentación en un valor por debajo del rango recomendado puede causar un rendimiento variado, incluido un mayor tiempo de arranque.

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 RACADM de Integrated Dell Remote Access Controller.

Configuración de la política de límite 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 límite sobre alimentación mediante la utilidad de configuración de iDRAC

Para ver y configurar políticas de alimentación:

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

   NOTA: El enlace **Configuración de energía** solo está disponible si la fuente de alimentación del servidor soporta el monitoreo de alimentación.

   Se muestra la página **Configuración de energía de Ajustes de iDRAC**.
2. Seleccione **Habilitado** para habilitar la **Política de límite de alimentación**, de lo contrario, seleccione **Deshabilitado**.
3. Utilice la configuración recomendada o en **Política de límite de alimentación definida** por el usuario, ingrese 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 **Back** (Atrás), haga clic en **Finish** (Terminar), y posteriormente, haga clic en **Yes** (Sí).
   Se configuran los valores de límite de alimentación.

Configuración de las opciones de fuente de alimentación

Puede configurar las opciones de fuente de alimentación, tales como la política de redundancia, el hot spare y la corrección del factor de energía.

NOTA: Es posible que las características de hot spare y de corrección del factor de energía no estén disponibles en algunas de las plataformas o versiones.

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 habilitar el hot spare, las PSU pueden activarse o pasar al modo de suspensión en función de la carga. Si el hot spare está habilitado, se habilita el uso compartido de corriente eléctrica asimétrica entre las dos PSU. Una PSU está **encendida** y proporciona la mayor parte de la corriente; la otra PSU está en modo de suspensión y proporciona una pequeña cantidad de la corriente. A menudo, esto se denomina 1 + 0 con dos PSU y hot spare habilitados. Si todas las PSU-1 están en el circuito A y todas las PSU-2 están en el circuito B, con el hot spare habilitado (configuración predeterminada de fábrica del hot spare), el circuito B tiene mucha menos carga y activa las advertencias. Si el hot spare está deshabilitado, el uso compartido de corriente eléctrica es de 50-50 entre las dos PSU; el circuito A y el circuito B normalmente 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 fuente de alimentación mediante la interfaz web

Para configurar las opciones de fuente de alimentación:

1. En la interfaz web de la iDRAC, vaya a **Configuración** > **Administración de energía** > **Configuración de energía**.
2. En **Política de redundancia de alimentación**, seleccione las opciones necesarias. Para obtener más información, consulte la **Ayuda en línea de iDRAC**.
3. Haga clic en **Aplicar**. Las opciones de fuente de alimentación están configuradas.

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 RACADM de Integrated Dell Remote Access Controller.

Configuración de las opciones de fuente de alimentación mediante la utilidad de configuración de iDRAC

Para configurar las opciones de fuente de alimentación:

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

   NOTA: El enlace **Configuración de energía** solo está disponible si la fuente de alimentación del servidor soporta el monitoreo de alimentación.

   Se muestra la página **Configuración de energía de Ajustes de iDRAC**.
2. En **Opciones de fuente de alimentación**:
   - Habilite o deshabilite la redundancia de la fuente de alimentación.
   - Habilite o deshabilite hot spare.
   - Establezca la fuente de alimentación principal.
   - Habilite o deshabilite la corrección del factor de energía. Para obtener más información acerca de las opciones, consulte la **Ayuda en línea de la utilidad de configuración de iDRAC**.
3. Haga clic en **Back** (Atrás), haga clic en **Finish** (Terminar), y posteriormente, haga clic en **Yes** (Sí).
   Las opciones de fuente de alimentación están configuradas.

Habilitación o deshabilitación del botón de encendido

Para habilitar o deshabilitar el botón de encendido en la parte frontal del sistema:

1. En la utilidad de configuración de iDRAC, vaya a **Seguridad del panel frontal**.
   Se muestra la página **Seguridad del panel frontal de Ajustes de iDRAC**.
2. Seleccione **Habilitado** para habilitar el botón de encendido o **Deshabilitado** para deshabilitarlo.
3. Haga clic en **Back** (Atrás), haga clic en **Finish** (Terminar), y posteriormente, haga clic en **Yes** (Sí).
   La configuración se guarda.

Enfriamiento multivector

Con el enfriamiento multivector, se implementa un enfoque multivector a los controles térmicos en las plataformas de servidor Dell. 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 de enfriamiento**. Incluye (entre otros elementos) lo siguiente:

- Un gran conjunto de sensores (térmicos, de alimentación, de inventario, etc.) que permite una interpretación precisa del estado térmico del sistema en tiempo real en varias ubicaciones dentro del servidor. Solo se muestra un pequeño subconjunto de sensores que son relevantes para las necesidades de los usuarios en función de 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:
  - Conocer la capacidad máxima de LFM de cada ranura dentro del servidor.
  - Conocer qué enfoque se emplea para el enfriamiento de PCIe de cada ranura (flujo de aire controlado, temperatura controlada).
  - Conocer el LFM mínimo que se entrega a una ranura si la tarjeta es de terceros (tarjeta personalizada definida por el usuario).
  - Marcar el valor mínimo de LFM personalizado para la tarjeta de otros fabricantes, lo cual permite definir con mayor precisión las necesidades de enfriamiento de la tarjeta que el usuario conoce mejor gracias a las especificaciones personalizadas de la tarjeta.
- Se muestra la métrica de flujo de aire del sistema en tiempo real (CFM o 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.
- Admite ajustes térmicos personalizados, como perfiles térmicos (máximo rendimiento frente a máximo rendimiento por vatio, límite de sonido), opciones de velocidad de ventilador personalizadas (velocidad mínima y compensaciones de velocidad del ventilador) y ajustes de temperatura de escape personalizada.
  - 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 otros fabricantes. El flujo de aire de provisión del algoritmo térmico para tarjetas de otros fabricantes puede ser mayor o menor que las necesidades de enfriamiento de la tarjeta real y el cliente puede ajustar la respuesta de la tarjeta si ingresa la métrica de LFM correspondiente a la tarjeta de otros fabricantes.

  - 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 (por ejemplo, un ajuste de salida personalizado de 45 °C con una temperatura de entrada alta [por ejemplo, 30 °C] y una configuración cargada [consumo de energía del sistema alto, y flujo de aire bajo]).

  - La opción de límite de sonido es nueva en los servidores PowerEdge de 14.ª generación. 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.
  - 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 una mayor eficiencia, un mejor rendimiento, una vida útil más prolongada y menos vibración. También proporcionan una mejor salida acústica.
  - La expectativa de vida útil promedio de un ventilador de servidor varía según la especificación de la plataforma.

- Si se extrae o se inserta un ventilador en caliente, las interfaces de iDRAC pueden tardar hasta 90 segundos en reflejar los cambios en la página **Enfriamiento** (**Sistema** > **Visión general** > **Enfriamiento** > **Ventiladores**)

- Los disipadores de calor personalizados están diseñados para optimizar el enfriamiento de los componentes con un flujo de aire mínimo (requerido); sin embargo, soportan CPU de alto rendimiento.

Configuración de recuperación de alimentación de CA

Puede configurar el estado de alimentación esperado después de una pérdida de alimentación y recuperación de energía del servidor.

1. Seleccione el estado esperado del servidor en el campo **Recuperación de alimentación de CA** después de la recuperación de alimentación. La opción predeterminada es **Encendido**.

   NOTA: Seleccione **Última** si desea restaurar el servidor a su estado antes de que ocurriera la pérdida de energía.

2. Seleccione la opción **Retraso en la recuperación de alimentación de CA** en función de cuándo desee encender el servidor.
3. Si seleccionó **Definido por el usuario** como el **Retraso en la recuperación de alimentación de CA**, ingrese el **Retraso definido por el usuario(120 s a 600 s)** en segundos (entre 120 y 600 segundos).

17

Actualizaciones de iDRAC Direct

La iDRAC proporciona la capacidad fuera de banda para actualizar el firmware de varios componentes de un servidor PowerEdge. La actualización directa de la iDRAC ayuda a eliminar los trabajos por etapas durante las actualizaciones. Solo los backplane SEP (pasivos) se soportan en las actualizaciones directas.

iDRAC se utiliza para realizar actualizaciones preconfiguradas con el fin de iniciar la actualización del firmware de los componentes. Desde esta versión, las actualizaciones directas se han aplicado a PSU y backplane. Con el uso de las actualizaciones directas y el backplane pueden tener actualizaciones más rápidas. En el caso de PSU, se evita un reinicio (para inicializar las actualizaciones) y la actualización se puede realizar en un solo reinicio.

Con la función de actualización directa de la iDRAC, puede eliminar el primer reinicio para iniciar las actualizaciones. El segundo reinicio es controlado por el propio dispositivo y la iDRAC notifica al usuario si hay necesidad de un restablecimiento por separado a través de un estado de trabajo.

NOTA: En el caso de que una actualización requiera el restablecimiento/reinicio de iDRAC o se reinicie iDRAC, se recomienda verificar si iDRAC se encuentra completamente listo; para ello, espere unos segundos hasta un máximo de 5 minutos antes de usar cualquier otro comando.

18

Inventario, monitoreo y configuración de dispositivos de red

Puede inventariar, monitorear y configurar los siguientes dispositivos de red:

- Tarjetas de interfaz de red (NIC)
- Adaptadores de red convergente (CNA)
- LAN en placas base (LOM)
- Tarjetas Open Compute Project (OCP)

Antes de desactivar NPAR o una partición individual en los dispositivos CNA, borre todos los atributos de identidad de E/S (por ejemplo: dirección IP, direcciones virtuales, iniciador y destinos de almacenamiento) y los atributos de nivel de partición (ejemplo: asignación de ancho de banda). Para inhabilitar una partición, cambie el ajuste del atributo VirtualizationMode a NPAR o desactive todas las personalidades en una partición.

Según el tipo de dispositivo CNA instalado, es posible que no se conserven los ajustes de los atributos de la partición desde la última vez que esta estuvo activa. Cuando active una partición, ajuste todos los atributos de identidad de E/S y los atributos relacionados con las particiones. Para activar una partición, cambie el ajuste del atributo VirtualizationMode a NPAR o active una personalidad (por ejemplo: NicMode) en la partición.

Temas:

Inventario y supervisión de dispositivos HBA FC

Es posible monitorear de manera remota la condición de los dispositivos de los adaptadores de bus de host Fibre Channel (FC HBA) y ver el inventario de los mismos en el sistema administrado. Se admiten los FC HBA Emulex y QLogic. Para cada dispositivo de FC HBA, puede ver la siguiente información de los puertos:

- Información objetivo del almacenamiento FC
- Información objetivo del almacenamiento NVMe
- Propiedades de puertos
- Estadísticas de recepción y transmisión

NOTA: No se soportan unidades HBAs de Emulex FC8.

Monitoreo de dispositivos FC HBA 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 RACADM de Integrated Dell Remote Access Controller.

Monitoreo de dispositivos de FC HBA mediante la interfaz web

Para ver la información del dispositivo FC HBA mediante la interfaz web, vaya a **Sistema** > **Visión general** > **Dispositivos de red** > **Fibre Channel**. Para obtener más información acerca de estas propiedades que se muestran, consulte la **Ayuda en línea de iDRAC**.

El nombre de la página también muestra el número de ranura donde está disponible el dispositivo FC HBA y el tipo de dispositivo FC HBA.

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

NOTA: En el caso del dispositivo NIC integrado, la representación del BIOS de cada puerto LOM se considera como un dispositivo NIC individual, de modo que la cadena FQDD se muestra como **NIC integrada 1, puerto 1, partición 1** y **NIC integrada 2, puerto 1, partición 1**.

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 RACADM de Integrated Dell Remote Access Controller.

Es posible que se muestren propiedades adicionales cuando se utiliza RACADM, además de las propiedades que se muestran en la interfaz web de la iDRAC.

Monitoreo de dispositivos de red mediante la interfaz web

Para ver la información del dispositivo de red mediante la interfaz web, vaya a **Sistema** > **Visión general** > **Dispositivos de red**. Se muestra la página **Dispositivos de red**. Para obtener más información acerca de estas propiedades que se muestran, consulte la **Ayuda en línea de iDRAC**.

NOTA: La propiedad de puerto **Wake on LAN** para los dispositivos de red en la UI de iDRAC puede contener datos obsoletos a medida que se actualiza durante CSIOR. Consulte el resultado de RACADM para obtener los datos correctos de esta propiedad.

Vista Conexión

La comprobación manual y la solución de problemas de las conexiones de red de los servidores no se pueden administrar en un entorno de centro de datos. La iDRAC optimiza el trabajo con la vista de conexión de la 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 la iDRAC, 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 la iDRAC. 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 de conexión proporciona información de los puertos del conmutador que están conectados a los puertos del servidor y al puerto dedicado de la iDRAC. Los puertos de red del servidor incluyen los de PowerEdge LOM, OCP, 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 la 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 `SwitchConnection View` de RACADM.

Habilitado	Seleccione **Activada** para activar la vista de conexión. La opción **Activado** está seleccionada de manera predeterminada.
Estado	Muestra **Activada** si se activa la opción de vista de conexión en **Vista de conexión** en la configuración de la 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 después de que la vista 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.

La iDRAC soporta el envío de paquetes de LLDP estándar a conmutadores externos. Esto proporciona opciones para detectar la iDRAC en la red. La iDRAC envía dos tipos de paquetes de LLDP a la red saliente:

- **LLDP de topología**: en esta función, el paquete de LLDP pasa por todos los puertos de NIC del servidor soportados para que un conmutador externo pueda localizar el servidor de origen, el puerto OCP [FQDD de NIC], la ubicación del IOM en el chasis, etc. El 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: 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 de LLDP solo pasa por el puerto de NIC de la iDRAC activo que está en uso (NIC dedicada o LOM compartida), de modo que el conmutador adyacente pueda localizar el puerto de conexión de la iDRAC en el conmutador. El LLDP de detección es específico solo para el puerto de red de la iDRAC activo y no se verá en todos los puertos de red del servidor. El LLDP de detección tendrá algunos detalles de la iDRAC, como la dirección IP, la dirección MAC, la etiqueta de servicio, etc. El conmutador puede detectar automáticamente los dispositivos de la iDRAC conectados a él y algunos datos de la iDRAC.

  NOTA: Si la dirección MAC virtual se borra en un puerto/partición, la dirección MAC virtual es igual a la dirección MAC.

Para activar o desactivar el LLDP de detección, vaya a **Configuración de la iDRAC** > **Conectividad** > **Red** > **Configuración común** > **LLDP de topología**.

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 habilitada se selecciona de manera predeterminada

El paquete de LLDP que se crea desde la iDRAC se puede ver desde el conmutador 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 de puerto del conmutador para el puerto de red del servidor o el puerto de red de la iDRAC. Si la información de conexión del conmutador y de conexión de puerto del conmutador no se actualizan durante cinco minutos, la información de conexión del conmutador y de conexión de puerto del conmutador se muestra como datos obsoletos (última información buena conocida) para todas las interfaces de usuario.

Valores posibles de la vista de conexión

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 soportado	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.

Inventario y supervisión de dispositivos transceptor SFP

Es posible supervisar de manera remota la condición de los dispositivos transceptor SFP conectados al sistema y ver el inventario de ellos. A continuación, se indican los transceptores compatibles:

- SFP
- SFP+
- SFP28
- SFP-DD
- QSFP
- QSFP+
- QSFP28
- QSFP-DD
- Módulos base-T
- Cables AOC y DAC
- RJ-45 base-T conectado con Ethernet
- Fibre Channel
- Puertos del adaptador IB

La información más útil del transceptor corresponde al número de serie y al número de pieza del transceptor EPROM. Esto permitiría comprobar los transceptores instalados de forma remota cuando se solucionen problemas de conectividad. Para cada dispositivo del transceptor SFP, puede ver la siguiente información de los puertos:

- Nombre de proveedor
- Número de referencia
- Revisión
- Número de serie
- Identificador del dispositivo
- Tipo de interfaz

Supervisión de dispositivos del transceptor SFP mediante la interfaz web

Para ver la información del dispositivo del transceptor SFP mediante la interfaz Web, vaya a**Sistema** > **Visión general** > **Dispositivos de red** y haga clic en un dispositivo específico. Para obtener más información acerca de estas propiedades que se muestran, consulte la **Ayuda en línea de iDRAC**.

El nombre de la página también muestra el número de ranura en el que está disponible el dispositivo del transceptor en estadísticas del puerto.

El monitoreo de datos para dispositivos SFP solo está disponible para SFP activos. A continuación, se muestra la siguiente información:

- Alimentación de salida TX
- Corriente de polarización TX
- Alimentación de entrada RX
- Voltaje VCC
- Temperatura

Supervisión de dispositivos transceptores SFP mediante RACADM

Para ver la información de dispositivos transceptores SFP mediante RACADM, utilice el comando `networktransceiverstatistics`.

Para obtener más información, consulte la *Guía de CLI de RACADM de Integrated Dell Remote Access Controller*.

Transmisión de telemetría

La telemetría les permite a los usuarios recopilar y transmitir métricas, eventos y registros de datos de dispositivos en tiempo real a partir de un servidor PowerEdge a una aplicación de cliente o servidor externa suscrita. Con la telemetría, puede establecer el tipo y la frecuencia de los informes que se deben generar.

NOTA: La característica está soportada en todas las plataformas y necesita licencia iDRAC Datacenter.

La telemetría es una solución de uno a muchos para recopilar y transmitir datos del sistema activo a partir de uno o varios servidores PowerEdge (iDRAC) a un "servicio de monitoreo, análisis y alerta de servidor remoto" centralizado. La función también es compatible con la recopilación de datos según la demanda de estos.

Entre los datos de telemetría, se incluyen métricas/inventario y registros/eventos. Los datos se pueden transmitir (expulsar) o recopilar (extraer) desde la iDRAC hacia los consumidores remotos o mediante estos, como el cliente de Redfish y el servidor Syslog remoto. Los datos de telemetría también se proporcionan al iDRAC SupportAssist Data Collector según la demanda. Los informes y la recopilación de datos se basan en las estadísticas de telemetría, el generador y las definiciones de informes predefinidos de Redfish. Los ajustes del streaming de telemetría se pueden configurar con la interfaz web del iDRAC, RACADM, Redfish y el perfil de configuración del servidor (SCP).

Para habilitar la telemetría, vaya a **Configuración** > **Ajustes del sistema** > **Filtrado de telemetría** y seleccione **Habilitado** en la lista de **Flujo de datos de telemetría**. La transmisión de datos es automática hasta que se habilite la telemetría.

En la siguiente tabla, se describen los informes de métricas que se pueden generar mediante telemetría:

Tabla 35. Informe de métricas

Tipo	Grupo de métricas	Inventario	Sensor	Statistics	Configuración	Métrica
Dispositivos de E/S	Tarjetas NIC	No	Sí	Sí	No	No
	HBA FC	No	Sí	Sí	No	No
Dispositivos del servidor	CPU	No	Sí	No	No	Sí
	Memoria	No	Sí	No	No	Sí
	Ventiladores	No	Sí	No	No	No
	PSU	No	No	No	No	Sí
	Sensores	No	Sí	No	No	No
Del entorno	Térmico	No	Sí	No	No	Sí
	Alimentación	No	No	Sí	No	Sí
	Rendimiento	No	No	Sí	No	No
Aceleradores	GPU	No	No	Sí	No	Sí

Para obtener más información acerca de las descripciones de los campos de la sección telemetría, consulte **Ayuda en línea de iDRAC**.

NOTA:

- Cuando el backplane SAS/SATA está conectado a la controladora SATA integrada, se espera que el backplane no se muestre como gabinete en el sistema y que tampoco se muestre en el inventario de hardware.
- StorageDiskSMARTDATA solo es compatible con unidades SSD que cuentan con el protocolo de bus SAS/SATA y detrás de la controladora BOSS.
- Los datos de StorageSensor se informan solo para las unidades en el modo listo/en línea/no RAID y no detrás de la controladora BOSS.

- NVMeSMARTData solo es soportado en unidades SSD (SSD PCIe/NVMe Express) que cuenten con protocolo de bus de PCIe (no detrás de SWRAID) y también detrás de la controladora BOSS-N1.
- Los datos de GPGPUStatistics solo están disponibles en modelos de GPGPU específicos compatibles con la capacidad de memoria de ECC.
- PSUMetrics no está disponible en las plataformas modulares.
- Las métricas de alimentación del ventilador y de alimentación de PCIe pueden aparecer como 0 para algunas plataformas.
- El informe de CUPS se renombró como SystemUsage en la versión 4.40.00.00 y es soportada por las plataformas INTEL y AMD.

Flujo de trabajo de telemetría:

1. Instale la licencia Datacenter, si no lo está.
2. Configure los ajustes globales de telemetría, lo que incluye la habilitación de la dirección de red y el puerto de red del servidor Rsyslog y de la telemetría mediante la IU de iDRAC, SCP, Redfish, o RACADM.
3. Configure los siguientes parámetros de transmisión del informe de telemetría en el informe o registro del dispositivo requerido utilizando la interfaz de RACADM o Redfish:
   - EnableTelemetry
   - ReportInterval
   - ReportTriggers

   NOTA: Habilite alertas de iDRAC y eventos de Redfish para el hardware específico sobre el cual necesita informes de telemetría.
4. El cliente de Redfish realiza una solicitud de suscripción al EventService de Redfish en iDRAC.
5. iDRAC genera e inserta el informe de métricas o los datos de registros y eventos en el cliente suscrito cuando se cumplen las condiciones predefinidas del generador.

Restricciones de la función:

1. Por motivos de seguridad, iDRAC solo es compatible con la comunicación con el cliente basada en HTTPS.
2. Por motivos de estabilidad, iDRAC es compatible con hasta ocho suscripciones.
3. La eliminación de suscripciones se admite únicamente a través de la interfaz de Redfish, incluso en el caso de la eliminación manual por parte del administrador.

Comportamiento de la función de telemetría:

- iDRAC genera e inserta (HTTP POST) el informe de métricas o los datos de registros y eventos en todos los clientes suscritos en el destino especificado en la suscripción cuando se cumplen las condiciones predefinidas del generador. Los clientes reciben nuevos datos solo después de la creación correcta de la suscripción.
- Entre los datos de métricas, se incluyen el registro de fecha y hora en formato ISO, horario UTC (termina en “Z”), en el momento de la recolección de datos desde la fuente.
- Los clientes pueden cancelar una suscripción mediante el envío de un mensaje ELIMINAR HTTP al URI del recurso de suscripción a través de la interfaz de Redfish.
- Si la suscripción se elimina mediante iDRAC o el cliente, iDRAC no envía informes (HTTP POST). Si la cantidad de errores de entrega supera los umbrales predefinidos, iDRAC puede eliminar una suscripción.
- Si un usuario tiene privilegios de administrador, puede eliminar las suscripciones, pero solo a través de la interfaz de Redfish.
- El cliente recibe una notificación acerca de la finalización de una suscripción a través de la iDRAC mediante el envío del evento “suscripción finalizada”, el cual será el último mensaje.
- Las suscripciones son persistentes y pueden permanecer incluso después de que se reinicie la iDRAC. Sin embargo, puede eliminar las suscripciones si realiza las operaciones `racresetcfg` o `racadm systemerase idrac`.
- En las interfaces de usuario, como RACADM, Redfish, SCP e iDRAC, se muestran el estado actual de las suscripciones del cliente.
- La disponibilidad de TelemetryService se puede comprobar mediante la adición del nuevo atributo `TelemetryServiceStatus` a la llamada de API `GetRemoteServiceAPIStatus`. Este atributo se agrega a la lista existente de LTStatus, RTStatus, ServerStatus y Status.

Definición de informe de métricas

Una definición de informe de métricas proporciona un medio para definir el conjunto de métricas que debe estar en un informe de telemetría y cómo se debe generar y transmitir el informe.

La transmisión de la telemetría de la iDRAC proporciona métricas que pueden proporcionar datos sobre el estado del servidor sin afectar el rendimiento del servidor principal. Entre estas métricas, se incluyen diversos parámetros del sistema, como uso de la CPU, uso de la memoria, consumo de energía, lecturas de temperatura y velocidad del ventilador, entre otros.

Importación y edición de la definición del informe de métricas

Si desea personalizar una definición de informe de métricas para sus necesidades específicas, importe la definición del informe de métricas y edite las propiedades.

1. Vaya a **Configuración** > **Ajustes del sistema** > **Configuración**
2. Seleccione el **Tipo de ubicación**.
3. Haga clic en **Elegir archivo** y seleccione el archivo.
4. Haga clic en **Importar**.
   Se importa el archivo del informe de métricas. El informe se muestra en la lista **Informes de telemetría**.
5. Si desea editar un informe de métricas específico, haga clic en **Acciones** > **Editar propiedades de informe** para ese informe específico.
   Aparece el cuadro de diálogo **Ajustes de informe**.
6. Edite los ajustes de informes y haga clic en **Guardar**.

Exportación de la definición del informe de métricas

Exporte la definición del informe de métricas si desea comparar el rendimiento de los servidores o usar el informe de métricas como plantilla para otros servidores.

1. Vaya a **Configuración** > **Ajustes del sistema** > **Configuración de telemetría** > **Definición del informe de métricas**.
2. Seleccione el **Tipo de ubicación**.
3. Seleccione la **Definición del informe de métricas**.
4. Haga clic en **Guardar**.
   Se guarda el archivo del informe de métricas.

Activadores

Los activadores de telemetría definen un conjunto de condiciones. En función de estas condiciones, se generan y transmiten los informes de métricas asociados. Las condiciones pueden incluir un evento del sistema o una condición definida por el usuario, como un valor de métrica que traspasa un límite de umbral o alcanza un valor igual a un valor discreto.

Los activadores se pueden configurar para monitorear una amplia variedad de condiciones, como fallas de hardware, cambios en el rendimiento del sistema u otros eventos significativos. La iDRAC envía el informe de métricas asociado mediante uno de los métodos de transmisión configurados. Estos métodos son Eventos enviados por el servidor (SSE) o Publicación en suscripción.

Exportación de activadores

Exporte los activadores si desea comparar los activadores de los servidores o utilizar el activador como plantilla para otros servidores.

1. Vaya a **Configuración** > **Ajustes del sistema** > **Configuración de telemetría** > **Activadores**.
2. Seleccione el **Tipo de ubicación**.
3. Seleccione el activador en la lista **Nombre de archivo**.
4. Haga clic en **Exportar**.
   El archivo de activadores se muestra en la lista **Activadores**.

Importación de activadores

Si desea personalizar un activador para sus necesidades específicas, importe el activador.

1. Vaya a **Configuración** > **Ajustes del sistema** > **Configuración de telemetría** > **Activadores**.
2. Seleccione el **Tipo de ubicación**.
3. Haga clic en **Elegir archivo** y seleccione el archivo.
4. Haga clic en **Importar**.
   Se importa el archivo activador. El activador se muestra en la lista **Activadores**.

Captura de datos en serie

iDRAC permite capturar la redirección en serie de la consola para su posterior recuperación con el uso de la característica de captura de datos en serie. Para esta característica, se requiere una licencia iDRAC Datacenter.

El propósito de la característica de captura de datos en serie es capturar los datos en serie del sistema y almacenarlos para que el cliente pueda recuperarlos posteriormente con 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, 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 o deshabilitar la captura de datos en serie mediante la interfaz de usuario de iDRAC, vaya a la página **Mantenimiento** > **Diagnósticos** > **Registros de datos en serie** y seleccione la casilla de verificación para habilitar o deshabilitar.

NOTA:
- Este atributo se mantiene después del reinicio de la iDRAC.
- El restablecimiento del firmware al valor predeterminado deshabilita esta característica.
- 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 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 se habilita la captura de datos en serie después de que el sistema haya arrancado, es necesario reiniciar el sistema, para que el BIOS pueda ver el nuevo ajuste (redirección de consola habilitada solicitada por la iDRAC) para obtener los datos en serie. La iDRAC comenzará a capturar los datos continuamente y los almacenará en la memoria compartida con un límite de 512 KB. Este buffer es circular.

NOTA:
- Para que esta función sea útil, debe contar con privilegios de inicio de sesión y privilegios de control del sistema.
- Para esta característica, se requiere una licencia iDRAC Datacenter.

Configuración dinámica de direcciones virtuales, iniciador y ajustes de objetivo de almacenamiento

Puede ver y configurar de forma dinámica la dirección virtual, el iniciador y el ajuste del destino de almacenamiento, y aplicar una política de persistencia. Permite que la aplicación realice los ajustes en función de los cambios en el estado de la alimentación (es decir, el reinicio del sistema operativo, el reinicio en caliente, el reinicio en frío o el ciclo de CA) y también en función de la configuración de la política de persistencia para ese estado de alimentación. Esto proporciona más flexibilidad en las implementaciones que requieren una reconfiguración rápida de las cargas de trabajo del sistema en otro sistema.

Las direcciones virtuales son:

- Dirección MAC virtual
- Dirección MAC iSCSI virtual
- Dirección MAC de FIP virtual
- WWN virtual
- WWPN virtual

NOTA: Cuando borra la política de persistencia, todas las direcciones virtuales se restablecen a la dirección permanente predeterminada establecida de fábrica.

NOTA: Algunas tarjetas con los atributos FIP virtual, WWN virtual y MAC WWPN virtual, los atributos WWN virtual y MAC WWPN virtual se configuran automáticamente cuando configura FIP virtual.

Con la característica de identidad de I/O, puede:

- Ver y configurar las direcciones virtuales para dispositivos de red y Fibre Channel (por ejemplo, NIC, CNA, FC HBA).
- Configurar el iniciador (para iSCSI y FCoE) y los ajustes de objetivo de almacenamiento (para iSCSI, FCoE y FC).
- Especificar la persistencia o la eliminación de los valores configurados en una pérdida de alimentación de CA del sistema y restablecimientos del sistema en frío y en caliente.

Los valores configurados para las direcciones virtuales, el iniciador y los destinos de almacenamiento pueden cambiar en función de la manera en que se maneja la alimentación principal durante el restablecimiento del sistema y de si el dispositivo HBA de la NIC, CNA o Fibre

Channel tiene alimentación auxiliar. La persistencia del ajuste de identidad de E/S se puede lograr en función de la configuración de la política establecida mediante la iDRAC.

Solo si la función de identidad de E/S está activada, se aplican las políticas de persistencia. Cada vez que el sistema se reinicia o se enciende, los valores se conservan o se borran en función del ajuste de la política.

NOTA: Una vez que se borran los valores, no puede volver a aplicar los valores antes de ejecutar el trabajo de configuración.

Ver el soporte de optimización de identidad de E/S en la interfaz web

En las **Propiedades de Puerto** de la tarjeta NIC específica (**Sistema** > **Dispositivos de red**), si la **funcionalidad Política de Persistencia** se muestra **Apta** para la tarjeta NIC específica, la tarjeta es compatible con la Optimización de Identidad de I/O.

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 36. 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 política de persistencia: dirección virtual
Dirección asignada de manera remota activada	Modo RemoteAssignedAddress	Habilitado	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	Habilitado	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 RemoteAssignedAddress	Deshabilitado	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 RemoteAssignedAddress	Deshabilitado	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 RemoteAssignedAddress	Habilitado	VAM configurada	VAM configurada persiste	Solo persistencia: No es posible borrar
Dirección asignada de manera remota desactivada	Modo RemoteAssignedAddress	Habilitado	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 RemoteAssignedAddress	Deshabilitado	Se configura mediante la ruta proporcionada en Lifecycle Controller	La configuración de Lifecycle Controller persiste durante ese ciclo	No se admite persistencia. Depende del comportamiento de la tarjeta

Tabla 36. 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 política de persistencia: dirección virtual
Dirección asignada de manera remota desactivada	Modo RemoteAssignedAddress	Deshabilitado	VAM no configurada	Establecer en dirección MAC de hardware	Establecer en dirección MAC de hardware
Dirección asignada de manera remota activada	Modo de consola	Habilitado	VAM configurada	VAM configurada persiste	Persistencia y borrado deben funcionar
Dirección asignada de manera remota activada	Modo de consola	Habilitado	VAM no configurada	Establecer en dirección MAC de hardware	Establecer en dirección MAC de hardware
Dirección asignada de manera remota activada	Modo de consola	Deshabilitado	Se configura mediante la ruta 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 de consola	Habilitado	VAM configurada	VAM configurada persiste	Persistencia y borrado deben funcionar
Dirección asignada de manera remota desactivada	Modo de consola	Habilitado	VAM no configurada	Establecer en dirección MAC de hardware	Establecer en dirección MAC de hardware
Dirección asignada de manera remota desactivada	Modo de consola	Deshabilitado	Se configura mediante la ruta 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	Deshabilitado	VAM no configurada	Establecer en dirección MAC de hardware	Establecer en dirección MAC de hardware

NOTA:

- La configuración de reemplazo de piezas para tarjetas compatibles con particiones funciona correctamente cuando VirtualizationMode (el atributo para activar el número de particiones) es igual que la tarjeta reemplazada y la tarjeta NIC presente en el servidor.
- La configuración de reemplazo de piezas no se activa cuando VirtualizationMode (número de particiones) de la tarjeta reemplazada no coincide con la tarjeta NIC presente en el servidor.
- En la ventana Reemplazo de partes antes de CSIOR, Lifecycle Controller restaura la configuración de NIC. Esto implica un arranque en frío seguido de un arranque mediante sistema operativo. Después de ambos reinicios, la NIC tiene el mismo firmware que se instala durante el proceso de restauración.
- La política de persistencia se aplica a cada reinicio según la política. En el arranque mediante suministro de energía, las identidades virtuales no se aplican debido a la incompatibilidad de la versión del firmware y a la eliminación de los datos de persistencia.
- La característica de la política de persistencia comprueba las ID de PCI y la versión del firmware de la NIC actual y anterior del mismo proveedor que se reemplaza. En caso de que estos campos no coincidan, no se aplican las identidades virtuales y los datos de persistencia (identidades virtuales) también se eliminan del iDRAC.
- Para el reemplazo de piezas, el proveedor debe mantener los mismos ID de PCI y la misma versión del firmware, o debe realizar una implementación de trabajo/plantilla de VAM.

Comportamiento del sistema para FlexAddress e identidad de E/S

Tabla 37. Comportamiento del sistema para FlexAddress e identidad de I/O

Tipo	Estado de la característica FlexAddress en CMC	Estado de la función de identidad de E/S en el iDRAC	Disponibilidad del agente remoto VA para el ciclo de reinicio	Fuente de programación VA	Comportamiento de persistencia del VA del ciclo de reinicio
Servidor con persistencia equivalente a FA	Habilitado	Deshabilitado	N/D	FlexAddress desde CMC	Según las especificaciones de FlexAddress
	N/A, habilitado o deshabilitado	Habilitado	Sí: nuevo o persistente	Dirección virtual del agente remoto	Según las especificaciones de FlexAddress
			No	Dirección virtual borrada	
	Deshabilitado	Deshabilitado	N/D	N/D	N/D
Servidor con la característica de política de persistencia de VAM	Habilitado	Deshabilitado	N/D	FlexAddress desde CMC	Según las especificaciones de FlexAddress
	Habilitado	Habilitado	Sí: nuevo o persistente	Dirección virtual del agente remoto	Por configuración de política de agente remoto
			No	FlexAddress desde CMC	Según las especificaciones de FlexAddress
	Deshabilitado	Habilitado	Sí: nuevo o persistente	Dirección virtual del agente remoto	Por configuración de política de agente remoto
			No	Dirección virtual borrada	
	Deshabilitado	Deshabilitado	N/D	N/D	N/D

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.

NOTA: Los atributos de identidad de I/O solo se deben configurar mediante SCP para que sean persistentes durante los reinicios. Si se utilizan otros métodos para configurarlos, no serán persistentes.

Para obtener la lista de atributos de optimización de la identidad de I/O que puede modificar en el archivo SCP, consulte el documento **Perfil de NIC** disponible en Página Soporte de Dell.

NOTA: No modifique los atributos que no corresponden a la optimización de la identidad de I/O.

Habilitación o deshabilitación de la optimización de la identidad de I/O mediante la interfaz web

Para habilitar o deshabilitar la optimización de la identidad de I/O:

1. En la interfaz web de iDRAC, vaya a **Configuración** > **Configuración del sistema** > **Configuración de hardware** > **Optimización de identidad de E/S**.
   Se muestra la página con la lista de **Optimización de identidad de I/O**.
2. Haga clic en la pestaña **Optimización de identidad de I/O** y seleccione la opción **Habilitada** para habilitar esta característica. Para desactivarlo, borre esta opción.
3. Haga clic en **Aplicar** para aplicar la configuración.

Habilitación o deshabilitación de la optimización de identidad de I/O mediante la RACADM

Para habilitar la optimización de identidad de I/O, utilice el comando:

```
racadm set idrac.ioidopt.IOIDOptEnable Enabled
```

Después de habilitar esta característica, debe reiniciar el sistema para que los ajustes surtan efecto.

Para deshabilitar la optimización de identidad de I/O, utilice el comando:

```
racadm set idrac.ioidopt.IOIDOptEnable Disabled
```

Para ver la configuración de optimización de identidad de I/O, 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 característica **Política de persistencia** no funcione cuando se establece como valor predeterminado. Si el atributo **VirtualAddressManagement** está establecido en **FlexAddress** en la iDRAC, asegúrese de configurar el atributo **VirtualAddressManagement** en modo de **Consola** en la iDRAC.

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 o notificaciones de correo electrónico. Los registros también se incluyen en los registros del sistema remoto.

Valores predeterminados para la política de persistencia

Tabla 38. 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	Seleccionados	Seleccionados
Dirección virtual: dispositivos que no son de alimentación auxiliar	No seleccionado	No seleccionado	Seleccionados
Iniciador	Seleccionados	Seleccionados	Seleccionados

Tabla 38. Valores predeterminados para la política de persistencia (continuación)

Política de persistencia	Pérdida de alimentación de CA	Reinicio mediante suministro de energía	Reinicio mediante sistema operativo
Destino de almacenamiento	Seleccionados	Seleccionados	Seleccionados

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.

Configuración de los ajustes 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 pestaña **Optimización de identidad de I/O**.
3. En la sección **Política de persistencia**, seleccione una o más 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 configuraron las políticas de persistencia.

Configuración de los ajustes de la política de persistencia mediante RACADM

Para configurar la política de persistencia, utilice el siguiente objeto racadm 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 objetivos de almacenamiento, utilice el objeto **iDRAC.IOIDOpt.StorageTargetPersistencePolicy**

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 39. Iniciador iSCSI: valores predeterminados

Iniciador iSCSI	Valores predeterminados en modo IPv4	Valores predeterminados en modo IPv6
IscsiInitiatorIpAddr	0.0.0.0	::

Tabla 39. Iniciador iSCSI: valores predeterminados (continuación)

Iniciador iSCSI	Valores predeterminados en modo IPv4	Valores predeterminados en modo IPv6
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 40. 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	Deshabilitado	Deshabilitado
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	NA
ConnectSecondTgt	Deshabilitado	Deshabilitado
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	NA

19

Administración de dispositivos de almacenamiento

La iDRAC es compatible con las controladoras PERC 12 y BOSS N1.

NOTA: El borrado de la caché de hardware falla en una controladora PERC12 externa configurada. Ejecute la operación de restablecimiento de la configuración antes de realizar el borrado de la caché de hardware.

NOTA:

- Las controladoras BOSS soportan solo RAID 0 y RAID 1.
- Todos los discos virtuales externos que se detecten detrás de las controladoras BOSS se deben borrar de la HII del BIOS o mediante la operación de restablecimiento de la controladora.
- En el caso de los controladores BOSS, es posible que la información completa de VD no se encuentre disponible si se desconectan y se vuelven a conectar ambos PD.
- En el caso de que una actualización requiera el restablecimiento/reinicio de iDRAC o se reinicie iDRAC, se recomienda verificar si iDRAC se encuentra completamente listo; para ello, espere unos segundos hasta un máximo de 5 minutos antes de usar cualquier otro comando.
- Para PERC12, la expansión de la capacidad en línea (OCE) con adición de unidades solo es posible en un disco virtual de tamaño completo. No se realiza OCE con adición de unidades en discos virtuales segmentados.
- Para evitar cualquier error impredecible, se recomienda no realizar ninguna operación relacionada con el almacenamiento cuando existe un trabajo de almacenamiento en curso.

iDRAC ha expandido la administración sin agentes para incluir la configuración directa de las controladoras PERC. Es posible configurar de manera remota los componentes de almacenamiento conectados al sistema en el tiempo de ejecución. Entre estos componentes, se incluyen las controladoras RAID y que no son RAID, los canales, los puertos, los chasis y los discos conectados a estos componentes.

Las tareas de detección, topología, supervisión de estado y configuración de todo el subsistema de almacenamiento se realizan con el marco de trabajo de administración incorporada completa (CEM) realizando una interfaz con las controladoras PERC internas y externas a través de la interfaz de protocolo MCTP mediante I2C.

NOTA: CEM no soporta el RAID de software (SWRAID) y, por lo tanto, no se soporta en la interfaz de usuario de iDRAC. SWRAID se puede administrar mediante RACADM o Redfish.

Con iDRAC, es posible realizar la mayoría de las funciones que se encuentran disponibles en OpenManage Storage Management, lo que incluye los comandos de configuración (sin reinicio) en tiempo real (por ejemplo, la creación de un disco virtual). También es posible configurar completamente RAID antes de instalar el sistema operativo.

Es posible configurar y administrar las funciones de la controladora sin tener acceso al BIOS. Estas funciones incluyen la configuración de discos virtuales y la aplicación de niveles de RAID y repuestos dinámicos para la protección de los datos. Es posible iniciar muchas otras funciones de la controladora, como la recreación y la solución de problemas. Para proteger los datos, se puede configurar la redundancia de datos o asignar repuestos dinámicos.

NOTA: Si se habilita la configuración del BIOS para Volume Management Device (VMD) (con soporte para módulos de ID) en un servidor PowerEdge, evite configurar unidades NVMe conectadas a la CPU para prevenir comportamientos impredecibles.

Los dispositivos de almacenamiento son:

- Controladoras: la mayoría de los sistemas operativos no leen datos directamente de los discos ni los escriben en ellos, sino que envían instrucciones de lectura y escritura a una controladora. La controladora es el hardware del sistema que interactúa directamente con los discos para escribir y recuperar datos. La controladora tiene conectores (canales o puertos) que están conectados a uno o más discos físicos o a un chasis que contiene discos físicos. Las controladoras RAID pueden organizar los límites de los discos en forma de tramos para crear una cantidad extendida de espacio de almacenamiento o un disco virtual mediante la capacidad de varios discos. Las controladoras también realizan otras tareas, como el inicio de recreaciones, la inicialización de discos y mucho más. Para completar sus tareas, las controladoras requieren un software especial, conocido como firmware y drivers. Para funcionar correctamente, la controladora debe tener instalada la versión mínima requerida del firmware y de los drivers. Cada controladora lee y escribe datos y realiza tareas de diferente manera. Para administrar el almacenamiento eficientemente, se recomienda entender dichas funciones.

- Discos o dispositivos físicos: estos residen dentro de un gabinete o están conectados a la controladora. En una controladora RAID, estos discos o dispositivos físicos se utilizan para crear discos virtuales.
- Disco virtual: es el almacenamiento creado por una controladora RAID a partir de uno o varios discos físicos. Aunque se puede crear un disco virtual a partir de varios discos físicos, el sistema operativo lo verá como un solo disco. Según el nivel de RAID usado, es posible que el disco virtual retenga datos redundantes en caso de una falla de disco o tenga atributos de rendimiento particulares. Los discos virtuales solo se pueden crear en una controladora RAID.
- Gabinete: se conecta al sistema de manera externa, mientras que el backplane y los discos físicos son internos. Si los gabinetes se conectan en una configuración de múltiples rutas, asegúrese de que se utilicen las siguientes combinaciones de puertos para conectarse a las controladoras:
  - Puerto 0 y puerto 2
  - Puerto 1 y puerto 3
- Backplane: es similar a un gabinete. En un plano posterior, el conector de la controladora y los discos físicos se conectan a un chasis, pero no se pueden usar las funciones de administración (sondas de temperatura, alarmas, etc.) asociadas con los chasis externos. Los discos físicos pueden ubicarse en un chasis o conectarse al plano posterior de un sistema.

NOTA: La configuración máxima con alrededor de 192 unidades físicas puede tardar un mínimo de 30 minutos en completar el inventario.

NOTA: Cuando un sistema tiene una amplia variedad de componentes de almacenamiento, como 240 discos virtuales y 60 unidades, se espera que ciertas operaciones de almacenamiento pendientes u operaciones de descarte pendientes puedan arrojar fallas junto con el error RAC0508.

NOTA: Cuando uno o varios backplanes se conectan a un expansor, la posición del gabinete se muestra como **Desconocida**.

NOTA: En algunas plataformas, la extracción/inserción activa del SLED no es soportada, y es posible que vea algunos errores inesperados. Se debe apagar antes de la extracción/inserción activa.

Además de administrar los discos físicos del chasis, puede supervisar el estado de los ventiladores, el suministro de energía y las sondas de temperatura del chasis. Es posible conectar chasis mediante acoplamiento activo. El acoplamiento activo se define como la incorporación de un componente a un sistema mientras el sistema operativo aún está ejecutándose.

NOTA: El estado de las unidades que se extraen en caliente se indica como **Eliminado**, y la información de la unidad queda disponible en los inventarios de hardware y firmware hasta el próximo reinicio del host.

Los dispositivos físicos conectados a la controladora deben tener el firmware más reciente. Para obtener el firmware compatible más reciente, comuníquese con su proveedor de servicios.

NOTA: Si realiza la actualización de firmware de la unidad en unidades conectadas en caliente, es posible que se pierda el registro de PR36 en los registros de LifeCycle, aunque la actualización se realice correctamente. Para evitar esto, reinicie el host antes de la actualización de firmware.

NOTA: PR36 no se registra para las baterías de reserva (BBU) y las unidades de procesamiento de datos (DPU) después de las actualizaciones de firmware.

Los eventos de almacenamiento procedentes de PERC se asignan a excepciones de SNMP según corresponda. Todos los cambios en las configuraciones de almacenamiento se registran en el registro de Lifecycle.

NOTA: Después de un reinicio flexible del servidor, es posible que iDRAC informe el registro de PDR8 LC para las unidades conectadas detrás de las controladoras PERC.

NOTA: En iDRAC, puede ver el backplane/gabinete asociado con la controladora PERC del sistema. Este gabinete informa 16 ranuras (a pesar de que el sistema no soporta tantas unidades).

En los sistemas en los que las unidades se conectan por cable directamente a la controladora RAID, se crea una entrada para cada posible conexión de una unidad a PERC. PERC soporta hasta 16 unidades conectadas por cable, por lo que se informan 16 ranuras.

Tabla 41. Capacidad de PERC

Capacidad de PERC	Controladora con capacidad de configuración CEM
Tiempo real	Si existen trabajos programados o pendientes para alguna controladora, es necesario borrar los trabajos o esperar a que se completen antes de aplicar la configuración en el momento de ejecución. No se requiere un reinicio para los trabajos en tiempo de ejecución o en tiempo real.
Organizado en etapas	N/D

Temas:

Comprensión de los conceptos de RAID

Storage Management utiliza la tecnología de arreglo redundante de discos independientes (RAID) para proporcionar capacidad a Storage Management. Para entender Storage Management es necesario conocer los conceptos de RAID, y saber cómo las controladoras RAID y el sistema operativo del sistema perciben el espacio del disco.

¿Qué es RAID?

RAID es una tecnología para administrar el almacenamiento de los datos en los discos físicos que residen o que están conectados en el sistema. Un aspecto clave de RAID es la capacidad de organizar los discos físicos en forma de tramos, de modo que la capacidad de almacenamiento combinada de varios discos físicos se pueda tratar como un solo espacio de disco ampliado. Otro aspecto clave de RAID es la capacidad para mantener datos redundantes que se pueden usar para restaurar la entrada de datos en caso de una falla del disco. RAID usa técnicas diferentes, como el seccionamiento, la duplicación y la paridad, para almacenar y reconstruir datos. Hay distintos niveles RAID que usan métodos diferentes para almacenar y reconstruir datos. Los niveles RAID tienen características diferentes en cuanto a rendimiento de lectura/escritura, protección de datos y capacidad de almacenamiento. No todos los niveles RAID mantienen datos redundantes, lo que significa que, para algunos niveles RAID, los datos perdidos no se pueden restaurar. La elección de un nivel RAID depende de si la prioridad es el rendimiento, la protección o la capacidad de almacenamiento.

NOTA: La placa de aviso de RAID (RAB) define las especificaciones que se utilizan para implementar RAID. Aunque la RAB define los niveles RAID, la implementación comercial de los niveles RAID de distintos proveedores puede variar con respecto a las especificaciones reales de RAID. 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 de hardware y software

RAID puede implementarse mediante hardware o software. Un sistema que usa RAID por hardware tiene una controladora RAID que implementa los niveles RAID y procesa la lectura y la escritura de los datos en los discos físicos. Cuando se usa el RAID por hardware que proporciona el sistema operativo, el sistema operativo implementa los niveles RAID. Por esta razón, la utilización de RAID por software por sí mismo puede reducir el rendimiento del sistema. Sin embargo, puede usar RAID por software junto con volúmenes RAID por hardware para proporcionar mejor rendimiento y variedad en la configuración de volúmenes RAID. Por ejemplo, puede reflejar un par de volúmenes RAID 5 por hardware entre dos controladoras RAID a fin de proporcionar redundancia de la controladora RAID.

Conceptos de RAID

RAID utiliza técnicas particulares para escribir datos en los discos. Estas técnicas permiten que RAID proporcione una redundancia de datos o un mejor rendimiento. Estas técnicas incluyen:

- Reflejado: duplicación de datos de un disco físico en otro disco físico. El reflejado proporciona redundancia de datos porque se mantienen dos copias de los mismos datos en discos físicos distintos. Si uno de los discos en el reflejo falla, el sistema puede continuar funcionando con el uso del disco que no está afectado. Ambos lados del reflejo contienen siempre los mismos datos. Cualquier lado del reflejo puede actuar como el lado operativo. Un grupo de discos RAID reflejado es comparable en rendimiento a un grupo de discos RAID 5 con respecto a las operaciones de lectura, pero es más rápido en las operaciones de escritura.
- Seccionamiento: el seccionamiento de discos graba los datos en todos los discos físicos de un disco virtual. Cada banda consta de direcciones de datos de disco virtual consecutivos que se asignan en unidades de tamaño fijo a cada disco físico del disco virtual con un patrón secuencial. Por ejemplo, si el disco virtual incluye cinco discos físicos, en la banda se escriben datos en los discos físicos del uno al cinco sin repetir ninguno de los discos físicos. La cantidad de espacio que consume una banda es la misma en todos los discos físicos. La parte de una banda que reside en un disco físico es un elemento de banda. La división de datos en bandas por sí sola no proporciona redundancia de datos. En combinación con la paridad sí que proporciona redundancia de datos.
- Tamaño de la sección: espacio total de disco que consume una sección, sin incluir un disco de paridad. Por ejemplo, piense en 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 banda: un elemento banda es la parte de una banda que se aloja en un solo disco físico.
- Tamaño del elemento de la sección: cantidad de espacio del disco que consume un elemento de la sección. Por ejemplo, piense en una sección que contiene 64 KB de espacio en el disco y que tiene 16 KB de datos que residen en cada disco en la sección. En este caso, el tamaño del elemento de la sección es de 16 KB y el tamaño de la sección es de 64 KB.
- Paridad: la paridad se refiere a los datos redundantes que se mantienen con el uso de un algoritmo en combinación con el seccionamiento. Cuando uno de los discos seccionados falla, los datos pueden reconstruirse a partir de la información de paridad con el uso del 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 de RAID

Cada nivel de RAID utiliza alguna combinación de reflejado, seccionamiento y paridad para proporcionar una redundancia de datos o un mejor rendimiento de lectura y escritura. Para obtener más información específica sobre cada nivel de RAID, consulte Elección de niveles de RAID.

Organización del almacenamiento de datos para obtener disponibilidad y rendimiento

RAID proporciona distintos métodos o niveles RAID para organizar el almacenamiento de disco. Algunos niveles RAID mantienen datos redundantes para que usted pueda restaurar los datos después de una falla del disco. Los distintos niveles RAID pueden implicar también un aumento o disminución en el rendimiento de E/S (lectura y escritura) del sistema.

El mantenimiento de datos redundantes requiere el uso de discos físicos adicionales. Entre más discos se vean involucrados, aumenta la probabilidad de una falla del disco. A causa de las diferencias en la redundancia y en el rendimiento de E/S, un nivel RAID puede ser más apropiado que otro según las aplicaciones que se utilicen en el entorno operativo y la naturaleza de los datos que se almacenen.

Al elegir un nivel RAID, se aplican las siguientes consideraciones de rendimiento y costo:

- **Disponibilidad o tolerancia ante fallas**: la disponibilidad o tolerancia a fallas se refiere a la capacidad que el sistema tiene para mantener las operaciones y proporcionar acceso a los datos aun cuando alguno de sus componentes haya fallado. En los volúmenes RAID, la disponibilidad o tolerancia ante fallas se consigue mediante el mantenimiento de datos redundantes. Los datos redundantes incluyen reflejos (datos duplicados) e información de paridad (reconstrucción de los datos mediante un algoritmo).
- **Rendimiento**: el rendimiento de lectura y escritura puede aumentar o disminuir según el nivel RAID que elija. Algunos niveles RAID pueden ser más apropiados para ciertas aplicaciones.
- **Optimización del costo**: el mantenimiento de datos redundantes o de información de paridad en relación con volúmenes RAID requiere de espacio de disco adicional. En situaciones en las que los datos son temporales, de fácil reproducción o no esenciales, es posible que no se justifique el aumento en el costo de la redundancia de datos.
- **Tiempo promedio entre fallas (MTBF)**: el uso de discos adicionales para mantener la redundancia de los datos también aumenta la probabilidad de sufrir fallas de disco en un momento determinado. Aunque esto no se puede evitar en situaciones en las que los datos redundantes son una necesidad, realmente puede repercutir en la carga de trabajo del personal de asistencia de sistemas de la organización.

- **Volumen**: el volumen se refiere a un solo disco virtual no RAID. Puede crear volúmenes mediante utilidades externas, como el O-ROM <Ctrl> <r>. Storage Management no admite la creación de volúmenes. Sin embargo, puede ver volúmenes y usar unidades de estos volúmenes para crear nuevos discos virtuales o para la expansión de la capacidad en línea (OCE) de los discos virtuales existentes, siempre que tenga espacio libre disponible.

Selección de niveles RAID

Puede usar RAID para controlar el almacenamiento de datos en varios discos. Cada nivel RAID o concatenación tiene distintos rendimientos y características de protección de datos.

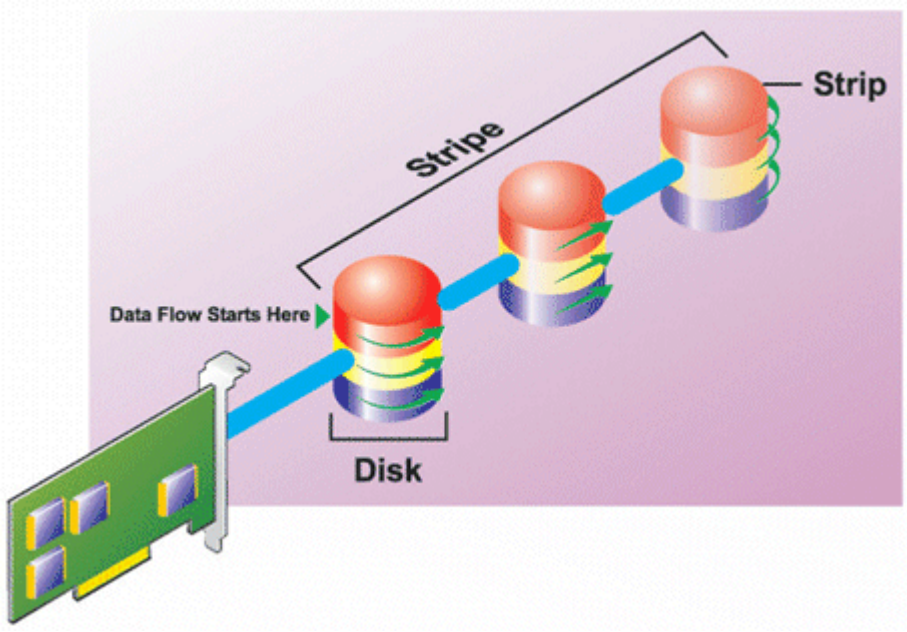
NOTA: Las controladoras PERC H3xx no soportan los niveles de RAID 6 y 60.

Los temas siguientes proporcionan 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 (fraccionado)
- Nivel RAID 1 (espejeado)
- Nivel RAID 5 (fraccionado con paridad distribuida)
- Nivel RAID 6 (fraccionado con paridad distribuida adicional)
- Nivel RAID 50 (fraccionado en conjuntos de RAID 5)
- Nivel RAID 60 (fraccionado en conjuntos de RAID 6)
- Nivel RAID 10 (fraccionado de conjuntos en espejo)

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.

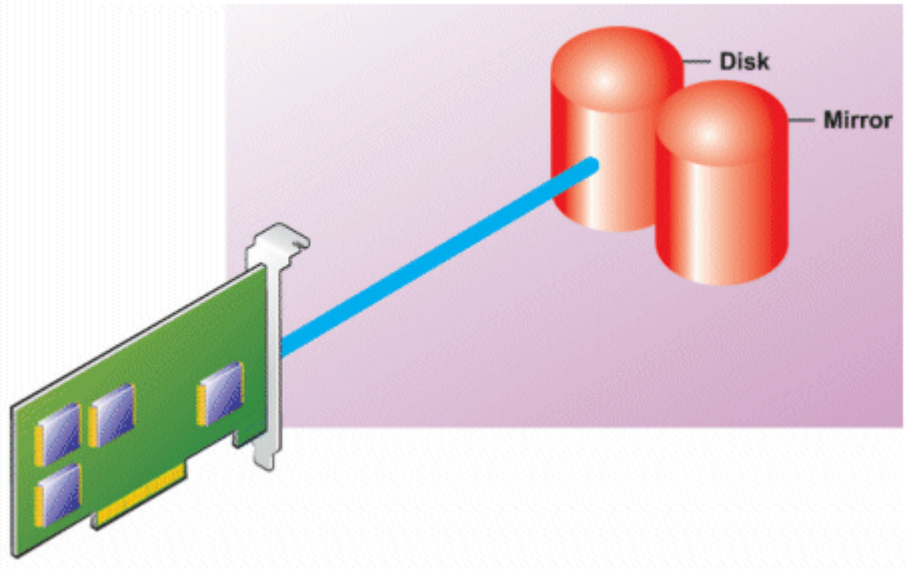


Características de RAID 0:

- 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 RAID 1 (espejeado)

RAID 1 es la forma más sencilla de mantener datos redundantes. En RAID 1, los datos se reflejan en uno o varios discos físicos. Si un disco físico genera errores, los datos pueden recrearse mediante el uso de los datos del otro lado del duplicado.

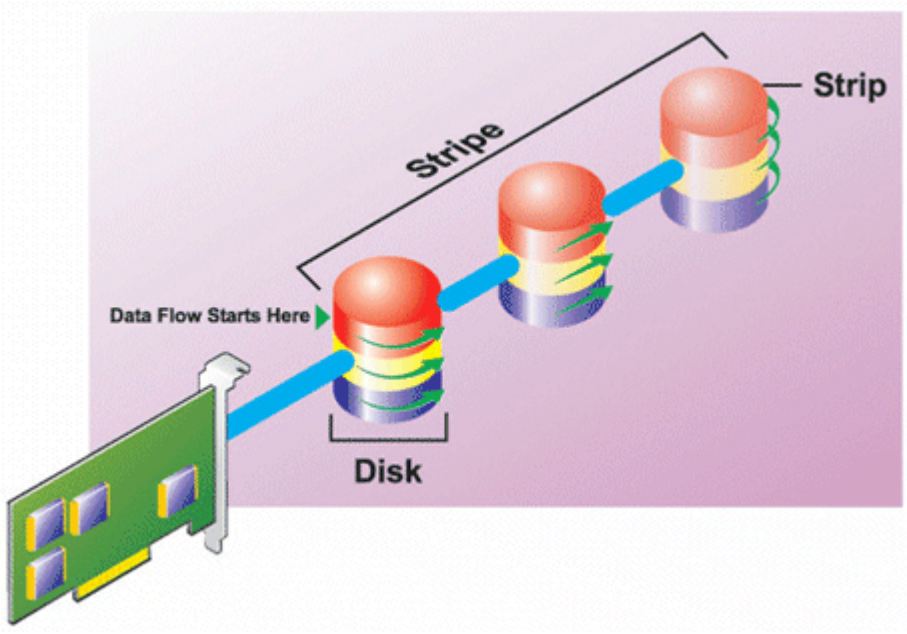


Características de RAID 1:

- Agrupa **n** + **n** discos como un disco virtual con la capacidad de **n** discos. Las controladoras que actualmente admite Storage Management permiten seleccionar dos discos cuando se crea un RAID 1. Debido a que estos discos se reflejan, la capacidad total de almacenamiento equivale a un disco.
- Los datos se copian en ambos discos.
- Cuando un disco falla, el disco virtual sigue funcionando. Los datos se leen desde el duplicado del disco fallido.
- Mejor rendimiento de lectura, pero un rendimiento de escritura ligeramente menor.
- Hay redundancia para la protección de datos.
- RAID 1 es más costoso en términos de espacio de disco, ya que se utiliza el doble de discos de lo que se requiere para almacenar los datos sin redundancia.

Nivel RAID 5 o fraccionado con paridad distribuida

RAID 5 proporciona redundancia de datos mediante el uso del seccionamiento de datos en combinación con la información de paridad. Sin embargo, en vez de dedicar un disco físico a la paridad, la información de paridad se secciona entre todos los discos físicos en el grupo de discos.

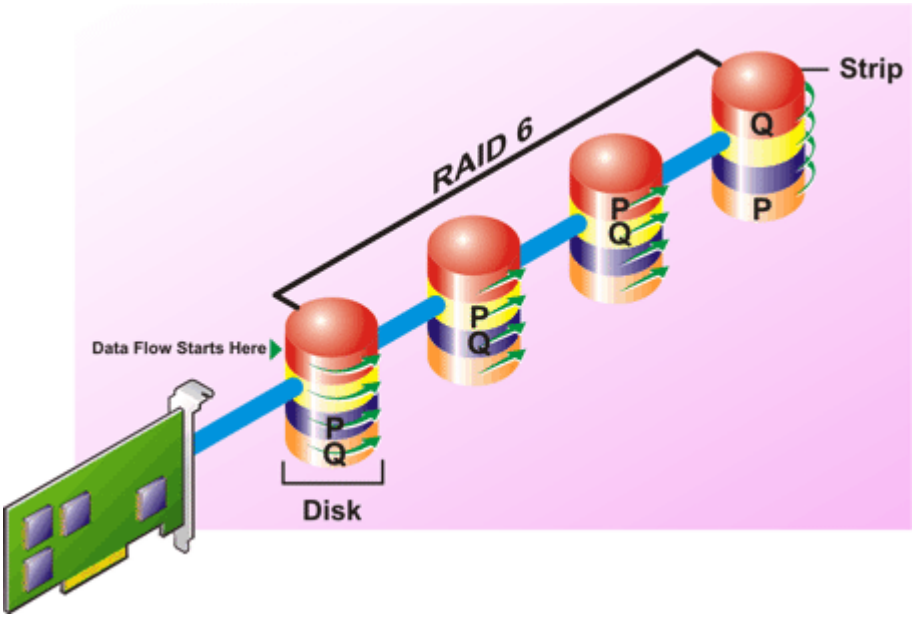


Características de RAID 5:

- Agrupa **n** discos en un disco virtual grande con capacidad de (**n**-1) discos.
- La información redundante (paridad) se almacena alternadamente entre todos los discos.
- Cuando un disco falla, el disco virtual seguirá funcionando, pero funcionará en estado degradado. Los datos se reconstruyen a partir de los discos que sobrevivan.
- Mejor rendimiento de lectura, pero un rendimiento de escritura más lento.
- Hay redundancia para la protección de datos.

Nivel RAID 6: fraccionado con paridad distribuida adicional

RAID 6 proporciona redundancia de datos mediante el uso del seccionamiento de datos en combinación con la información de paridad. Tal como sucede en RAID 5, la paridad se distribuye dentro de cada sección. Sin embargo, RAID 6 utiliza un disco físico adicional para mantener la paridad, de manera que cada sección en el grupo de discos mantiene dos bloques de disco con información de paridad. La paridad adicional proporciona protección de datos en caso de que se produzcan fallas en los dos discos. En la siguiente imagen, los dos conjuntos de información de paridad se identifican como **P** y **Q**.



Características de RAID 6:

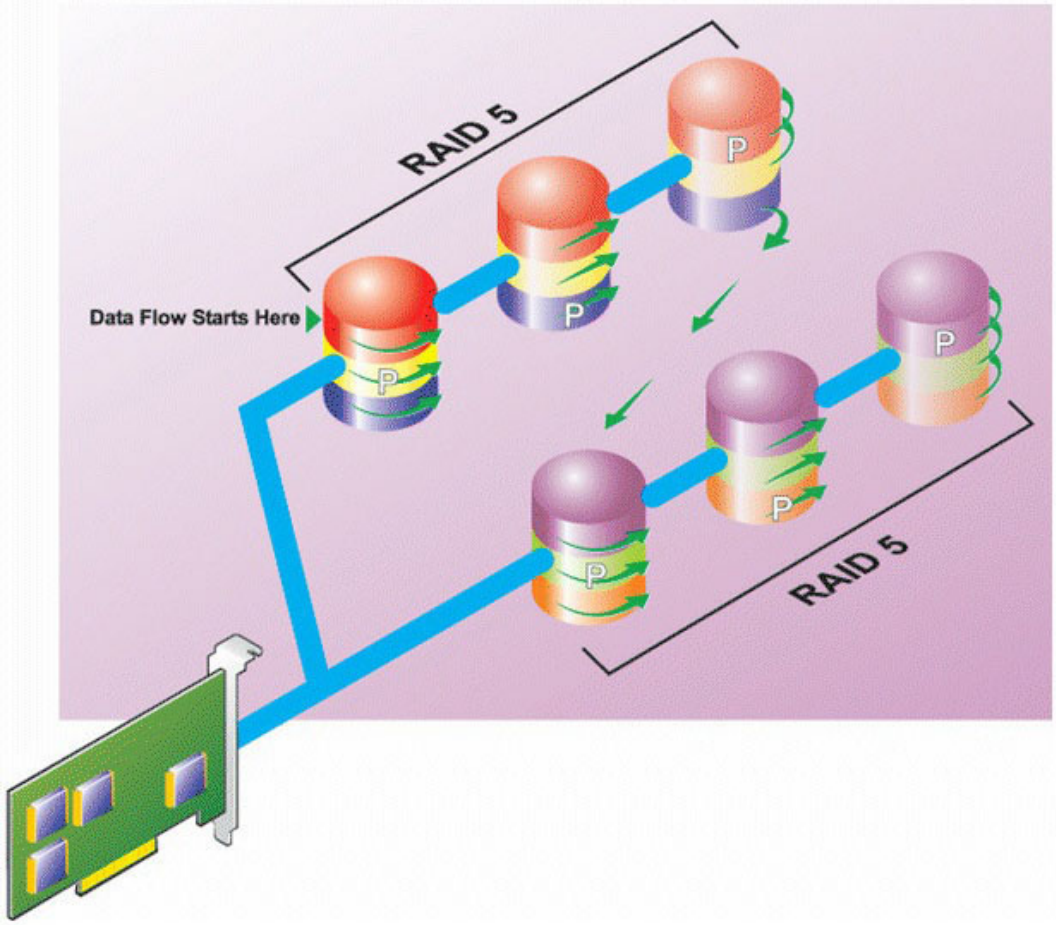
- Agrupa **n** discos en un disco virtual grande con capacidad de (**n**-2) discos.

- La información redundante (paridad) se almacena alternadamente entre todos los discos.
- El disco virtual sigue funcionando hasta con dos fallos de disco. Los datos se reconstruyen a partir de los discos que sobrevivan.
- Mejor rendimiento de lectura, pero un rendimiento de escritura más lento.
- Mayor redundancia para la protección de datos.
- Se requieren dos discos por tramo para la paridad. RAID 6 es más costoso en términos de espacio de disco.

Nivel RAID 50: fraccionado en conjuntos de RAID 5

RAID 50 es el seccionamiento en más de un tramo de discos físicos. Por ejemplo, un grupo de discos RAID 5 que esté implementado con tres discos físicos y, luego, continúe con un grupo de tres discos físicos adicionales sería un RAID 50.

Es posible implementar RAID 50, incluso cuando el hardware no lo admita directamente. En este caso, puede implementar varios discos virtuales de RAID 5 y, a continuación, convertir los discos de RAID 5 en discos dinámicos. A partir de ahí, puede crear un volumen dinámico que se extienda a todos los discos virtuales de RAID 5.

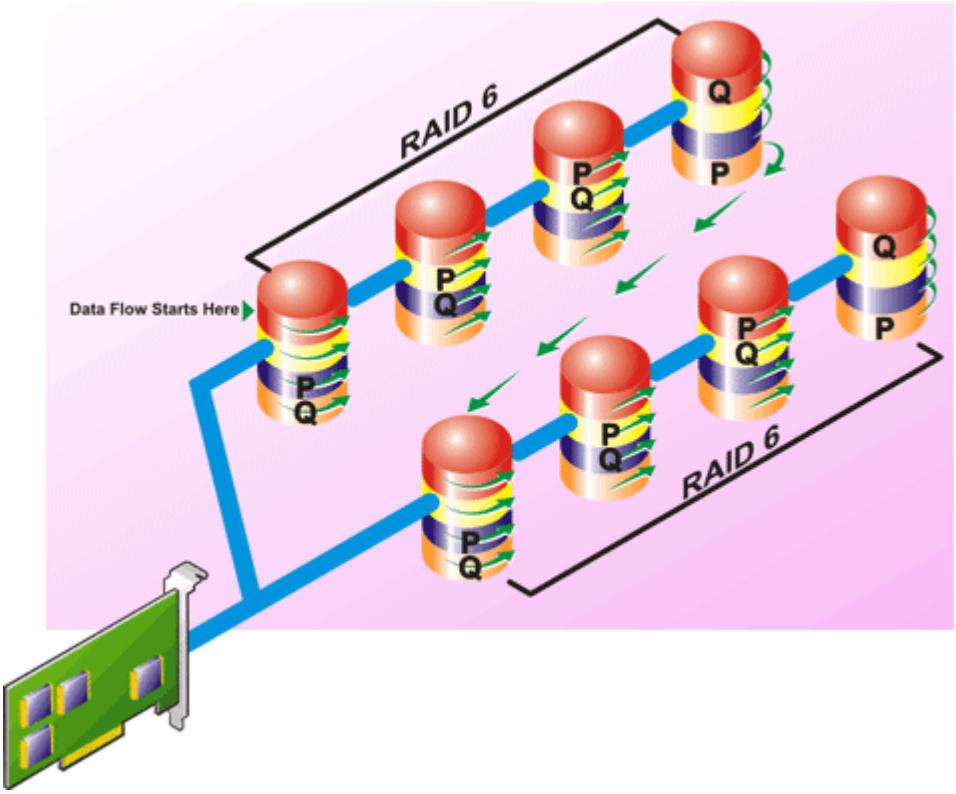


Características de RAID 50:

- Agrupa discos **n*****s** para formar un disco virtual grande con capacidad de discos **s***(**n**-1), en el que **s** representa el número de tramos y **n** es el número de discos dentro de cada tramo.
- La información redundante (paridad) se almacena alternadamente en todos los discos de cada tramo de RAID 5.
- Mejor rendimiento de lectura, pero un rendimiento de escritura más lento.
- Se requiere tanta información de paridad como en RAID 5 convencional.
- Los datos se seccionan en todos los tramos. RAID 50 es más costoso en términos de espacio de disco.

Nivel RAID 60: fraccionado en conjuntos de RAID 6

RAID 60 se secciona en más de un tramo de discos físicos configurados como RAID 6. Por ejemplo, un grupo de discos RAID 6 que esté implementado con cuatro discos físicos y, luego, continúe con un grupo de cuatro discos físicos adicionales sería un RAID 60.

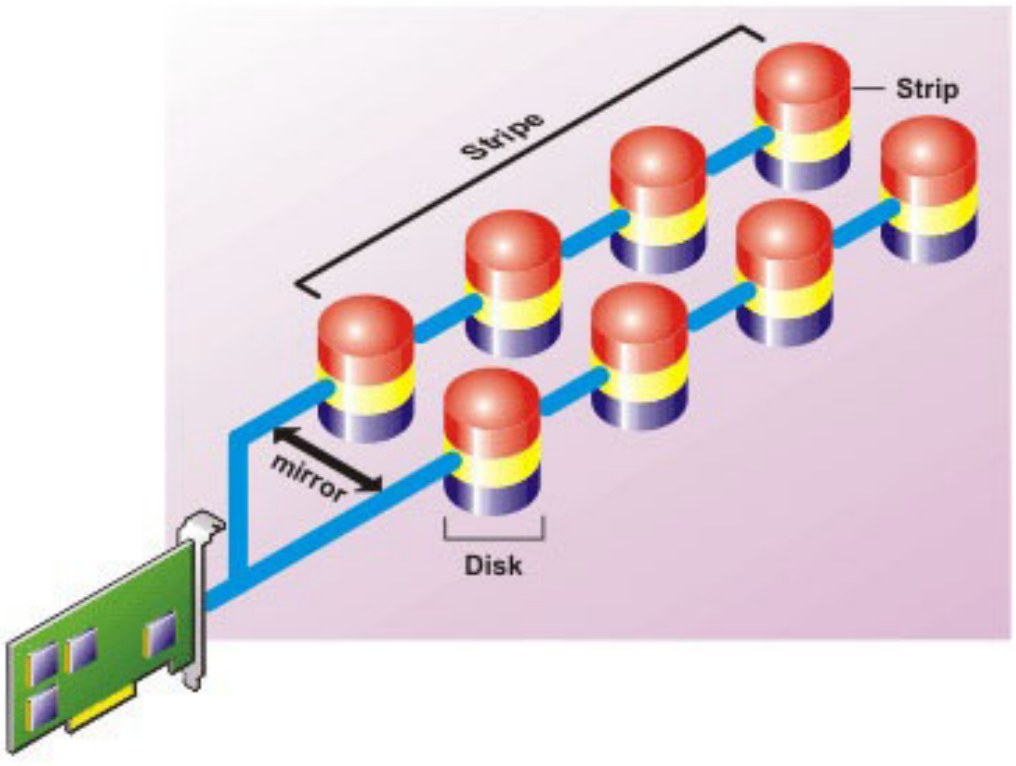


Características de RAID 60:

- Agrupa discos **n*****s** para formar un disco virtual grande con capacidad de discos **s***(**n**-2), en el que **s** representa el número de tramos y **n** es el número de discos dentro de cada tramo.
- La información redundante (paridad) se almacena alternadamente en todos los discos de cada tramo de RAID 6.
- Mejor rendimiento de lectura, pero un rendimiento de escritura más lento.
- La redundancia aumentada proporciona mayor protección de datos que un RAID 50.
- Proporcionalmente, requiere de tanta información de paridad como el RAID 6.
- Se requieren dos discos por tramo para la paridad. RAID 60 es más costoso en términos de espacio de disco.

Nivel RAID 10: reflejos seccionados

RAB considera que el nivel RAID 10 es una implementación del nivel RAID 1. RAID 10 combina los discos físicos reflejados (RAID 1) con el seccionamiento de datos (RAID 0). Con RAID 10, los datos se seccionan entre varios discos físicos. Después, el grupo de discos seccionados se refleja en otro conjunto de discos físicos. RAID 10 puede considerarse un **reflejo de secciones**.



Características de RAID 10:

- Agrupa **n** discos en un disco virtual grande con una capacidad total de (**n**/2) discos, en los que **n** es un número entero par.
- Las imágenes de reflejo de los datos se seccionan entre conjuntos de discos físicos. Este nivel proporciona redundancia a través del reflejado.
- Cuando un disco falla, el disco virtual sigue funcionando. Los datos se leen desde el disco reflejado que sobrevive.
- Rendimiento de lectura mejorado y rendimiento de escritura.
- Hay redundancia para la protección de datos.

Comparación del rendimiento del nivel de 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 42. Comparación de rendimiento de nivel de RAID

Nivel RAID	Redundancia de datos	Rendimiento de lectura	Rendimiento de escritura	Rendimiento de reconstrucción	Cantidad mínima necesaria de discos	Usos sugeridos
RAID 0	Ninguna opción	Muy buena	Muy buena	N/D	N	Datos no críticos.
RAID 1	Excelente	Muy buena	Buena	Buena	2N (N = 1)	Bases de datos pequeñas, registros de bases de datos e información fundamental.
RAID 5	Buena	Lecturas secuenciales: Bueno. Lecturas transaccionales: muy bien	Regular, a menos que se utilice la caché de escritura no simultánea	Regular	N + 1 (N = al menos dos discos)	Bases de datos y otros usos transaccionales de lecturas intensivas.

Tabla 42. Comparación de rendimiento de nivel de RAID (continuación)

Nivel RAID	Redundancia de datos	Rendimiento de lectura	Rendimiento de escritura	Rendimiento de reconstrucción	Cantidad mínima necesaria de discos	Usos sugeridos
RAID 10	Excelente	Muy buena	Regular	Buena	2N x X	Ambientes con uso intensivo de datos (registros grandes).
RAID 50	Buena	Muy buena	Regular	Regular	N + 2 (N = al menos 4)	Usos transaccionales de tamaño mediano o usos intensivos de datos.
RAID 6	Excelente	Lecturas secuenciales: Bueno. Lecturas transaccionales: muy bien	Regular, a menos que se utilice la caché de escritura no simultánea	Deficiente	N + 2 (N = al menos dos discos)	Información fundamental. Bases de datos y otros usos transaccionales de lecturas intensivas.
RAID 60	Excelente	Muy buena	Regular	Deficiente	X x (N + 2) (N = al menos 2)	Información fundamental. Usos transaccionales de tamaño mediano o usos intensivos de datos.
N = número de discos físicos y X = número de conjuntos RAID						

Controladoras admitidas

Controladoras RAID admitidas

Las interfaces de iDRAC son compatibles con las siguientes controladoras PERC12:

- PERC H965i frontal
- PERC H965e

Las interfaces de la iDRAC son compatibles con la siguiente controladora BOSS:

- BOSS-N1

Gabinetes admitidos

iDRAC es compatible con gabinetes MD1400 y MD1420.

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 43. Funciones soportadas para las controladoras de almacenamiento PERC 12

Características	H965i frontal y H965i de adaptador	Adaptador H965e	Adaptador H465i
Asignar o desasignar un disco físico como un repuesto dinámico global	Tiempo real	Tiempo real	No corresponde
Convertir en RAID	No corresponde	No se aplica	No se aplica
Convertir en RAID/no RAID,	En tiempo real (convierte la unidad en un volumen no RAID)	En tiempo real (convierte la unidad en un volumen no RAID)	Tiempo real
Recreación	Tiempo real	Tiempo real	No corresponde
Cancelar recreación	Tiempo real	Tiempo real	No corresponde
Crear discos virtuales	Tiempo real	Tiempo real	No corresponde
Cambiar el nombre de los discos virtuales	Tiempo real	Tiempo real	No corresponde
Editar las políticas de la caché de los discos virtuales	Tiempo real	Tiempo real	No corresponde
Ejecutar una revisión de coherencia en el disco virtual	Tiempo real	Tiempo real	No corresponde
Cancelar revisión de congruencia	No corresponde	No se aplica	No se aplica
Inicializar discos virtuales	Tiempo real	Tiempo real	No corresponde
Cancelar inicialización	Tiempo real	Tiempo real	No corresponde
Cifrar discos virtuales	Tiempo real	Tiempo real	No corresponde
Asignar o desasignar repuestos dinámicos dedicados	Tiempo real	Tiempo real	No corresponde
Eliminar discos virtuales	Tiempo real	Tiempo real	No corresponde
Cancelar la inicialización en segundo plano	Tiempo real	Tiempo real	No corresponde
Expansión de la capacidad en línea	No corresponde	No se aplica	No se aplica
Migración de nivel de RAID	No corresponde	No se aplica	No se aplica
Descarte de caché preservada	Tiempo real	Tiempo real	Tiempo real
Establecer modo de lectura de patrullaje	No corresponde	No se aplica	No se aplica
Modo de lectura de patrullaje manual	Tiempo real	Tiempo real	No corresponde
Áreas de lectura de patrullaje no configuradas	Tiempo real	Tiempo real	No corresponde
Modo de revisión de coherencia	No corresponde	No se aplica	No se aplica
Modo de escritura diferida	No corresponde	No se aplica	No se aplica
Modo de equilibrio de carga	No corresponde	No se aplica	Tiempo real
Porcentaje de revisión de congruencia	Tiempo real	Tiempo real	No corresponde

Tabla 43. Funciones soportadas para las controladoras de almacenamiento PERC 12 (continuación)

Características	H965i frontal y H965i de adaptador	Adaptador H965e	Adaptador H465i
VD de arranque	No corresponde	No se aplica	No se aplica
Cambiar el estado de PD	No corresponde	No se aplica	Tiempo real
Porcentaje de recreación	Tiempo real	Tiempo real	No corresponde
Porcentaje de inicialización de segundo plano	Tiempo real	Tiempo real	No corresponde
Porcentaje de reconstrucción	Tiempo real	Tiempo real	No corresponde
Importar configuración ajena	Tiempo real	Tiempo real	No corresponde
Importar configuración ajena automáticamente	No corresponde	No se aplica	No se aplica
Borrar configuración ajena	Tiempo real	Tiempo real	No corresponde
Restablecer configuración de la controladora	Tiempo real	Tiempo real	No corresponde
Crear o cambiar claves de seguridad	Tiempo real	Tiempo real	Tiempo real
Administrador de clave empresarial segura	Tiempo real	Tiempo real	Tiempo real
Inventario y supervisar de forma remota la condición de los dispositivos SSD PCIe	No corresponde	No se aplica	No se aplica
Preparar para quitar SSD PCIe	No corresponde	No se aplica	No se aplica
Borrar los datos de manera segura para SSD PCIe	No corresponde	No se aplica	Tiempo real
Configurar el modo backplane (dividido/unificado)	Tiempo real	Tiempo real	No corresponde
Hacer parpadear o dejar de hacer parpadear LED de componentes	Tiempo real	Tiempo real	Tiempo real
Cambiar modo de la controladora	No corresponde	No se aplica	No se aplica
Compatibilidad de T10PI para discos virtuales	No corresponde	No se aplica	No se aplica

Tabla 44. Funciones admitidas para los dispositivos de almacenamiento

Funciones	BOSS-N1
Crear discos virtuales	Organizado en etapas
Restablecer configuración de la controladora	Organizado en etapas
Inicialización rápida	Organizado en etapas
Eliminar discos virtuales	Organizado en etapas
Full Initialization (Inicialización completa)	No corresponde
Inventario y supervisar de forma remota la condición de los dispositivos SSD PCIe	No corresponde
Preparar para quitar SSD PCIe	No corresponde

Tabla 44. Funciones admitidas para los dispositivos de almacenamiento (continuación)

Funciones	BOSS-N1
Borrar los datos de manera segura para SSD PCIe	No corresponde
Hacer parpadear o dejar de hacer parpadear LED de componentes	Tiempo real
Conexión directa de unidades	Tiempo real
SEKM	Organizado en etapas
Niveles de RAID compatibles	RAID 0 y RAID 1

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), fuente de alimentación, sonda de ventilador y sonda de temperatura.
- Discos físicos
- Discos virtuales
- Baterías

NOTA:

- En un sistema con más discos virtuales, el inventario de hardware puede mostrar datos de unidades físicas vacías para algunos de los discos virtuales.
- Se generan alertas y excepciones de SNMP para los sucesos de almacenamiento. Los errores se registran en el registro de Lifecycle.
- Si intenta eliminar los trabajos finalizados de la fila de trabajo en espera cuando un trabajo está en progreso, este trabajo en progreso puede fallar. Por lo tanto, se recomienda esperar a que se complete el trabajo en progreso antes de eliminar el trabajo.
- 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.
- Los discos físicos en un sistema con varios backplanes se pueden incluir con otro backplane. 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 de Lifecycle de la controladora PERC no está disponible cuando se procesan los eventos de la controladora PERC anterior y esto no afecta la funcionalidad. El procesamiento de eventos pasados puede variar según la configuración.
- Durante la extracción en caliente de la unidad M.2 para la controladora BOSS N1, el estado del panel de iDRAC se vuelve ámbar, pero el LED del indicador de estado frontal/posterior del servidor permanece en color azul.

NOTA: Puede ver el error SRV015 en dos casos: cuando el dispositivo no soporta la recopilación de TSR como controladoras AHCI o si el dispositivo soporta la recopilación de TSR, pero aún no está inventariado en banda lateral.

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**.

NOTA: Si hay un número impar de ranuras en el servidor, se agrega una fila de ranuras vacía en la lista **Resumen de ranuras** de la página **Gabinete**.

NOTA: Para obtener la información más reciente sobre las propiedades soportadas y sus valores, consulte **Ayuda en línea de la iDRAC**.

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 la iDRAC.
- Si las SSD NVMe de la ranura de backplane admiten los comandos NVMe-MI y la conexión I2C está en buen estado, la iDRAC detectará estas SSD NVMe y las registrará en las interfaces, independientemente de las conexiones de PCI de las ranuras de backplane respectivas.

NOTA:

Tabla 45. Soporte de GUI y otras interfaces

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.

Monitoreo de dispositivos de almacenamiento mediante RACADM

Para ver la información dispositivos de almacenamiento, utilice el comando `storage`.

Para obtener más información, consulte Guía de la CLI RACADM de Integrated Dell Remote Access Controller.

Monitoreo del backplane mediante la utilidad de configuración de iDRAC

En la utilidad de confiuración de iDRAC, vaya a **Resumen del sistema**. Se muestra la página **Resumen del sistema de Ajustes de iDRAC**. En la sección **Inventario de backplane**, se muestra la información del backplane. Para obtener información acerca de los campos, consulte la **Ayuda en línea de la utilidad de configuración de iDRAC**.

Visualización de la topología del dispositivo de almacenamiento

Puede ver la vista jerárquica de contención física de los componentes de almacenamiento clave, es decir, una lista de controladoras, gabinetes conectados a la controladora y un enlace al disco físico contenido en cada gabinete. También se muestran los discos físicos conectados directamente a la controladora.

Para ver la topología del dispositivo de almacenamiento, vaya a **Almacenamiento** > **Visión general**. En la página **Visión general**, se muestra 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

Puede realizar las siguientes operaciones para discos físicos:

- Ver propiedades del disco físico
- Asignar un disco físico o anular la asignación de este como un hot spare global
- Convertir en disco con capacidad de RAID
- Convertir en disco no RAID
- Hacer parpadear o dejar de hacer parpadear el LED
- Reconstruir el disco físico
- Cancelar la reconstrucción de un disco físico
- Borrado criptográfico

NOTA: Si alguna de las unidades seguras SEKM que están directamente conectadas al servidor o detrás de una controladora no son visibles o accesibles para el sistema operativo, se recomienda revisar los registros de Lifecycle y asegurarse de que todas las unidades seguras estén desbloqueadas. De lo contrario, realice las acciones recomendadas mencionadas en los registros de Lifecycle.

Asignación o desasignación de hot spare dedicados

Un hot spare dedicado es un disco de copia de seguridad no utilizado que está asignado a un disco virtual. Cuando falla un disco físico del disco virtual, el repuesto dinámico se activa con el fin de reemplazar al disco físico fallido sin que se interrumpa el sistema ni se requiera ninguna intervención.

Debe tener el privilegio de Inicio de sesión y Control del servidor para ejecutar esta operación.

Solo puede asignar unidades 4K como hot spare a discos virtuales 4K.

Si ha asignado un disco físico como hot spare dedicado en el modo de funcionamiento Agregar a operación pendiente, se crea la operación pendiente, pero no se crea un trabajo. A continuación, si intenta desasignar el hot spare dedicado, se borrará la operación pendiente de asignar hot spare dedicado.

Si ha desasignado un disco físico como hot spare dedicado en el modo de funcionamiento Agregar a operación pendiente, se crea la operación pendiente, pero no se crea un trabajo. Por lo tanto, si intenta asignar el hot spare dedicado, la operación pendiente para desasignar el hot spare dedicado se borra.

NOTA: Si la operación de exportación de registro está en curso, no podrá ver información sobre hot spare dedicados en la página **Administrar discos virtuales**. Una vez finalizada la operación de exportación de registros, vuelva a cargar o actualice la página **Administrar discos virtuales** para ver la información.

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 **Almacenamiento** > **Descripción general** > **Discos físicos**.
2. Se muestran todos los discos físicos.
3. Para asignar un repuesto dinámico global, en los menús desplegables de la columna **Acción**, seleccione **Asignar un repuesto dinámico global** para uno o varios discos físicos.
4. Para desasignar un repuesto dinámico, en los menús desplegables de la columna **Acción**, seleccione **Desasignar repuesto dinámico** para uno o varios discos físicos.
5. Haga clic en **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 hot spare global mediante RACADM

Utilice el comando `storage` y especifique el tipo como hot spare global.

Para obtener más información, consulte Guía de la CLI RACADM de Integrated Dell Remote Access Controller.

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.

Puede convertir las unidades de discos físicos en modo RAID o no RAID de la siguiente manera:

- Mediante las interfaces de la iDRAC, como la interfaz web de la iDRAC, RACADM o Redfish
- 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 la iDRAC, como la interfaz gráfica de usuario de la iDRAC, RACADM y Redfish, sea algo menor que el tamaño real del disco. Sin embargo, puede utilizar la capacidad total del disco para implementar sistemas operativos.

Conversión de discos físicos al modo compatible con RAID o no RAID mediante la interfaz web de iDRAC

Para convertir los discos físicos al modo RAID o al modo 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 ajustes se aplican en función de la opción seleccionada en el modo de operación.

Conversión de discos físicos a modo compatible con RAID o no RAID mediante RACADM

En función de si desea convertir en modo RAID o no RAID, utilice los siguientes comandos RACADM:

- Para convertir al modo RAID, utilice el comando `racadm storage converttoraid`.
- Para convertir al 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 RACADM de Integrated Dell Remote Access Controller.

Borrado de discos físicos

La función borrado del sistema permite borrar el contenido de las unidades físicas. Es posible acceder a esta característica mediante RACADM o la interfaz 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 las unidades ISE, SED SAS y SATA, además de las SSD de PCIe.

NOTA: Las unidades ISE siguen el estándar NIST SP 800-88r1 y cumplen con la depuración de NIST. Esto significa que ninguno de los **datos antiguos** se puede recuperar tras la eliminación.

- Unidades de borrado con sobrescritura: incluyen todas las unidades que no soportan el borrado criptográfico.

NOTA: La opción de borrado del sistema solo se aplica a las unidades dentro del servidor. La iDRAC no puede borrar unidades en un gabinete externo, como un JBOD.

El subcomando de 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 de discos físicos BOSS se puede realizar mediante el método `SystemErase` que se soporta con LC-UI 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 mediante RACADM o la interfaz de usuario de iDRAC. Para obtener más información, consulte las secciones Borrado de datos de un dispositivo SSD PCIe y Borrado de datos de un dispositivo SED mediante la IU.

Para obtener información sobre la función de borrado del sistema dentro de la interfaz de usuario de Lifecycle Controller, consulte *Guía del usuario de Dell Lifecycle Controller* disponible en Manuales de iDRAC..

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.
- Tiene 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.
- El borrado criptográfico también se puede realizar mediante PSID.

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 realizar el borrado criptográfico:

```
<SED FQDD> -psid<PSID>
```

Para obtener más información, consulte la *Guía de CLI de RACADM de Integrated Dell Remote Access Controller*.

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 la 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 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)
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 crea la operación pendiente, aparece un mensaje de error. Si la operación pendiente se realiza de manera correcta y la creación del trabajo no se realiza correctamente, se muestra un mensaje de error.

Recompilar disco físico

Recrear un disco físico es la capacidad para reconstruir el contenido de un disco que ha fallado. Esto es verdad solo cuando la opción de recreación automática se establece en falso. Si hay un disco virtual redundante, la operación de reconstrucción puede reconstruir el contenido de un disco físico fallido. Se puede realizar una recreación durante la operación normal, pero degrada el rendimiento.

Cancelar reconstrucción se puede utilizar para cancelar una reconstrucción que está en curso. Si cancela una reconstrucción, el disco virtual permanece en el estado degradado. La falla de un disco físico adicional puede causar que el disco virtual falle y se puede traducir en la pérdida de datos. Se recomienda realizar una reconstrucción en el disco físico fallido lo antes posible.

Si cancela la reconstrucción de un disco físico que está asignado como un hot spare, reinicie la reconstrucción en el mismo disco físico para poder restaurar los datos. La cancelación de la recreación de un disco físico y luego asignar otro disco físico como un repuesto dinámico no hace que el repuesto dinámico recién asignado recree los datos.

Administración de discos virtuales

Puede 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) o la herramienta de línea de comandos PERCCLI.

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 mediante 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 alcanzó la cantidad máxima 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 alcanzó la cantidad máxima de discos virtuales que soporta 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 se complete 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 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: 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 y Redfish, no se debe especificar el tamaño del disco virtual.

NOTA: No se permite crear discos virtuales en unidades que ya están protegidas.

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 un cierto número 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 y RAID 0 solo son compatibles con las controladoras 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.

NOTA: Algunas acciones pueden hacer que el ID objetivo de arranque no se restablezca a ffff cuando no hay un disco virtual ni EPD-PT configurados.

Creación de discos virtuales mediante RACADM

Utilice el comando `racadm storage createvd`.

Para obtener más información, consulte Guía de la CLI RACADM de Integrated Dell Remote Access Controller.

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.

Creación de discos virtuales mediante la interfaz web

Para crear un disco virtual:

1. En la interfaz web de la 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 el número de discos físicos.

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

4. En el menú desplegable **Aplicar modo de operación**, seleccione el momento en que desea aplicar la configuración.
5. Haga clic en **Crear disco virtual**.

Según en la opción de **Aplicar modo de operación** seleccionada, se aplicará la configuración.

NOTA: Puede utilizar caracteres alfanuméricos, guiones y guiones bajos en el nombre del disco.

Edición de las políticas de la caché de los discos virtuales

Puede cambiar la política de lectura, escritura o caché de disco de un disco virtual.

NOTA: Algunas de las controladoras no son soportadas en todas las políticas de lectura o escritura. Por lo tanto, cuando se aplica una política, se muestra un mensaje de error.

Las políticas de lectura indican si la controladora debe leer los sectores secuenciales del disco virtual cuando busca datos.

- **Lectura anticipada adaptativa**: la controladora inicia la lectura anticipada solamente si las dos solicitudes de lectura más recientes accedieron a sectores secuenciales del disco. Si las solicitudes de lectura accedieron a sectores aleatorios del disco, la controladora revierte a la política sin lectura anticipada. La controladora continúa evaluando si las solicitudes de lectura están accediendo a sectores secuenciales del disco e inicia la lectura anticipada si es necesario.
- **Lectura anticipada**: La controladora lee los sectores secuenciales del disco virtual cuando busca datos. La política Lectura anticipada puede mejorar el rendimiento del sistema si los datos se escriben en 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 debe enviar una señal de finalización de solicitud de escritura cuando los datos se encuentran en la caché o después de que se escriben en el disco.

- **Escritura simultánea**: la controladora envía una señal de finalización de la solicitud de escritura solamente después de que los datos se escriben en el disco. La escritura simultánea en la memoria caché proporciona una mayor seguridad para los datos que la escritura no simultánea en la memoria caché, ya que el sistema da por entendido que los datos solo estarán disponibles después de que escriban de manera segura en el disco.
- **Escritura no simultánea**: la controladora envía una señal de terminación de solicitud de escritura en cuanto los datos están en la memoria caché de la controladora pero todavía no se han escrito en el disco. La escritura no simultánea en la memoria caché puede mejorar el rendimiento, puesto que las solicitudes de lectura posteriores pueden recuperar rápidamente los datos, primero de la memoria caché y luego del disco. Sin embargo, existe el riesgo de que se pierdan datos si se produce un fallo en el sistema que impida que los datos se escriban en un disco. También es posible que otras aplicaciones experimenten problemas si sus acciones asumen que los datos están disponibles en el disco.
- **Forzar escritura no simultánea**: la memoria 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. Esta configuración no afecta a la política de lectura anticipada.

NOTA:

- La caché no volátil de la controladora y la batería de reserva de la caché de la controladora afectan la política de lectura o la política de escritura que puede soportar una controladora. No todas las PERC tienen batería y caché.
- La lectura anticipada y la reescritura necesitan caché. Por lo tanto, si la controladora no tiene caché, no le permite establecer el valor de la política.
  - De manera similar, si la PERC tiene caché, pero no batería y se establece una política que requiere acceso a la caché, es posible que se pierdan datos si se apaga la base. Es posible que muy pocas PERC no permitan esa política.

- Por lo tanto, según la PERC, se establece el valor de la política.

Eliminación de discos virtuales

La eliminación de un disco virtual destruye toda la información, incluidos los sistemas de archivos y los volúmenes en el disco virtual, y quita el disco virtual de la configuración de la controladora. Al eliminar discos virtuales, todos los repuestos dinámicos globales asignados se pueden desasignar automáticamente en el momento en que se elimina el último disco virtual asociado con la controladora. Cuando se elimina el último disco virtual de un grupo de discos, todos los repuestos dinámicos dedicados asignados se convierten en repuestos dinámicos globales automáticamente.

Si elimina todos los discos virtuales de un hot spare global, el hot spare se elimina automáticamente.

Debe tener el privilegio de Inicio de sesión y Control del servidor para eliminar discos virtuales.

Cuando se permite esta operación, puede eliminar una unidad virtual de inicio. Se realiza desde la banda lateral e independientemente del sistema operativo. Por lo tanto, aparece un mensaje de aviso antes de eliminar la unidad virtual.

Si se elimina un disco virtual y se crea inmediatamente 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 la recreación de un nuevo disco virtual, vuelva a inicializar el disco virtual.

NOTA: Las operaciones de restablecimiento de la configuración y eliminación de discos virtuales no se pueden apilar con un máximo de 240 operaciones de creación de discos virtuales. Esto da como resultado una falla de la operación. Estas dos operaciones se pueden ejecutar como trabajos independientes con una diferencia mínima de 2 minutos.

Revisión de congruencia en el disco virtual

Esta operación verifica la precisión de la información redundante (paridad). Esta tarea solo corresponde a 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 coherencia 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. Debe inicializar un disco virtual que esté configurado antes de utilizarlo.

NOTA: No inicialice los discos virtuales cuando intente volver a crear una configuración existente.

Puede realizar una inicialización rápida, una inicialización completa o cancelar la operación de inicialización.

NOTA: La opción de cancelar la inicialización es una operación en tiempo real. Puede cancelar la inicialización solo con la interfaz web de la iDRAC, sin usar la interfaz de RACADM.

Inicialización rápida

La inicialización rápida se aplica a todos los discos físicos que se incluyen en el disco virtual. Actualiza los metadatos en los discos físicos, de modo que todo el espacio de disco quede disponible para las operaciones futuras de escritura. 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 futuras operaciones de escritura sobrescribirán toda la información que permanezca en los discos físicos.

La inicialización rápida solo elimina la información de la sección y del sector de arranque. Realice una inicialización rápida solo si hay limitaciones de tiempo o si las unidades de disco duro son nuevas o no se utilizan. La inicialización rápida tarda menos tiempo en completarse (por lo general, de 30 a 60 segundos).

PRECAUCIÓN: Realizar una inicialización rápida hace que no se pueda obtener acceso a los datos existentes.

La tarea de inicialización rápida no escribe ceros en los bloques de discos de los discos físicos. Dado que la tarea de inicialización rápida no realiza una operación de escritura, causa menos deterioro al disco.

Una inicialización rápida en un disco virtual sobrescribe los primeros y últimos 8 MB del disco virtual, y borra cualquier registro de arranque o información de partición. La operación tarda solo de 2 a 3 segundos en completarse y se recomienda cuando se recrean discos virtuales.

Una inicialización en segundo plano comienza cinco minutos después de que se completa la inicialización rápida.

Inicialización completa o lenta

La inicialización completa (también denominada inicialización lenta) inicializa todos los discos físicos incluidos en el disco virtual. Se actualizan los metadatos en los discos físicos y se borran todos los datos y los sistemas de archivos existentes. Puede realizar una inicialización completa después de crear el disco virtual. A diferencia de la inicialización rápida, se recomienda utilizar la inicialización completa si hubo algún problema con un disco físico o si se sospecha que este contiene bloques de discos dañados. La inicialización completa reasigna los bloques dañados y escribe ceros en todos los bloques del disco.

Si se realiza la inicialización completa de un disco virtual, no se requiere la inicialización en segundo plano. Durante la inicialización completa, el host no puede acceder al disco virtual. Si el sistema se reinicia durante una inicialización completa, la operación se anula y se inicia una inicialización de segundo plano en el disco virtual.

Siempre se recomienda realizar una inicialización completa en las unidades que anteriormente contenían datos. La inicialización completa puede tardar de 1 a 2 minutos por GB. La velocidad de la inicialización depende del modelo de la controladora, la velocidad de las unidades de disco duro y la versión del firmware.

La tarea de Inicialización lenta inicializa un disco físico a la vez.

NOTA: La inicialización completa se admite en tiempo real únicamente. Solo algunas controladoras son compatibles con la inicialización completa.

Cifrado de discos virtuales

Cuando el cifrado esté inhabilitado en una controladora (es decir, se elimina la clave de seguridad), active manualmente el cifrado para los discos virtuales creados mediante unidades de SED. Si el disco virtual se crea después de habilitar el cifrado en una controladora, el disco virtual se cifra automáticamente. Se configura automáticamente como un disco virtual cifrado, a menos que la opción de cifrado activada esté inhabilitada durante la creación del disco virtual.

Es necesario tener el privilegio de inicio de sesión y control del servidor para administrar las llaves de cifrado.

NOTA: A pesar de que el cifrado está habilitado en las controladoras, el usuario debe habilitar manualmente el cifrado en el disco virtual si se crea un disco virtual desde la iDRAC.

Asignación o desasignación de hot spare dedicados

Un hot spare dedicado es un disco de copia de seguridad no utilizado que está asignado a un disco virtual. Cuando falla un disco físico del disco virtual, el repuesto dinámico se activa con el fin de reemplazar al disco físico fallido sin que se interrumpa el sistema ni se requiera ninguna intervención.

Debe tener el privilegio de Inicio de sesión y Control del servidor para ejecutar esta operación.

Solo puede asignar unidades 4K como hot spare a discos virtuales 4K.

Si ha asignado un disco físico como hot spare dedicado en el modo de funcionamiento Agregar a operación pendiente, se crea la operación pendiente, pero no se crea un trabajo. A continuación, si intenta desasignar el hot spare dedicado, se borrará la operación pendiente de asignar hot spare dedicado.

Si ha desasignado un disco físico como hot spare dedicado en el modo de funcionamiento Agregar a operación pendiente, se crea la operación pendiente, pero no se crea un trabajo. Por lo tanto, si intenta asignar el hot spare dedicado, la operación pendiente para desasignar el hot spare dedicado se borra.

NOTA: Si la operación de exportación de registro está en curso, no podrá ver información sobre hot spare dedicados en la página **Administrar discos virtuales**. Una vez finalizada la operación de exportación de registros, vuelva a cargar o actualice la página **Administrar discos virtuales** para ver la información.

Cambiar nombre del disco virtual

Para cambiar el nombre de un disco virtual, el usuario debe tener el privilegio de control del sistema. El nombre del disco virtual solo puede contener caracteres alfanuméricos, guiones y guiones bajos. La longitud máxima del nombre depende de la controladora individual. En la mayoría de casos, la longitud máxima es de 15 caracteres. Cada vez que se cambia el nombre de un disco virtual, se crea un registro de LC.

Edición de la capacidad del disco

La expansión de la capacidad en línea (OCE) le permite aumentar la capacidad de almacenamiento de niveles RAID seleccionados mientras el sistema permanece en línea. La controladora redistribuye los datos en el arreglo (lo que se denomina reconfiguración), lo que libera espacio nuevo al final de cada arreglo RAID.

La expansión de capacidad en línea (OCE) se puede lograr de dos maneras:

- Si hay espacio libre disponible en la unidad física más pequeña del grupo de discos virtuales después de iniciar el LBA de discos virtuales, la capacidad del disco virtual se puede ampliar dentro de dicho espacio libre. Esta opción le permite introducir el nuevo tamaño de disco virtual ampliado. Si el grupo de discos de un disco virtual tiene espacio libre solo antes de iniciar el LBA, entonces no se permite Editar capacidad del disco en el mismo grupo de discos a pesar de que haya espacio disponible en una unidad física.
- También es posible ampliar la capacidad de un disco virtual mediante la adición de discos físicos compatibles al grupo de discos virtuales. Esta opción no le permite introducir el nuevo tamaño de disco virtual ampliado. El nuevo tamaño del disco virtual se calcula y se muestra al usuario según el espacio de disco usado del grupo de discos físicos existente en un disco virtual específico, el nivel raid existente del disco virtual y el número de nuevas unidades agregadas al disco virtual.

Expansión de capacidad permite que el usuario especifique el tamaño final del disco virtual. Internamente, el tamaño final del disco virtual se transmite a PERC en 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 expanda). Debido a este porcentaje, el tamaño final de la VD lógica después de que se completa la reconfiguración puede diferir de lo que proporcionó el usuario en caso de que el usuario no proporcione el tamaño máximo de VD posible como el tamaño final de VD (el porcentaje resulta ser inferior al 100 %). El usuario no ve la diferencia entre este tamaño de VD introducido y el tamaño final de VD después de la reconfiguración; si el usuario ingresa el tamaño de VD máximo posible.

Migración de nivel RAID

El cambio del nivel RAID de un disco virtual se denomina migración de nivel RAID (RLM). La iDRAC ofrece una opción para aumentar el tamaño del disco virtual mediante RLM. De cierto modo, RLM permite migrar el nivel de RAID de un disco virtual, que, a su vez, puede aumentar el tamaño de los discos virtuales.

La migración de nivel de RAID es el proceso de conversión de un DV de 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 46. Diseños posibles 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	NA
R0	R5/R6	N/D
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 47. 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	Parpadeante	Eliminar
Exportar registro	Parpadeante	Dejar de parpadear	Parpadeante
Establecer modo de lectura de patrullaje	Dejar de parpadear	Asignar un repuesto dinámico global	Dejar de parpadear
Comenzar lectura de patrullaje	N/D	Convertir en discos no RAID	Renombrar
Cambiar propiedades de la controladora	N/D	N/D	Cambiar política
Administrar las propiedades de alimentación de discos físicos	N/D	N/D	Inicialización lenta
Convertir en discos con capacidad de RAID	N/D	N/D	Inicialización rápida
Convertir en discos no RAID	N/D	N/D	Reemplazar un disco miembro
Cambiar modo de controladora	N/D	N/D	N/D

Cancelar inicialización

Esta característica permite cancelar la inicialización en segundo plano en un disco virtual. En las controladoras PERC, la inicialización en segundo plano de los discos virtuales redundantes comienza automáticamente después de crear el 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, algunos procesos como la creación de un disco virtual no pueden ejecutarse mientras la inicialización en segundo plano está en curso. Cancelar la inicialización proporciona la capacidad de cancelar manualmente la inicialización en segundo plano. Si se cancela, la inicialización de segundo plano se reinicia automáticamente entre 0 y 5 minutos después.

NOTA: La inicialización en segundo plano no se aplica a los discos virtuales RAID 0.

Restricciones o limitaciones de OCE y RLM

A continuación, se indican las limitaciones comunes para OCE y RLM:

- OCE/RLM está restringida al caso en el que el grupo de discos contiene solo un disco virtual.
- OCE no soporta RAID50 y RAID60. La RLM no está soporta en RAID10, RAID50 y RAID60.
- Si la controladora ya contiene el número máximo de discos virtuales, no puede realizar una migración de nivel RAID o expansión de capacidad en ningún disco virtual.
- La controladora cambia la política de caché de escritura de todos los discos virtuales en los que se está realizando una RLM/OCE a escritura simultánea hasta que finaliza la RLM/OCE.
- Generalmente, la reconfiguración de los Virtual Disks (Discos virtuales) afecta al rendimiento del disco hasta que la operación de reconfiguración concluya.
- La cantidad total de discos físicos de un grupo de discos no puede ser superior a 32.
- Si ya se está ejecutando alguna operación en segundo plano (como BGI/reconstrucción/copia diferida/lectura de vigilancia) en el VD/PD correspondiente, la reconfiguración (OCE/RLM) no se permite en ese momento.
- Cualquier tipo de migración de disco cuando la reconfiguración (OCE/RLM) está en curso en las unidades asociadas con VD hace que la reconfiguración falle.
- Cualquier unidad nueva agregada para OCE/RLM pasa a formar parte del disco virtual una vez finalizada la reconstrucción. Pero el estado para esos nuevos cambios de unidad a En línea justo después de que comience la reconstrucción.

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 discos virtuales:

```
racadm storage init:<VD FQDD> -speed {fast|full}
```

- Para comprobar la coherencia de los discos virtuales (no soportada en RAID0):

```
racadm storage ccheck:<vdisk fqdd>
```

  Para cancelar la comprobación de coherencia:

```
racadm storage cancelcheck: <vdisks fqdd>
```

- Para cifrar discos virtuales:

```
racadm storage encryptvd:<VD FQDD>
```

- Para asignar o desasignar hot spare:

```
racadm storage hotspare:<Physical Disk FQDD> -assign <option> -type dhs -vdkey: <FQDD of
VD>
```

  <option>=sí

  Asignar hot spare

  <Option>=no

  Desasignar el hot spare

Administración de discos virtuales mediante la interfaz web

1. En la interfaz web de la iDRAC, vaya a **Almacenamiento** > **Visión general** > **Discos virtuales**.
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.
   - **Renombrar**
   - **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.

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:

PRECAUCIÓN: Si se fuerza a un disco físico para conectarse en línea u offline puede ocasionar la pérdida de datos.

Tabla 48. Función de la configuración de RAID

Funciones	Comando 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.		

Tabla 48. Función de la configuración de RAID (continuación)

Funciones	Comando RACADM	Descripción
Force Offline (Forzar desconexión)	`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 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 controladoras:

- Configurar propiedades de la controladora
- Importar o importar automáticamente una configuración ajena
- Borrar configuración ajena
- Restablecer configuración de la controladora
- Crear, cambiar o eliminar claves de seguridad
- Descarte de 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

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 tarea de revisión de coherencia comprueba la precisión de la información redundante (de paridad). Esta tarea solo corresponde a discos virtuales redundantes. De ser necesario, la tarea de revisión de coherencia reconstruye los datos redundantes. Cuando el estado de un disco virtual es de error en la redundancia, realizar una revisión de coherencia 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 coherencia de 0 % no significa que el proceso quede detenido o en pausa. Con un valor de 100 %, la revisión de coherencia 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.

Configuración de las propiedades de la controladora mediante RACADM

- Para configurar el modo de lectura de vigilancia:

```
racadm set storage.controller.<index>.PatrolReadMode  {Automatic | Manual | Disabled}
```

- Si el modo de lectura de vigilancia está establecido en manual, utilice los siguientes comandos para iniciar y detener el modo de lectura de vigilancia:

```
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. Si bien es posible invocar las operaciones correctamente mediante la interfaz de iDRAC, las operaciones fallan cuando se inicia el trabajo asociado.

NOTA: Los atributos de almacenamiento PatrolReadMode y PersistHotspare asignados a las controladoras HBA12 y PERC12 son inmutables. Si intenta modificar estos atributos, es posible que se produzcan errores. Aunque el trabajo se crea y se ejecuta, los valores originales se mantienen iguales.

- Para especificar el modo de revisión de coherencia, utilice el objeto **Storage.Controller.CheckConsistencyMode**.
- Para habilitar o deshabilitar el modo de escritura diferida, use el objeto **Storage.Controller.CopybackMode**.
- Para habilitar o deshabilitar el modo de balanceo de carga, use el objeto **Storage.Controller.PossibleloadBalancedMode**.
- Para especificar el porcentaje de recursos del sistema dedicados a realizar una revisión de coherencia en un disco virtual redundante, use el objeto **Storage.Controller.CheckConsistencyRate**.
- Para especificar el porcentaje de recursos de la controladora dedicados a reconstruir un disco fallido, use el objeto **Storage.Controller.RebuildRate**.
- Para especificar el porcentaje de recursos de la controladora dedicados a realizar una inicialización en segundo plano (BGI) de un disco virtual después de su creación, use 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 de RAID de un disco virtual que reside en el grupo de discos, use el objeto **Storage.Controller.ReconstructRate**.
- Para habilitar o deshabilitar la importación automática mejorada de la configuración externa para la controladora, use el objeto **Storage.Controller.EnhancedAutoImportForeignConfig**.
- Para crear, modificar o eliminar la clave de seguridad a fin de cifrar 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>
```

Configuración de las propiedades de la controladora mediante la interfaz web

1. En la interfaz web de iDRAC, vaya a **Almacenamiento** > **Descripción general** > **Controladoras**.
   Se mostrará la página **Configuración de controladoras**.
2. En la sección **Controladora**, seleccione la controladora que desea configurar.
3. Especifique la información necesaria para las distintas propiedades.

   La columna **Valor actual** muestra los valores existentes para cada propiedad. Puede modificar este valor si selecciona la opción del menú desplegable **Acción** de cada propiedad.

   Para obtener información acerca de los campos, consulte la **Ayuda en línea de iDRAC7**.
4. En **Aplicar modo de operación**, seleccione el momento en que desea aplicar los ajustes.

5. Haga clic en **Aplicar**.
   Según el modo de operación seleccionado, se aplicará la configuración.

Protocolo de seguridad y modelo de datos (SPDM)

El protocolo SPDM se utiliza para establecer las funcionalidades de seguridad y la autenticidad entre los componentes de hardware. SPDM permite el intercambio de mensajes entre iDRAC y dispositivos finales, como controladoras de almacenamiento (PERC12), FC y CPU. Esto incluye certificados de identidad de hardware. Puede habilitar SPDM mediante Redfish o RACADM.

Tabla 49. Licencias y funciones de SPDM

Funciones	Licencia
Inventario: Detección de dispositivos compatibles con SPDM	Sin licencia
Recopilación de identidad de hardware de dispositivos	Enterprise
Recopilación de mediciones de dispositivos	Enterprise
Establecimiento de confianza en el certificado del dispositivo mediante SCV	Licencia de SCV
Canal de comunicación cifrado	Licencia de SEKM

Cuando un dispositivo es compatible con SPDM, los datos de SCV recopilados contienen certificados de identidad de hardware de SPDM, además de los campos existentes. Los certificados de identidad del firmware no se incluyen en el certificado de SCV.

NOTA: Es posible que observe que falta el número de puerto NIC en el nombre del archivo descargado del certificado de hardware de SPDM.

NOTA: La falla del trabajo del certificado de SPDM de exportación se puede ver en la cola de trabajos cuando realiza reinicios frecuentes.

Habilitar SPDM mediante RACADM

La función SPDM en iDRAC le permite administrar y monitorear el estado de seguridad de varios componentes.

1. Ejecute el siguiente comando para habilitar SPDM:
   `racadm set idrac.SPDM.enable enabled`
2. Ejecute los siguientes comandos para asegurarse de que se reflejen todos los cambios:
   `racadm racreset`
   `racadm get idrac.SPDM`

Habilitar SPDM mediante Redfish

La función SPDM en iDRAC le permite administrar y monitorear el estado de seguridad de varios componentes.

1. Realice una solicitud PATCH para la siguiente URI utilizando la carga útil `{"Attributes":{"SPDM.1.Enable":"Enabled"}}`:
   `/redfish/v1/Managers/iDRAC.Embedded.1/Oem/Dell/DellAttributes/iDRAC.Embedded.1`
2. Realice `racreset` para asegurarse de que se reflejen los cambios.

Importación o importación automática de 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 ajenas, de manera que los discos virtuales no se pierdan tras el traslado de los discos físicos. Una configuración ajena se puede importar solo si contiene un disco virtual que está en estado listo o degradado o en un hot spare dedicado a un disco virtual que se puede importar o ya está presente.

Todos los datos de un disco virtual deben estar presentes, pero si el disco virtual utiliza un nivel RAID redundante, los datos redundantes adicionales no son necesarios.

Por ejemplo, si la configuración ajena contiene solo un lado de un reflejo en un disco virtual RAID 1, entonces el disco virtual se encuentra en estado Degradado y puede importarse. Si la configuración ajena contiene solo un disco físico que se configuró originalmente como un RAID 5 mediante el uso de tres discos físicos, entonces el disco virtual RAID 5 se encuentra en estado de error y no puede importarse.

Además de discos virtuales, una configuración ajena puede consistir en un disco físico que se ha asignado como hot spare de una controladora y que a continuación se ha movido a otra controladora. La tarea Importar configuración ajena importa el nuevo disco físico como hot spare. Si el disco físico se ha establecido como un hot spare dedicado en la controladora anterior, pero el disco virtual al que el hot spare se ha asignado ya no está presente en la configuración ajena, el disco físico se importa como un hot spare global.

La tarea Importar la configuración ajena solo aparece cuando la controladora ha detectado una configuración ajena. También puede identificar si un disco físico contiene una configuración ajena (disco virtual o hot spare) 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: Como parte de la importación de configuración ajena, si una configuración está incompleta, no se importa. Sin embargo, el trabajo no fallará. El estado del trabajo se muestra como **Se completó correctamente**. Debe comprobar el estado del PD para saber si el disco virtual se importó o no.

NOTA: La tarea de importación de configuración ajena importa todos los discos virtuales que residen en los discos físicos que se han agregado a la controladora. Si hay más de un disco virtual ajeno presente, se importan todas las configuraciones ajenas.

La controladora PERC9 proporciona soporte para la importación automática de la configuración ajena sin necesidad de interacciones del usuario. La importación automática se puede habilitar o inhabilitar. Si esta opción está activada, la controladora PERC puede importar automáticamente cualquier configuración ajena detectada sin intervención manual. Si no se habilita, la PERC no importa automáticamente ninguna configuración ajena.

Debe tener el privilegio de Inicio de sesión y Control del servidor para importar configuraciones ajenas.

Las controladoras de hardware PERC que se ejecutan en modo HBA no soportan esta tare.

NOTA: No se recomienda quitar el cable de una carcasa externa cuando el sistema operativo se está ejecutando en el sistema. Quitar el cable puede provocar una configuración ajena cuando la conexión se vuelva a establecer.

Puede administrar configuraciones ajenas en los siguientes casos:

- Todos los discos físicos de una configuración se quitan y se reinsertan.
- Algunos de los discos físicos de una configuración se quitan y se reinsertan.
- Todos los discos físicos de un disco virtual se quitan, pero en momentos diferentes, y luego se reinsertan.
- Se quitan los discos físicos de un disco virtual no redundante.

Las siguientes restricciones se aplican a los discos físicos que se consideran para una importación:

- El estado de la unidad de un disco físico puede cambiar desde el momento en que se analiza la configuración ajena hasta cuando se produce la importación real. La importación ajena ocurre solo en las unidades que se encuentran en buen estado sin configurar.
- Las unidades que estén en el estado de error o desconectadas no pueden importarse.
- El firmware no permite importar ni borrar las configuraciones ajenas si hay más de ocho unidades ajenas presentes.

Importación de una configuración ajena mediante la RACADM

Para importar la configuración ajena:

```
racadm storage importconfig:<Controller FQDD>
```

Para obtener más información, consulte **Guía de referencia de la línea de comandos RACADM de iDRAC**, disponible en **dell.com/idracmanuals**.

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 la iDRAC, vaya a **Almacenamiento** > **Descripción general** > **Controladoras**.
2. En las opciones de **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**.

Borrado de la 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. Puede borrar o eliminar la información del disco virtual de los discos físicos recién conectados.

La tarea Borrar configuración ajena destruye 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 tiene una configuración ajena incompleta que no puede importarse, haga clic en la opción Borrar configuración ajena para borrar los datos ajenos en los discos físicos.

Borrado de la configuración ajena mediante la interfaz web

Para borrar la configuración ajena:

1. En la interfaz web de iDRAC, vaya a **Almacenamiento** > **Descripción general** > **Controladoras**.
   Se muestra la página **Configuración de la controladora**.
2. En las opciones de **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 **Guía de referencia de la línea de comandos RACADM de iDRAC**, disponible en **dell.com/idracmanuals**.

Restablecimiento de la configuración de la controladora

Puede restablecer la configuración de una controladora. Esta operación elimina las unidades de disco virtual y cancela la asignación de todos los hot spares de la controladora. No borra los datos; solo elimina los discos de la configuración. Restablecer configuración tampoco quita configuraciones ajenas. Restablecer configuración no borrará datos. Puede volver a crear exactamente la misma configuración sin una operación de inicialización que puede dar como resultado una recuperación de los datos. Debe contar con el privilegio de control del servidor.

NOTA: El restablecimiento de la configuración de la controladora no elimina una configuración ajena. Para eliminar una configuración ajena, realice una operación de borrado de la configuración.

Restablecimiento de la configuración de la controladora mediante la interfaz web

Para restablecer la configuración de la controladora:

1. En la interfaz web de iDRAC, vaya a **Almacenamiento** > **Descripción general** > **Controladoras**.
2. En **Acciones**, seleccione **Restablecer configuración** para una o más controladoras.
3. En el menú desplegable **Aplicar modo de operación**, seleccione el momento en que desea aplicar los ajustes.
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 **Guía de referencia de la línea de comandos RACADM de iDRAC**, disponible en **dell.com/idracmanuals**.

Cambio de modo de la controladora

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.

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.

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.

Excepciones al cambiar el modo de la controladora

La siguiente lista proporciona las excepciones cuando configura el modo de la controladora mediante las interfaces de la iDRAC, como la interfaz web y RACADM:

- 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 **Activado**.

En la siguiente lista se proporcionan las excepciones cuando configura el modo de la controladora mediante la característica de perfil de configuración del servidor mediante la interfaz de RACADM:

- La función "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 comentar el atributo RAIDaction en el archivo SCP.
- Cuando la controladora PERC está en modo HBA, si ejecuta la vista previa de importación en el archivo SCP de exportación que está editado para cambiar el modo de la controladora a RAID e intenta crear un disco virtual (VD), no funcionará 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 del modo de la controladora mediante la interfaz web de 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 los ajustes actuales 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 del modo de la controladora mediante RACADM

Para cambiar el modo de la controladora mediante RACADM, ejecute los siguientes comandos.

- Para ver el modo actual de la controladora:

  ```
  $ racadm get Storage.Controller.1.RequestedControllerMode[key=<Controller_FQDD>]
  ```

  Se muestra la siguiente salida:

  ```
  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 **Guía de referencia de la interfaz de línea de comandos RACADM de iDRAC**, disponible en **dell.com/idracmanuals**.

Operaciones del adaptador HBA

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.

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 (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:
- 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.

NOTA: No se admite la detección de unidades fallidas detrás de las controladoras HBA SAS.

Monitoreo del análisis predictivo de fallas en unidades

Storage Management soporta la Tecnología de supervisión automática, análisis y generación de informes (SMART) en discos físicos habilitados para SMART.

SMART realiza un análisis predictivo de fallas en cada disco y envía alertas si se predice una falla del disco. Las controladoras comprueban los discos físicos en busca de predicciones de fallos y, si las encuentran, pasan esta información a iDRAC. La iDRAC registra una alerta de inmediato.

Operaciones de la controladora en modo no RAID o modo HBA

Si la controladora está en modo no RAID (modo HBA), entonces:

- Los discos virtuales o hot spare no están disponibles.
- El estado de seguridad de la controladora es deshabilitado.
- Todos los discos físicos están en modo no RAID.

Si la controladora está en modo no RAID, puede realizar las siguientes operaciones:

- Hacer parpadear o dejar de hacer parpadear el disco físico.
- Configurar todas las propiedades, incluidas las siguientes:
  - Modo de balanceo de carga
  - Modo de revisión de congruencia
  - Modo de lectura de vigilancia
  - Modo de escritura diferida
  - Modo de arranque 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 backplane
  - Áreas de lectura de patrullaje no configuradas
- Vea todas las propiedades aplicables a una controladora RAID, excepto para los discos virtuales.
- Borrar configuración ajena

NOTA: Si una operación no está soportada en el modo no RAID, se muestra un mensaje de error.

No puede monitorear las sondas de temperatura, los ventiladores y las fuentes de alimentación del gabinete cuando la controladora está en modo no RAID.

Ejecución de trabajos de configuración de RAID en varias controladoras de almacenamiento

Mientras realiza operaciones en más de dos controladoras de almacenamiento desde cualquier interfaz de iDRAC soportada, asegúrese de hacer lo siguiente:

- Ejecute los trabajos en cada controladora individualmente. Espere a que se complete cada trabajo antes de iniciar la configuración y la creación de trabajos en la siguiente controladora.
- Programe varios trabajos para que se ejecuten en un momento posterior mediante las opciones de programación.

Administrar caché preservada

La característica de caché preservada administrada es una opción de la controladora que proporciona al usuario la opción de 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 coloca fuera de línea o se elimina por cualquier motivo, se perderán los datos de la caché.

La controladora PREC conserva los datos escritos en la caché preservada o contaminada en caso una falla de alimentación o desconexión del cable hasta que 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 ajena.
- La controladora no tiene ningún disco virtual fuera de línea o perdido.
- Ningún disco virtual tiene los cables desconectados.

Administración de SSD PCIe

El Dispositivo de estado sólido (SSD) Peripheral Component Interconnect Express (PCIe) es un dispositivo de almacenamiento de alto rendimiento diseñado para soluciones que requieren una latencia baja, muchas operaciones de entrada/salida por segundo (IOPS) y un almacenamiento profesional confiable y funcional. El SSD PCIe está diseñado sobre la base de la tecnología Flash NAND de celda de nivel individual (SLC) y celda de nivel múltiple (MLC) con una interfaz compatible con PCIe 2.0, PCIe 3.0 o PCIe 4.0 de alta velocidad.

Si se usan interfaces de iDRAC, es posible visualizar y configurar los unidades SSD PCIe de NVMe.

A continuación, se indican las funciones clave de PCIe SSD:

- Capacidad de acoplamiento activo
- Dispositivo de alto rendimiento

Es posible realizar las siguientes operaciones para SSD PCIe:

- Crear inventario y supervisar de manera remota la condición de los dispositivos SSD PCIe en el servidor
- Preparar para quitar dispositivo SSD PCIe
- Borrar los datos de manera segura
- LED del dispositivo parpadeante o no parpadeante (identificar el dispositivo)

Es posible realizar las siguientes operaciones para SSD HHHL:

- Inventario y supervisión en tiempo real del SSD HHHL en el servidor
- Informe y registro de tarjeta fallida en iDRAC y OMSS
- Borrado seguro de datos y extracción de la tarjeta
- Informes de registros TTY

Puede realizar las siguientes operaciones para SSD:

- Informe de estado de la unidad, como En línea, Fallido y Desconectado

NOTA: Capacidad de acoplamiento en marcha, preparar para quitar, y hacer parpadear o dejar de hacer parpadear el LED de los dispositivos no se aplican a los dispositivos SSD PCIe HHHL.

NOTA: Cuando los dispositivos NVMe se controlan detrás de SW RAID, no se soportan las operaciones de preparación para quitar y de borrado criptográfico, ya que se soportan el parpadeo y el no parpadeo.

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

  NOTA: 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 monitoreo de SSD PCIe mediante la interfaz web

Para realizar un inventario y monitorear los dispositivos SSD PCIe, en la interfaz web de iDRAC, vaya a **Almacenamiento** > **Visión general** > **Discos físicos**. Se muestra la página **Propiedades**. En el caso de los SSD PCIe, la columna **Nombre** muestra **SSD PCIe**. Expanda para ver las propiedades.

Inventario y monitoreo de SSD PCIe mediante RACADM

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 del backplane de SSD PCIe:

```
racadm storage get enclosures
```

NOTA: Para todos los comandos mencionados, también se muestran los dispositivos PERC.

Para obtener más información, consulte la **Guía de referencia de la línea de comandos RACADM de la iDRAC**, disponible en **dell.com/idracmanuals**

Prepararse para quitar una 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 Prepararse para quitar no está soportada en las unidades SSD PCIe en los sistemas VMware vSphere (ESXi) ni en los dispositivos SSD PCIe HHHL.

La operación Preparase para quitar se puede realizar en tiempo real mediante el iDRAC Service Module.

Esta operación de Prepararse para quitar detiene las actividades en segundo plano y las actividades de I/O continuas de modo que el dispositivo puede extraerse de forma segura. Hace que parpadeen los LED de estado del dispositivo. Puede quitar el dispositivo del sistema de forma segura en las siguientes condiciones, después de iniciar la operación Prepararse 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 la SSD PCIe para la extracción, asegúrese de lo siguiente:

- iDRAC Service Module está instalado.
- Lifecycle Controller está activado.
- Tiene privilegios de inicio de sesión y control del servidor.

Prepararse para quitar la SSD PCIe mediante la interfaz web

Para prepararse a fin de quitar la SSD PCIe:

1. En la interfaz web de iDRAC, vaya a **Almacenamiento** > **Visión general** > **Discos físicos**.
   Aparecerá la página **Configuración de discos físicos**.
2. Desde el menú desplegable **Controladora**, seleccione la extensión para ver los SSD PCIe asociados.
3. En los menús desplegables, seleccione **Prepararse para quitar** para una o varias unidades SSD PCIe.
   Si ha seleccionado **Prepararse 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 el iSM esté instalado y en ejecución para realizar la operación `preparetoremove`.
4. En el menú desplegable **Aplicar modo de operación**, seleccione **Aplicar ahora** para aplicar las acciones de inmediato.
   Si hay trabajos pendientes de finalización, esta opción aparece atenuada.
   NOTA: Para los dispositivos SSD PCIe, solo está disponible la opción **Aplicar ahora**. Esta operación no está soportada 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 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 crea la operación pendiente, aparece un mensaje de error. Si la operación pendiente se realiza de manera correcta y la creación del trabajo no se realiza correctamente, se muestra un mensaje de error.

Prepararse para quitar la SSD PCIe mediante RACADM

Para preparar la unidad SSD PCIe para la extracción:

```
racadm storage preparetoremove:<PCIeSSD FQDD>
```

Para crear el trabajo de objetivo 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 información sobre los caracteres recomendados para los nombres de usuario y las contraseñas, consulte Caracteres recomendados para nombres de usuario y contraseñas.

Eliminación de datos del 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 los datos del dispositivo SSD PCIe, asegúrese de lo siguiente:

- Lifecycle Controller está activado.
- Tiene privilegios de inicio de sesión y control del servidor.

NOTA:

- SSD PCIe solo se puede borrar como una operación 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 conectar en caliente una SSD PCIe, puede tardar varios segundos en 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 **Almacenamiento** > **Descripción general** > **Discos físicos**.
   Aparecerá la página **Discos físicos**.
2. Desde el menú desplegable **Controladora**, seleccione la controladora para ver los SSD PCIe asociados.
3. En los menús desplegables, seleccione **Borrado criptográfico** para una o varias unidades SSD PCIe.
   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:
   - **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 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)
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 crea la operación pendiente, aparece un mensaje de error. Si la operación pendiente se realiza de manera correcta y la creación del trabajo no se realiza correctamente, se muestra un mensaje de error.

Borrado de datos de un dispositivo SSD PCIe mediante RACADM

Para borrar de forma segura un dispositivo SSD 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 la *Guía de referencia de comandos de la iDRAC RACADM*.

Administración de gabinetes o backplane

Puede realizar lo siguiente para gabinetes o backplane:

- Ver propiedades
- Configurar el modo universal o el modo dividido
- Ver información de ranura (universal o compartida)
- Configurar el modo SGPIO
- Establecer la etiqueta de activo
- Nombre de la propiedad

Configuración del modo de backplane

Los servidores PowerEdge soportan una nueva topología de almacenamiento interno, en la que se pueden conectar dos controladoras de almacenamiento (PERC) a unidades internas a través de un solo expansor. Esta configuración se utiliza para el modo de alto rendimiento sin ninguna funcionalidad de conmutación por error ni 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 específica. No existen requisitos de licencia para esta función. Esta característica solo es compatible con algunos sistemas.

El backplane soporta los siguientes modos:

- 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 cuatro 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 ocho 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 ocho 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.
- Información no disponible: indica que la información de la controladora no está disponible.

La iDRAC permite la configuración del modo dividido si el expansor puede admitir la configuración. Asegúrese de habilitar este modo antes de instalar la segunda controladora. La iDRAC realiza una comprobación de la funcionalidad del expansor antes de permitir que se configure este modo y no comprueba 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.

NOTA: Cuando dos o más backplanes están conectados a una sola controladora PERC, la controladora los combina y los muestra como gabinete único. Por lo tanto, se espera ver un solo backplane en la página Inventario de hardware o Almacenamiento. En Inventario de firmware, se muestra la cantidad real de backplanes presentes en el sistema.

Para modificar los ajustes, debe tener privilegios 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:

- Se muestran mensajes de advertencia cuando se cambian los ajustes, ya que existe la posibilidad de una pérdida de datos.
- Las operaciones de borrado de LC o de restablecimiento de la iDRAC no cambian los ajustes del expansor para este modo.
- Esta operación solo se soporta en tiempo real y no en etapas.
- Puede cambiar la configuración del backplane varias veces.
- Si el backplane se configura con el atributo **Ranuras físicas** en **0**, la HII de iDRAC no muestra los detalles del backplane.
- La operación de división del backplane puede provocar la pérdida de datos o la configuración externa si la asociación de unidades cambia de una controladora a otra.
- Durante la operación de división del backplane, la configuración de RAID puede verse afectada en función de 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 gabinete mediante RACADM

Para configurar el gabinete o backplane, utilice el comando `set` con los objetos en **BackplaneMode**.

Por ejemplo, para establecer el atributo BackplaneMode en modo dividido:

1. Ejecute el siguiente comando para ver el modo de backplane actual:

   ```
   racadm get storage.enclosure.1.backplanecurrentmode
   ```

   La salida es:

   ```
   BackplaneCurrentMode=UnifiedMode
   ```

2. Ejecute el siguiente comando para ver el modo solicitado:

   ```
   racadm get storage.enclosure.1.backplanerequestedmode
   ```

   La salida es:

   ```
   BackplaneRequestedMode=None
   ```

3. Ejecute el siguiente comando para establecer el modo de backplane solicitado en modo dividido:

   ```
   racadm set storage.enclosure.1.backplanerequestedmode "splitmode"
   ```

   Se mostrará una pantalla que indica que el comando se ejecutó correctamente.

4. Ejecute el siguiente comando para verificar si el atributo **backplanerequestedmode** está configurado en modo dividido:

   ```
   racadm get storage.enclosure.1.backplanerequestedmode
   ```

   La salida es:

   ```
   BackplaneRequestedMode=None (Pending=SplitMode)
   ```

5. Ejecute el comando `storage get controllers` y anote el ID de instancia de la controladora.
6. Ejecute el siguiente comando para crear un trabajo:

   ```
   racadm jobqueue create <controller instance ID> -s TIME_NOW --realtime
   ```

   Se devuelve un ID de trabajo.

7. Ejecute el siguiente comando para consultar el estado del trabajo:

   ```
   racadm jobqueue view -i JID_xxxxxxxx
   ```

en el que, `JID_xxxxxxxx` es el ID de trabajo del paso 6.

El estado se muestra como Pendiente.

Continúe consultando el ID de trabajo hasta que vea el estado Completo (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
```

La salida es:

```
BackplaneRequestedMode=SplitMode
```

9. Ejecute el siguiente comando para realizar un reinicio en frío del servidor:

```
racadm serveraction powercycle
```

10. Después de que el sistema complete la POST y CSIOR, escriba el siguiente comando para verificar `backplanerequestedmode`:

```
racadm get storage.enclosure.1.backplanerequestedmode
```

La salida es:

```
BackplaneRequestedMode=None
```

11. Ejecute lo siguiente para verificar si el modo de backplane está configurado en modo dividido:

```
racadm get storage.enclosure.1.backplanecurrentmode
```

La salida es:

```
BackplaneCurrentMode=SplitMode
```

12. Ejecute el siguiente comando y verifique que solo se muestren de 0 a 11 unidades:

```
racadm storage get pdisks
```

Para obtener más información sobre los comandos de RACADM, consulte **Guía de referencia de la interfaz de línea de comandos RACADM para iDRAC**, disponible en **dell.com/idracmanuals**.

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 la iDRAC, vaya a **Almacenamiento** > **Descripción general** > **Gabinetes**.
2. En la opción **Gabinete**, seleccione el gabinete que desea configurar.
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 las siguientes:
   - Modo unificado
   - Modo dividido
   - Modo dividido 4:20
   - Modo dividido 8:16
   - Modo dividido 16:8
   - Modo dividido 20:4
5. Haga clic en **Agregar a operaciones pendientes**.
   Se creará una identificación de trabajo.
6. Haga clic en **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.

NOTA: Para evitar problemas de inventario, en caso de que se produzca algún cambio en la conexión de cables del backplane, es necesario un reinicio adicional de la iDRAC y un ciclo de encendido y apagado del host.

Ajuste del modo 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 necesita un ciclo de apagado y encendido del servidor para que cualquier cambio en el ajuste surta efecto.

Debe tener privilegios de control de servidor para modificar este ajuste.

NOTA: No puede establecer el modo SGPIO mediante la interfaz web de iDRAC.

Configuración del modo de SGPIO mediante RACADM

Para configurar el modo de SGPIO, utilice el comando `set` con los objetos en el grupo `SGPIOMode`.

Si se establece en deshabilitado, es el modo I2C. Si está habilitado, se establece en modo 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 el nombre de recurso del gabinete

Establecer el Nombre de activo del gabinete permite al usuario configurar el Nombre de activo de un gabinete de almacenamiento.

El usuario puede cambiar la propiedad Nombre de activo del gabinete para identificar los recintos fácilmente. Estos campos se comprueban en busca de valores no válidos y se muestra un error si se ingresa un valor no válido. Estos campos forman parte del firmware del gabinete; los datos que se muestran inicialmente son los valores guardados en el firmware.

NOTA: El Nombre del activo tiene un límite de 32 caracteres que incluye el carácter nulo.

NOTA: Estas operaciones no están soportadas en gabinetes internos.

Establecer la etiqueta de recurso del gabinete

Establecer la Etiqueta de activo del gabinete le permite configurar la Etiqueta de activo de un gabinete de almacenamiento.

El usuario puede cambiar la propiedad de la Etiqueta de activo del gabinete para identificar los gabinetes. Estos campos se comprueban en busca de valores no válidos y se muestra un error si se ingresa un valor no válido. Estos campos forman parte del firmware del gabinete; los datos que se muestran inicialmente son los valores guardados en el firmware.

NOTA: La Etiqueta de activo tiene un límite de 10 caracteres que incluye el carácter nulo.

NOTA: Estas operaciones no están soportadas en gabinetes internos.

Selección del modo de operación para aplicar los ajustes

Cuando cree y administre discos virtuales, configure discos físicos, controladoras y gabinetes, o restablezca controladoras, antes de aplicar los diversos ajustes, debe seleccionar el modo de operación. Es decir, especifique cuándo desea aplicar la configuración:

- Inmediatamente
- Durante el siguiente reinicio del sistema
- A una hora programada
- Como una operación pendiente que se aplicará como un lote como parte de un solo trabajo.

Elección del modo de operación mediante la interfaz web

A fin de seleccionar el modo de funcionamiento para aplicar los ajustes:

1. Puede seleccionar el modo de operación cuando se encuentra en cualquiera de las siguientes páginas:
   - **Almacenamiento** > **Discos físicos**.
   - **Almacenamiento** > **Discos virtuales**
   - **Almacenamiento** > **Controladoras**
   - **Almacenamiento** > **Gabinetes**
2. Seleccione una de las siguientes opciones en el menú desplegable **Aplicar modo de operación**:
   - **Al siguiente reinicio**: Seleccione esta opción para aplicar los ajustes durante el siguiente reinicio del sistema.
   - **A la hora programada**: Seleccione esta opción para aplicar los ajustes 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. Los ajustes se aplican entre la hora de inicio y la hora de finalización.
     - En el menú desplegable, seleccione el tipo de reinicio:
       - Sin reinicio (se reinicia el sistema manualmente)
       - Apagado ordenado
       - Forzar apagado
       - Realizar ciclo de encendido del sistema (reinicio mediante suministro de energía)
   - **Agregar a operaciones pendientes**: Seleccione esta opción a fin de crear una operación pendiente para aplicar los ajustes. Puede ver todas las operaciones pendientes de una controladora en la página **Almacenamiento** > **Descripción general** > **Operaciones pendientes**.

   NOTA:
   - La opción **Agregar a operaciones pendientes** no se aplica a la página **Operaciones pendientes** ni a SSD PCIe en la página **Discos físicos** > **Configuración**.
   - Solo la opción **Aplicar ahora** está disponible en la página **Configuración del gabinete**.
3. Haga clic en **Aplicar**.
   Según el modo de funcionamiento seleccionado, se aplican los ajustes.

Selección 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 RACADM de Integrated Dell Remote Access Controller.

Visualización y aplicación de operaciones pendientes

Puede ver y confirmar las operaciones pendientes de la controladora de almacenamiento. Todos los valores se aplicarán a la vez, durante el siguiente reinicio o a una hora programada en función de las opciones seleccionadas. Puede eliminar todas las operaciones pendientes para una controladora. No puede eliminar las operaciones pendientes individuales.

Se crean operaciones pendientes en los componentes seleccionados (controladoras, gabinetes, discos físicos y discos virtuales).

Los trabajos de configuración se crean solo en la controladora. En el caso de SSD PCIe, el trabajo se crea en el disco SSD PCIe y no en el extensor PCIe.

Visualización, aplicación o eliminación de operaciones pendientes mediante la interfaz web

1. En la interfaz web de iDRAC, vaya a **Almacenamiento** > **Descripción general** > **Operaciones pendientes**.
   Aparecerá 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 muestra 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 de 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:
   - **Al siguiente reinicio**: Seleccione esta opción para confirmar todas las operaciones durante el siguiente reinicio del sistema.
   - **A la hora programada**: Seleccione esta opción para confirmar las operaciones en un día y hora programados.
     - **Hora de inicio** y **Hora de finalización**: haga clic en los íconos de calendario y seleccione los días. Desde los menús desplegables, seleccione la hora. La acción 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)
5. Si el trabajo de confirmación no se ha creado, aparecerá un mensaje indicando que la creación de trabajos no se completó correctamente. También se muestra la identificación del mensaje y la acción de respuesta recomendada.
6. Si el trabajo de confirmación no se ha creado, aparecerá un mensaje indicando que no se creó la Id. del trabajo para la controladora seleccionada. Haga clic en **Cola de trabajos** para ver el progreso del trabajo en la página **Cola de trabajos**.

   Si las operaciones de borrar configuración ajena, importar configuración ajena, operaciones de clave de seguridad o de cifrar discos virtuales están en estado pendiente y, si estas son las únicas operaciones pendientes, no podrá crear un trabajo desde la página **Operaciones pendientes**. Debe realizar cualquier otra operación de configuración de almacenamiento o utilizar RACADM para crear el trabajo de configuración necesario en la controladora requerida.

   No puede ver ni borrar las operaciones pendientes de las SSD PCIe en la página **Operaciones pendientes**. Utilice el comando racadm a fin de borrar las operaciones pendientes para las SSD PCIe.

Visualización y aplicación de operaciones pendientes mediante RACADM

Para aplicar las operaciones pendientes, utilice el comando **jobqueue**.

Para obtener más información, consulte **Guía de referencia de la línea de comandos RACADM de iDRAC**, disponible en **dell.com/idracmanuals**.

Dispositivos de almacenamiento: aplicar situaciones de 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 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 ve la opción para crear un trabajo en las páginas de configuración de almacenamiento, vaya a la página **Visión general del almacenamiento** > **Operaciones pendientes** a fin de ver las operaciones pendientes existentes y crear un trabajo nuevo 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 a fin de borrar las operaciones pendientes para las SSD de PCIe.

LED de componentes que parpadean o no

Puede localizar un disco físico, una unidad de disco virtual y una SSD PCIe dentro en un gabinete haciendo parpadear uno de los diodos emisores de luz (LED) en el disco.

Debe tener privilegios de inicio de sesión + control y configuración del sistema para hacer que un LED parpadee o deje de parpadear.

La controladora debe ser apta para la configuración en tiempo real. La compatibilidad en tiempo real de esta función solo está disponible en el firmware de la PERC 9.1 y versiones posteriores.

NOTA: La opción de hacer parpadear o dejar de parpadear no se soporta con los servidores sin backplane.

Hacer parpadear o dejar de hacer parpadear los LED de componentes mediante la interfaz web

Para hacer parpadear o dejar de hacer parpadear LED de componentes.

1. En la interfaz web de iDRAC, vaya a cualquiera de las siguientes páginas según sus requisitos:
   - **Almacenamiento** > **Visión general** > **Discos físicos** > **Estados**: muestra la página de los discos físicos identificados, en la que puede hacer parpadear o dejar de hacer parpadear los discos físicos y las SSD PCIe.
   - **Almacenamiento** > **Visión general** > **Discos virtuales** > **Estados**: muestra la página de los discos virtuales identificados, en la que puede 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 de todas las unidades de disco físico o SSD PCIe: seleccione la opción **Seleccionar/deseleccionar todo** y haga clic en **Hacer parpadear** a fin de iniciar el parpadeo para todas las unidades de disco físico y los SSD PCIe. De forma similar, haga clic en **Dejar de hacer parpadear** para detener el parpadeo de los LED .
   - Seleccione o anule la selección de unidades de disco físico o SSD PCIe: seleccione una o más unidades de disco físico y haga clic en **Hacer parpadear** para iniciar el parpadeo de los LED para las unidades de disco físicas o los SSD PCIe. De forma similar, haga clic en **Dejar de hacer parpadear** para detener el parpadeo de los LED .
4. Si se encuentra en la página **Identificar disco virtual**:
   - 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 parpadear o dejar de parpadear no es satisfactoria, aparecerá un mensaje de error.

Hacer parpadear o dejar de hacer parpadear la LED de componentes mediante RACADM

Para hacer parpadear o dejar de hacer parpadear las LED de los 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 **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.

NOTA: Después de realizar un arranque en caliente del servidor, es posible que iDRAC informe un mensaje `Disk Inserted` en los registros de LC para las unidades que están detrás del HBA. Ignore esta entrada de registro.

20

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, los atributos se muestran en orden alfabético.

NOTA: El contenido de ayuda de nivel de atributo se genera dinámicamente.

Aplicar

El botón **Aplicar** permanece atenuado hasta que se modifica alguno de los atributos. Después de cambiar un atributo, haga clic en **Aplicar**. El atributo se modifica con los cambios necesarios. Si la solicitud no puede establecer el atributo del BIOS, se muestra un mensaje de error. Para obtener más información, consulte *Guía de referencia de mensajes de error y eventos de los servidores PowerEdge 17G, 16G, 15G, 14G y 13G de Dell Technologies* que se encuentra disponible en el sitio de soporte de Dell.

Descartar cambios

El botón **Descartar cambios** permanece atenuado hasta que se modifica 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 para aplicar, el usuario se redirige a la página de 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 de LC.

Si hace clic en **Aplicar y reiniciar**, se reinicia el servidor inmediatamente para configurar todos los cambios necesarios. Si la solicitud no puede establecer los atributos del BIOS, se muestra un mensaje de error.

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. Si la solicitud no puede establecer los atributos del BIOS, se muestra un mensaje de error.

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, este puede hacer clic en el botón **Eliminar todos los valores pendientes** para finalizar todas las modificaciones. Si la solicitud no puede eliminar los atributos del BIOS, se muestra un mensaje de error.

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 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 de 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 característica, se requiere una licencia iDRAC Datacenter.
- Debe tener el privilegio de depuración para poder utilizar esta función.

iDRAC realiza automáticamente la verificación de secciones inmutables de la imagen del BIOS en las siguientes situaciones:

- 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 de recuperación del BIOS**: la imagen del BIOS se recupera automáticamente durante el proceso de arranque del host después de que el mismo BIOS detecta 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 la ROM del BIOS principal**: la única ROM principal se divide en ROM de datos y ROM de código. La iDRAC tiene control/acceso completo a la ROM de 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: Cuando se enciende el servidor desde el estado **Apagado**, es posible que la iDRAC tarde entre 20 y 30 segundos en informar el estado de alimentación como **Encendido**.

21

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. 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
- Cifrado de video: activado / desactivado
- Video del servidor local: activado / desactivado
- 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 soportado.

  NOTA:
  - Cualquier cambio en la configuración del servidor Web provocará la finalización de la sesión de consola virtual existente.
  - Incluso si la opción de cifrado de video está deshabilitada en la GUI, puede configurar la característica mediante otras interfaces. El cifrado de video está habilitado de manera predeterminada.
  - Puede que el enlace de la consola virtual se interrumpa mientras se ejecuta el estrés de video en Internet Explorer.
- 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.
- Puede abrir hasta seis sesiones de consola virtual de la estación de administración en el servidor administrado.
- 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.

.

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 explorador para acceder a la consola virtual, consulte Configuración de exploradores web para usar la consola virtual.

Temas:

Resoluciones de pantalla y velocidades de actualización soportadas

En la siguiente tabla, se enumeran las resoluciones de pantalla y las velocidades de actualización soportadas correspondientes para una sesión de consola virtual que se ejecuta en el servidor administrado.

Tabla 50. Resoluciones de pantalla y velocidades de actualización soportadas

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
1920x1200	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 una 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 la 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 información acerca de las opciones, consulte la **Ayuda en línea de la iDRAC**.

   NOTA: Si utiliza un sistema operativo Nano, deshabilite la característica **Bloqueo automático del sistema** en la página **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 el comando `set` con los objetos en el grupo **iDRAC.VirtualConsole**.

Para obtener más información, consulte Guía de la CLI RACADM de Integrated Dell Remote Access Controller.

Visualización previa de la consola virtual

Antes de iniciar la consola virtual, puede obtener una vista previa del estado de la consola virtual en la página **Sistema** > **Propiedades** > **Resumen del sistema**. En la sección **Vista previa de la consola virtual** se muestra una imagen en la que se muestra 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 solo estará disponible si habilitó 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 una sesión de consola virtual desde un explorador web del sistema administrado.

Antes de iniciar la consola virtual, asegúrese de lo siguiente:

- Dispone de privilegios de administrador.
- Hay un ancho de banda de red mínimo de 1 Mb/seg disponible.

NOTA: Cuando el puerto HTTP personalizado o el puerto predeterminado están configurados en iDRAC, borre la caché del navegador y, a continuación, inicie iDRAC con HTTPS y acepte los certificados. A continuación, inicie sesión en iDRAC e inicie la consola virtual.

NOTA: Si la controladora de video integrada está desactivada en el BIOS y se inicia la consola virtual, el visor de la consola virtual aparecerá en blanco.

La consola virtual incluye los siguientes controles de consola:

1. **General**: establece las macros de teclado, la relación de aspecto y el modo táctil.
2. **KVM**: muestra la velocidad de fotogramas, el ancho de banda, la compresión y la velocidad de los paquetes.
3. **Rendimiento**: cambia la calidad y la velocidad del video.
4. **Lista de usuarios**: muestra 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.

NOTA: En el iDRAC versión 5.10.00.00, si la sesión de RFS está activa, se bloquea la sesión de medios virtuales. Por lo tanto, si actualiza de la versión 4.40.00.00 a la versión 5.10.00.00 con la sesión de RFS activa, RFS se vuelve a montar cuando iDRAC esté activo. En este caso, si intenta iniciar una sesión de medios virtuales, se produce un error y se muestra el mensaje `Virtual media already in use`.

Inicio de la consola virtual mediante la interfaz web

Puede iniciar la consola virtual de las siguientes maneras:

- 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 el acceso no autorizado a la aplicación, navegue por estos cuadros de mensaje en un plazo de tres minutos. De lo contrario, se le solicitará que vuelva a iniciar la aplicación.

Si aparece una o más ventanas de alerta de seguridad durante el inicio del 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 una URL

Para iniciar la consola virtual mediante la URL:

1. Abra un navegador web soportado y, en el cuadro dirección, escriba la siguiente URL en minúscula: **https://iDRAC_ip/console**
2. Según la configuración de inicio de sesión, se muestra la página **Inicio de sesión** correspondiente:
   - Si el Single Sign On está deshabilitado y el inicio de sesión local, de Active Directory, LDAP o con tarjeta inteligente está habilitado, se muestra la página de **Inicio de sesión** correspondiente.
   - Si el inicio de sesión único está habilitado, se inicia el **Visor de la consola virtual** y se muestra la página de la **Consola virtual** en segundo plano.

   NOTA: Internet Explorer soporta los inicios de sesión locales, de Active Directory, LDAP, de tarjeta inteligente (SC) y de inicio de sesión único (SSO). Firefox soporta inicios de sesión locales, AD y SSO en sistemas operativos basados en Windows e inicios de sesión locales, de Active Directory y LDAP en sistemas operativos basados en Linux.

   NOTA: Si no tiene el privilegio de acceso a la consola virtual, pero tiene el privilegio de acceso a medios virtuales, el uso de esta URL inicia los medios virtuales en lugar de la consola virtual.

Uso del visor de la consola virtual

El visor de la consola virtual ofrece varios controles, como la sincronización de mouse, el escalamiento de la consola virtual, las opciones de chat, las macros de teclado, las acciones de alimentación, los dispositivos de arranque siguientes y el acceso a los medios virtuales. Para obtener información acerca de cómo usar estas características, consulte la **Ayuda en línea de iDRAC**.

NOTA: Si el servidor remoto está apagado, se mostrará el mensaje "Sin señal".

En la barra de título Visor de la consola virtual, se muestra el nombre DNS o la dirección IP de la iDRAC a la que está conectado desde la estación de administración. Si iDRAC no tiene un nombre DNS, se muestra la dirección IP. El formato es:

- Servidores en rack y torre:`<DNS name / IPv6 address / IPv4 address>, <Model>, User: <username>, <fps>`

En ocasiones, el visor de la consola virtual puede mostrar videos de baja calidad. Esto se debe a la lentitud de la conectividad de red, que provoca la pérdida de uno o dos fotogramas de video cuando inicia la sesión de la consola virtual. Para transmitir todos los fotogramas de video y mejorar la calidad de video posterior, 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**.

Uso de una consola virtual

NOTA: De manera predeterminada, el tipo de consola virtual está establecido como eHTML5.

Puede iniciar una consola virtual como una ventana emergente mediante uno de los métodos siguientes:

- En la página de inicio del iDRAC, haga clic en el enlace **Iniciar la consola virtual** disponible en la sesión Vista previa de consola.
- En la página Consola virtual del iDRAC, haga clic en el enlace **Iniciar la consola virtual**.
- En la página de inicio de sesión de iDRAC, escriba **https//<iDRAC IP>/console**. Este método se denomina inicio directo.

En la consola virtual de eHTML5 están disponibles las siguientes opciones de menú:

- Alimentación

- Arranque
- Charla
- Teclado
- Captura de pantalla
- Actualizar
- Pantalla completa
- Desconectar visor
- Controles de la consola
- Medios virtuales

La opción **Pasar todas las pulsaciones de teclas al servidor** no es soportada en la consola virtual eHTML5. Utilice el teclado y las macros del teclado para todas las teclas de función.

- **General**:
  - **Control de consola**: tiene las siguientes opciones de configuración:
    - Macros del teclado: Son soportadas en la consola virtual eHTML5 y aparecen en las siguientes opciones de menú desplegable. Haga clic en **Aplicar** para aplicar la combinación de teclas seleccionada en el servidor.
      - Ctrl+Alt+Supr
      - 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+Espacio
      - Alt+Intro
      - Alt+Guion
      - 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
      - Pausa
      - Pestaña
      - Ctrl+Intro
      - PetSis
      - Alt+SysReq
      - Win + P

- Relación de aspecto: La imagen de video de la consola virtual eHTML5 ajusta automáticamente el tamaño para que se pueda ver la imagen. Las siguientes opciones de configuración aparecen en una lista desplegable:
  - Mantener
  - No mantener.

  Haga clic en **Aplicar** para aplicar los valores seleccionados en el servidor.
- Modo táctil: La consola virtual eHTML5 soporta la función de modo táctil. Las siguientes opciones de configuración aparecen en una lista desplegable:
  - Directo
  - Relativa

  Haga clic en **Aplicar** para aplicar los valores seleccionados en el servidor.

- **Portapapeles virtual**: El portapapeles virtual permite cortar/copiar/pegar el búfer de texto de la consola virtual en el servidor host de iDRAC. El servidor host podría estar en el BIOS, UEFI o en un símbolo del sistema operativo. Esta es una acción unidireccional desde el sistema cliente hasta el servidor host de iDRAC únicamente. Siga estos pasos para utilizar el portapapeles virtual:
  - Coloque el cursor del mouse o el foco del teclado en la ventana deseada en el escritorio del servidor host.
  - Seleccione el menú **Controles de la consola** en vConsole.
  - Copie el búfer del portapapeles del SO mediante las teclas de acceso directo del teclado, el mouse o los controles del panel táctil, según el sistema operativo del cliente. O bien, puede escribir el texto manualmente en el cuadro de texto.
  - Haga clic en **Enviar Portapapeles al host**.
  - A continuación, aparece el texto en la ventana activa del servidor host.

  NOTA:
  - Esta característica está disponible en la licencia Enterprise y Datacenter.
  - Esta función solo admite texto ASCII.
  - Esta función solo soporta el teclado en inglés.
  - No se admiten caracteres de control.
  - Se permiten caracteres como **nueva línea** y **tabulador**.
  - El tamaño del búfer de texto está limitado a 4000 caracteres.
  - Si se pega más del búfer máximo, el cuadro de edición en la interfaz de usuario de iDRAC lo truncará al tamaño máximo del búfer.

- **KVM**: este menú incluye una lista de los siguientes componentes de solo lectura:
  - Velocidad de fotogramas
  - Ancho de banda
  - Compression
  - Velocidad de paquetes
- **Rendimiento**: use el botón deslizante para ajustar **Calidad máxima de video** y **Velocidad máxima de video**.
- **Lista de usuarios**: vea la lista de usuarios que han iniciado sesión en la consola virtual.
- **Teclado**: la diferencia entre el teclado virtual y el físico es que el teclado virtual cambia su diseño según el idioma del navegador.

  NOTA: Asegúrese de que el idioma de vKeyboard y el idioma del sistema operativo del host sean los mismos.

- **Medios virtuales**: haga clic en la opción **Conectar medios virtuales** para iniciar la sesión de medios virtuales.
  - **Conectar medios virtuales**: este menú contiene las opciones “Asignar CD/DVD”, “Asignar disco extraíble”, “Asignar dispositivo externo” y “Restablecimiento de USB”.
  - **Estadísticas de medios virtuales**: este menú muestra la velocidad de transferencia (solo lectura). Además, muestra los detalles de CD/DVD y discos extraíbles, como los detalles de asignación, estado (solo lectura, o no), duración y bytes de lectura/escritura.
  - **Crear imagen**: este menú le permite seleccionar una carpeta local y generar un archivo FolderName.img con contenido de la carpeta local.

NOTA: Por motivos de seguridad, el acceso de lectura/escritura está deshabilitado cuando se accede a la consola virtual en eHTML5.

Navegadores soportados

La consola virtual de eHTML5 se admite en los siguientes exploradores:

- Microsoft EDGE
- Safari 16.6
- Safari 17.x

- Mozilla Firefox 128
- Mozilla Firefox 129
- Mozilla Firefox 130
- Google Chrome 137
- Google Chrome 138

NOTA: Se recomienda tener la versión de Mac OS 10.10.2 (o posterior) instalada en el sistema.

NOTA: Si está utilizando el navegador Chrome/Edge, es posible que vea el mensaje Inicio de sesión denegado.

Para obtener más detalles sobre los exploradores y las versiones compatibles, consulte *Notas de la versión de la Guía del usuario de Integrated Dell Remote Access Controller* disponibles en la página Manuales de iDRAC..

22

Uso del módulo de servicio del iDRAC

El módulo de servicio de la iDRAC es una aplicación de software que le recomendamos instalar en el servidor (no está instalado de forma predeterminada). Complementa a iDRAC con información de monitoreo desde el sistema operativo. Cuando se importa una contraseña mediante <codeph>SHA256Password</codeph>, la iDRAC no aplicará la comprobación de la longitud de la contraseña. Puede configurar las funciones que el módulo de servicio de iDRAC monitorea para controlar la CPU y la memoria consumidas en el sistema operativo del servidor. Se ha introducido la interfaz de línea de comandos del sistema operativo del host para habilitar o deshabilitar el estado del ciclo de encendido completo de todos los componentes del sistema, excepto la PSU.

NOTA:

- Use iDRAC Service Module solo si ha instalado la licencia Express o Enterprise/Datacenter del iDRAC.
- Las versiones de iSM anteriores a la versión 4.2 no soportan TLS 1.3.
- Si la red host no está configurada correctamente, la página SupportAssist de iDRAC informa el registro de LC para indicar que hay un problema de conexión con iSM.
- Si observa la advertencia SRV042 en LC de iDRAC durante la creación de recopilaciones de SupportAssist, realice un restablecimiento completo de iDRAC para resolver esta advertencia en LC de iDRAC.

Antes de utilizar el módulo de servicio de iDRAC, asegúrese de que:

- Tiene privilegios de inicio de sesión, configuración y control del servidor en el iDRAC para habilitar o deshabilitar las características de iDRAC Service Module.
- No desactiva a opción **Configuración de iDRAC mediante RACADM local**.
- El canal de paso del sistema operativo a iDRAC está habilitado 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 iDRAC Service Module se ejecuta por primera vez, habilita 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 habilita a través de LOM en iDRAC, no se puede utilizar iDRAC Service Module.

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 la Guía del usuario de iDRAC Service Module disponible en la página iDRAC Service Module.

NOTA: Si la NIC USB está deshabilitada en iDRAC, el instalador de iSM la habilitará. Una vez finalizada la instalación, deshabilite la NIC USB si es necesario.

Instalación del módulo de servicio de la iDRAC desde la iDRAC Core

Desde la página de configuración del **iDRAC Service Module**, haga clic en **Instalar módulo de servicio**.

1. El instalador del módulo de servicio está disponible para el sistema operativo del host y se crea un trabajo en iDRAC.
   Para los sistemas operativos Microsoft Windows o Linux, inicie sesión en el servidor de forma remota o local.
2. Busque el volumen montado denominado "**SMINST**" en la lista de dispositivos y ejecute el script correspondiente:
   - En Windows, abra la línea de comandos y ejecute el archivo del lote **ISM-Win.bat**.
   - En Linux, abra el indicador de shell y ejecute el archivo de script **ISM-Lx.sh**.
3. Una vez finalizada la instalación, iDRAC mostrará el módulo de servicio como **Instalado** y la fecha de instalación.

   NOTA: El instalador estará disponible para el sistema operativo del host durante 30 minutos. Si no inicia la instalación en el plazo de 30 minutos, debe reiniciar la instalación del módulo de servicio.

Instalación del módulo de servicio de iDRAC desde iDRAC Enterprise

1. En la interfaz de usuario de iDRAC, vaya a **Ajustes de iDRAC** > **Ajustes** > **Configuración del módulo de servicios de iDRAC**.
2. Desde la página **Configuración del módulo de servicios de iDRAC**, haga clic en **Instalar módulo de servicios**.
3. Haga clic en **Iniciar consola virtual** y, luego, en **Continuar** en el cuadro de diálogo de advertencia de seguridad.
4. Para localizar el archivo del instalador de iSM, inicie sesión en el servidor de manera remota o local.

   NOTA: El instalador estará disponible para el sistema operativo del host durante 30 minutos. Si no inicia la instalación en el plazo de 30 minutos, deberá reiniciar la instalación.

5. Busque el volumen montado denominado "**SMINST**" en la lista de dispositivos y ejecute el script correspondiente:
   - En Windows, abra la línea de comandos y ejecute el archivo del lote **ISM-Win.bat**.
   - En Linux, abra el indicador de shell y ejecute el archivo de script **ISM-Lx.sh**.
6. Siga las instrucciones que aparecen en la pantalla para completar la instalación.
   En la página **Configuración de iDRAC Service Module**, el botón **Instalar módulo de servicios** queda deshabilitado después de que se completa la instalación y el estado del módulo de servicios se muestra como **En ejecución**.

Sistemas operativos admitidos para el módulo de servicio de iDRAC

Para obtener la lista de sistemas operativos soportados en iDRAC Service Module, consulte la Guía del usuario de iDRAC Service Module disponible en la página iDRAC Service Module.

Funciones de supervisión del módulo de servicio del iDRAC

El módulo de servicio del iDRAC (iSM) proporciona las siguientes funciones de supervisión:

Tabla 51. Características soportadas de iSM

En ejecución	En ejecución (funcionalidad limitada)
Compatibilidad de perfil de Redfish para atributos de red	Servicio en el sistema operativo host
Restablecimiento forzado del iDRAC	Información sobre el sistema operativo
Acceso a la iDRAC mediante el sistema operativo del host (función experimental)	Recuperación de sistema automática
Alertas SNMP de iDRAC en banda	Permitir que el módulo de servicio realice el restablecimiento forzado de la iDRAC.

Tabla 51. Características soportadas de iSM (continuación)

En ejecución	En ejecución (funcionalidad limitada)
Ver información sobre el sistema operativo	N/D
Replicar los registros de Lifecycle Controller en los registros del sistema operativo.	N/D
Utilizar las opciones de recuperación automática del sistema.	N/D
Llenado de proveedores de administración del instrumental de administración de Windows (WMI).	N/D
Integración con SupportAssist Collection. **NOTA:** Esto se aplica únicamente si se ha instalado el módulo de servicio de iDRAC versión 2.0 o posterior.	N/D
Prepárese para quitar el SSD de PCIe de NVMe **NOTA:** Para obtener más información, consulte la página Soporte para el iDRAC Service Module de Dell.	N/D
Ciclo de apagado y encendido del servidor remoto	N/D

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.

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) se replican en el registro del sistema operativo mediante el iDRAC Service Module. 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: 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.

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 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 capturas. No obstante, debe configurar el destino de la excepción.

- **Sistema operativo ESXi VMware**

  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 la página Soporte de Dell.

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 la iDRAC y las interfaces de RedFish usando la dirección IP del host sin configurar la dirección IP de la 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 del 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. El

iSM redirige la conexión a la iDRAC. El iSM crea una regla de firewall entrante, 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 de host del servidor en el que el 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 la iDRAC y las interfaces 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 **verdadero**, **falso** u **obtener**.
- **Puerto**: este es el 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 "FALSO", 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:

Para instalar, activar y configurar esta función, utilice el comando siguiente:

```
./Enable-iDRACAccessHostRoute <Enable-Flag> [ <source-port> <source-IP-range/source-ip-range-mask>]
```

<Enable-Flag>=0

Deshabilitar

`<source-port>` y `<source-IP-range/source-ip-range-mask>` no son necesarios.

<Enable-Flag>=1

Habilitar

`<source-port>` es necesario y `<source-ip-range-mask>` es opcional.

<source-IP-range>

El rango de IP debe estar en el formato **<IP-Address/subnet-mask>**. Por ejemplo: 10.95.146.98/24.

Uso de iDRAC Service Module desde la interfaz web de iDRAC

Para usar iDRAC Service Module desde la interfaz web de iDRAC, realice los siguientes pasos:

1. Vaya a **Configuración de iDRAC** > **Descripción general** > **Módulo de servicios de iDRAC** > **Configurar el módulo de servicios**. Aparece la página **Configuración de iDRAC Service Module**.
2. Puede ver lo siguiente:
   - Versión de iDRAC Service Module instalada en el sistema operativo del host
   - Estado de conexión de iDRAC Service Module con 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 realizar funciones de monitoreo 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 deshabilitada 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**
     - **Ciclo de apagado y encendido del sistema**

     Esta opción está deshabilitada si OpenManage Server Administrator está instalado en el sistema.

NOTA: Cuando iSM se encuentra en un estado de funcionalidad de modo completo o limitado e iDRAC se restablece a los ajustes de fábrica, no hay manera de que iDRAC establezca el estado de funcionalidad de modo limitado para el estado de iSM.

Uso de iDRAC Service Module desde RACADM

Para utilizar iDRAC Service Module desde RACADM, utilice los objetos del grupo `ServiceModule`.

Para obtener más información, consulte Guía de la CLI RACADM de Integrated Dell Remote Access Controller.

23

Uso del puerto USB tipo C de modo doble para la administración de servidores

En los servidores de 17.ª generación, se proporciona un puerto USB tipo C de modo doble dedicado en el panel de control, que se encuentra en la parte frontal del servidor. De manera predeterminada, el puerto está en el modo de sistema operativo. Hay un botón de ID del sistema (¡) en el panel de control. Para cambiar el puerto al modo iDRAC, mantenga presionado el botón ¡ durante 5 a 10 segundos hasta que se encienda el LED de la llave. Para volver a cambiar el puerto al modo de sistema operativo, mantenga presionado el botón ¡ nuevamente durante 5 a 10 segundos, hasta que el LED de la llave se apague.

Las operaciones de importación de perfiles de configuración del servidor (SCP) a través de USB solo son compatibles con la licencia Enterprise o Datacenter.

Puede realizar las siguientes funciones mediante el puerto USB tipo C de modo doble cuando el puerto está en modo iDRAC:

- 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 tipo C de modo doble 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 cuando se inserta un dispositivo USB.

Temas:

Configuración de iDRAC mediante perfiles de configuración del servidor en el dispositivo USB

Con el puerto USB tipo C de modo dual en modo iDRAC, puede configurar iDRAC en el servidor. Configure los valores del puerto USB tipo C de modo dual en la 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.

Configuración de los ajustes del puerto USB tipo C de modo doble mediante la interfaz de usuario de la iDRAC

Para configurar el puerto USB tipo C de modo doble:

1. Habilite el puerto USB tipo C de modo dual del servidor en la iDRAC (**Configuración** > **Configuración de BIOS** > **Dispositivos integrados**. Asegúrese de que **Todos los puertos encendidos** o **Todos los puertos apagados (dinámicos)** estén seleccionados como **Puertos USB accesibles para el usuario**. Cuando seleccione **Todos los puertos apagados (dinámicos)**, asegúrese de que **Habilitar solo los puertos frontales** esté **Habilitado**.
2. Mantenga presionado el botón de ID del sistema en el panel de control durante aproximadamente 5 a 10 segundos hasta que se encienda el LED de la llave.
   El LED USB comienza a mostrarse verde fijo y el puerto se configura como un puerto de la iDRAC.
3. En la interfaz web de iDRAC, vaya a **Configuración de iDRAC** > **Configuración** > **Configuración de USB de administración**. El **Puerto de administración USB** se establece en **Activado**.
4. En la **iDRAC administrada: SCP de USB**, seleccione una de las opciones habilitadas:
   - **Deshabilitado**
   - **Activado solamente cuando el servidor contiene configuraciones de credenciales predeterminadas.**
   - **Activado solo para archivos de configuración comprimidos**

- **Habilitado**

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

NOTA: iDRAC10 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.

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

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 la iDRAC, como la interfaz web, RACADM y Redfish, 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 la Guía del usuario de Integrated Dell Remote Access Controller* disponibles en la página Manuales de iDRAC..

NOTA: Si utiliza el sistema operativo Windows, instale un controlador RNDIS para usar esta característica.

Para acceder a la interfaz de iDRAC por medio del puerto USB:

1. Apague todas las redes inalámbricas y desconéctese de cualquier otra red cableada. Asegúrese de que ninguna de las redes o los ajustes externos o internos interfiera con la comunicación.
2. Asegúrese de que el puerto UBS se encuentre en el modo iDRAC.
3. Espere unos segundos hasta que la laptop adquiera la dirección IP 169.254.0.4. La iDRAC adquiere la dirección IP 169.254.0.3.
4. Comience a utilizar las interfaces de red de la iDRAC, como la interfaz web, RACADM y Redfish.
   Por ejemplo, para acceder a la interfaz web de la iDRAC, abra un navegador compatible y escriba la dirección **169.254.0.3** y, a continuación, presione <Intro>.
5. Cuando iDRAC utiliza el puerto USB, el indicador LED parpadea para indicar actividad. La frecuencia es de un parpadeo cada dos segundos.
6. Después de completar las acciones requeridas, desconecte el cable USB del sistema.
   El LED vuelve a verde fijo.

Importación de un perfil de configuración del servidor desde un dispositivo USB

Cree un directorio en la raíz de un dispositivo USB denominado `System_Configuration_XML` en el que se encuentren los archivos de configuración 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 incluye todos los pares atributo-valor del servidor. Esto incluye atributos de iDRAC, PERC, RAID y BIOS. Puede editar este archivo para configurar cualquier atributo en el servidor. El nombre del archivo puede ser `<servicetag>-config.xml`, , `<modelnumber>-config.xml<servicetag>-config.json`,`config.xml<modelnumber>-config.json` 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:
  - ShutdownType – Graceful, Forced, No Reboot.
  - TimeToWait (in secs) – 300 minimum and 3600 maximum.
  - EndHostPowerState – on or off.

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>
```

Debe tener privilegios de control de 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 a iDRAC:

1. Configure el puerto de administración de USB:
   - Establezca el **modo de puerto de administración de USB** en la iDRAC.
   - Establezca **iDRAC administrada: SCP de USB en "Habilitado con credenciales predeterminadas"** o **"Habilitado"**.
2. Inserte la llave USB (que tiene los archivos `configuration.xml` y `control.xml`) en el puerto USB de 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.

   NOTA: La unidad USB debe tener solo el sistema de archivos FAT32 compatible.
3. El perfil de configuración del servidor se detecta en el dispositivo USB en el subdirectorio `System_Configuration_XML` en directorio raíz del dispositivo USB. Se detecta en la siguiente secuencia:
   - `<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 detecta, la operación se detiene.

   Si **iDRAC administrada: configuración SCP de USB** se configuró en **Habilitado con credenciales predeterminadas** y la contraseña de configuración de la BIOS no es nula o si se ha modificado alguna de las cuentas de usuario del iDRAC, aparece un mensaje de error y la operación se detiene.
5. 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 se aplica la configuración. Solo cuando el servidor ya está apagado, la configuración por etapas se aplica incluso si se especifica la opción **Sin reinicio**.
7. Una vez finalizado el trabajo de importación, la pantalla LED indica que el trabajo ha finalizado.
8. Si el dispositivo USB se deja insertado en el servidor, el resultado de la operación de importación se registra en el archivo `results.xml` del dispositivo USB.

Registros de LC y mensajes de error durante las operaciones relacionadas con 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 evento en los registros de Lifecycle Controller cuando:

- El dispositivo se encuentra en modo iDRAC y se inserta o se extrae el dispositivo USB.
- El modo de puerto de administración de USB se modifica.

- El dispositivo se cambia manualmente de la iDRAC a modo de sistema operativo.
- El dispositivo se elimina de la iDRAC.

Cuando un dispositivo supera sus requisitos de alimentación según lo permitido por la especificación de USB, el dispositivo se desconecta y se genera un evento de sobrecorriente con las siguientes propiedades:

- Categoría : estado del sistema
- Tipo: dispositivo USB
- Gravedad: precaución
- Notificaciones permitidas: correo electrónico, captura de SNMP y syslog remoto.
- Acciones: ninguna

Se muestra un mensaje de error y se registra en el registro de Lifecycle Controller cuando:

- Cuando los archivos de entrada para la operación del perfil de configuración del servidor (SCP) son incorrectos.
- Cuando la unidad USB tiene errores de hardware o sistemas de archivos no compatibles.

Comportamiento del 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.

- Apagado: el puerto USB tipo C de modo doble está en modo de sistema operativo.
- Verde fijo: el puerto USB está conectado a la iDRAC o el trabajo de importación del SCP se completó correctamente.
- Verde intermitente: el trabajo de importación de SCP está en curso o I/O está en curso.
- Amarillo fijo: el trabajo de importación de SCP falló.
- Amarillo intermitente: el hardware USB tiene errores.

Archivos de registros y resultados

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 se deja insertado, los resultados del trabajo se registran en el archivo de resultados ubicado en la llave 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 haya devuelto un ID de trabajo o un error.
- ID de trabajo: los datos se registran después de que la operación de importación haya devuelto un ID de trabajo.
- Fecha y hora de inicio del trabajo: los datos se registran después de que la operación de importación haya devuelto un ID de trabajo.
- Estado: los datos se registran cuando la operación de importación devuelve un error o cuando los resultados del trabajo están disponibles.

24

Uso de Quick Sync 2

Si ejecuta Dell OpenManage Mobile en un dispositivo móvil Android o iOS, puede acceder fácilmente al servidor directamente o a través de la consola OpenManage Essentials u OpenManage Enterprise (OME). Le permite revisar los detalles del servidor y el inventario; ver los registros de eventos del sistema y LC; obtener notificaciones automáticas en dispositivos móviles desde una consola OME; asignar la dirección IP y modificar la contraseña de iDRAC; configurar los atributos clave del BIOS; y tomar medidas correctivas según sea necesario. También puede realizar un ciclo de apagado y encendido en un servidor, acceder a la consola del sistema o acceder a la GUI de la iDRAC.

OMM se puede descargar de forma gratuita desde la App Store de Apple o desde Google Play Store.

Debe instalar la aplicación OpenManage Mobile en el dispositivo móvil (admite dispositivos móviles con iOS 9.0+ y Android 5.0+) para administrar el servidor mediante la interfaz de Quick Sync 2 de iDRAC.

NOTA: Esta sección se muestra solo en aquellos servidores que tienen el módulo Quick Sync 2 en el lado izquierdo del rack.

NOTA: Esta función se admite actualmente en los dispositivos móviles con iOS de Apple y el sistema operativo Android.

Una vez Quick Sync esté configurado, active 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 a través de un dispositivo móvil (Android 5.0+ o iOS 9.0+, OMM 2.0 o superior).

Con OpenManage Assistant, es posible:

- Ver información de inventario
- Ver información de supervisión
- Configurar los valores de red básicos de iDRAC

Para obtener más información acerca de OpenManage Mobile, consulte *Guía del usuario de Dell OpenManage Mobile* disponible en la página Manuales de OpenManage..

Temas:

Configuración de iDRAC Quick Sync 2

Con la interfaz web de la iDRAC, RACADM e iDRAC HII, se puede configurar la función de Quick Sync 2 de la 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. La opción Minutos está seleccionada de manera predeterminada. El valor predeterminado es 2 minutos. El rango se encuentra entre 2 y 60 minutos.
  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 lo desactiva, el temporizador no le permite ingresar un período de tiempo de espera agotado.
- **Autenticación de lectura**: se configura en Habilitado. Esta es la opción predeterminada.
- **Wi-Fi**: se configura en Activado. Esta es la opción predeterminada.

Para configurar los ajustes, debe contar con privilegio de control del servidor. No es necesario reiniciar el servidor para que se implementen los ajustes. Una vez configurados, puede activar el botón 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 incluye una entrada en el registro de Lifecycle Controller cuando se modifica 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 RACADM de Integrated Dell Remote Access Controller.

Configuración de los ajustes de iDRAC Quick Sync 2 mediante la interfaz web

Para configurar iDRAC Quick Sync 2:

1. En la interfaz web de la iDRAC, vaya a **Configuración** > **Ajustes del sistema** > **Ajustes de hardware** > **iDRAC Quick Sync**.
2. En la sección **iDRAC Quick Sync**, en el menú **Acceso**, seleccione una de las siguientes opciones para proporcionar acceso al dispositivo móvil Android o iOS:
   - Lectura y escritura
   - Read-only
   - Deshabilitado
3. Habilitar temporizador.
4. Especificar el límite de tiempo de espera agotado.

   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 la utilidad de configuración de iDRAC

Para configurar iDRAC Quick Sync 2:

1. En la GUI de la iDRAC, vaya a **Configuración** > **Ajustes del sistema** > **Ajustes de hardware** > **iDRAC Quick Sync**.
2. En la sección **iDRAC Quick Sync**:
   - Especifique el nivel de acceso.
   - Habilite el tiempo de espera agotado.
   - Especifique el límite de tiempo de espera agotado 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 **Back** (Atrás), haga clic en **Finish** (Terminar), y posteriormente, haga clic en **Yes** (Sí).
   Se aplica los ajustes.

Uso de un dispositivo móvil para ver la información de iDRAC

Para ver la información de la iDRAC desde el dispositivo móvil, consulte *Guía del usuario de Dell OpenManage Mobile* disponible en la página Manuales de OpenManage. para ver los pasos necesarios.

25

Administración de medios virtuales

La iDRAC proporciona medios virtuales con un cliente basado en HTML5 con soporte de archivos ISO e IMG locales y 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 o 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 o deshabilitado
- Estado de conexión: conectado o 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
- Instalar aplicaciones.
- Actualizar controladores
- Instalar un sistema operativo en el sistema administrado.

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 (de 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 de 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.

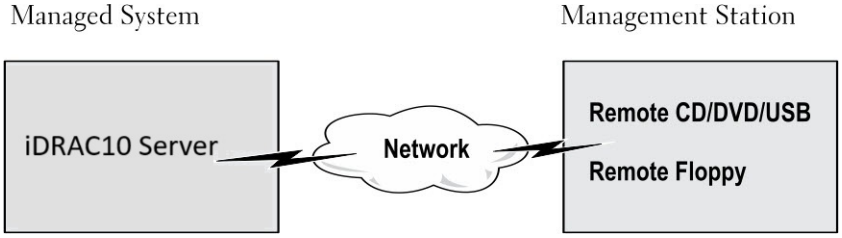


Ilustración 4. Configuración de medios virtuales

Temas:

Unidades y dispositivos compatibles

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

Tabla 52. Unidades y dispositivos compatibles

Unidad	Medios de almacenamiento compatibles
Unidades ópticas virtuales	• Archivo de imagen ISO • Archivo de imagen IMG
Unidades Flash USB	• Imagen de llave USB en el formato ISO9660

Configuración de medios virtuales

Configuración de los medios virtuales mediante la interfaz web de iDRAC

Para configurar los ajustes de medios virtuales:

PRECAUCIÓN: No restablezca la iDRAC cuando ejecute una sesión de medios virtuales. De lo contrario, se pueden producir resultados no deseados, como la pérdida de datos.

1. En la interfaz web de iDRAC, vaya a **Configuración** > **Medios virtuales** > **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, use el comando `set` con los objetos en **iDRAC.VirtualMedia group**.

Para obtener más información, consulte Guía de la CLI RACADM de Integrated Dell Remote Access Controller.

Configuración de medios virtuales mediante la utilidad de configuración de iDRAC

Puede conectar, desconectar o conectar automáticamente medios virtuales mediante la utilidad de configuración de iDRAC. Para hacerlo, realice estos pasos:

1. En la utilidad de configuración de iDRAC, vaya a **Ajustes de medios y puertos USB**.
   Se muestra la página **Ajustes de medios y puertos USB de Ajustes de iDRAC**.
2. En la sección **Medios virtuales**, seleccione **Desconectar**, **Conectar** o **Conectar automáticamente** según los requisitos. Para obtener más información acerca de estas opciones, consulte la **Ayuda en línea de la utilidad de configuración de iDRAC**.
3. Haga clic en **Back** (Atrás), haga clic en **Finish** (Terminar), y posteriormente, haga clic en **Yes** (Sí).
   Se configuran los ajustes de medios virtuales.

Estado de medios conectados y respuesta del sistema

En la siguiente tabla, se describe la respuesta del sistema en función de los ajustes de los medios conectados.

Tabla 53. Estado de medios conectados y respuesta del sistema

Estado de medios conectados	Respuesta del sistema
Desconectar	No se puede asignar una imagen al sistema.
Conectar	Los medios se asignan incluso cuando la **Vista de cliente** está cerrada.
Conexión automática	Los medios se asignan cuando se abre la **Vista de cliente** y se anulan cuando se cierra la **Vista de cliente**.

Configuración del servidor para ver dispositivos virtuales en medios virtuales

Debe configurar los siguientes ajustes en la estación de administración para permitir la visibilidad de las unidades vacías. Para ello, en el Explorador de Windows, en el menú **Organizar**, haga clic en **Opciones de carpeta y búsqueda**. En la pestaña **Ver**, deseleccione la opción **Ocultar unidades vacías en la carpeta Computadora** y haga clic en **Aceptar**.

Acceso a medios virtuales

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

Los medios virtuales y RFS son mutuamente exclusivos. Si la conexión del RFS se activa e intenta iniciar el cliente de medios virtuales, aparecerá el siguiente mensaje de error: **Los medios virtuales no están disponibles actualmente. Hay una sesión de medios virtuales o recurso compartido de archivos remoto en uso**.

Los medios virtuales y RFS son mutuamente exclusivos. Si la conexión del RFS se activa e intenta iniciar el cliente de medios virtuales, aparecerá el siguiente mensaje de error: `Virtual Media is currently unavailable. A Virtual Media or Remote File Share session is in use. If virtual media connected first then user can able to connect RFS1 also.`

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.

El archivo.img asignado a través de **Consola virtual** > **Medios virtuales o medios virtuales independientes** no soporta las operaciones de escritura en el SO del host.

Inicio de medios virtuales mediante la consola virtual

Antes de iniciar medios virtuales a través de la consola virtual, asegúrese de lo siguiente:

- La consola virtual está activada.
- El sistema está configurado para no ocultar unidades vacías: En el Explorador de Windows, vaya a **Opciones de carpeta**, borre la opción **Ocultar unidades vacías en la carpeta Equipo** y haga clic en **Aceptar**.

Para acceder a los medios virtuales mediante la consola virtual:

1. En la interfaz web de iDRAC, vaya a **Configuración** > **Consola virtual**.
   Aparece la página **Consola virtual**.
2. Haga clic en **Iniciar consola virtual**.
   Se inicia el **Visor de la consola virtual**.
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**. Se abre la ventana **Medios virtuales**.
4. En el menú **Medios virtuales**, haga clic en **Asignar CD/DVD** o **Asignar disco extraíble**. Para obtener más información, consulte Asignar discos virtuales.
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 del dispositivo virtual en el sistema administrado no coinciden con las letras de unidad física 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 conectado por USB al sistema operativo del servidor. Para agregar imágenes de medios virtuales:

1. Haga clic en **Medios virtuales** > **Crear imagen...**.
2. En el campo **Carpeta de fuente**, haga clic en **Examinar** y especifique la carpeta o el directorio que desea usar como fuente 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 aviso 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 correctamente, aparecerá un mensaje para indicarlo.
5. Haga clic en **Finish**.

   Se crea la imagen.

   Cuando se agrega una carpeta como una imagen, se crea un archivo **.img** en el escritorio de la estación de administración desde la cual se utiliza esta característica. Si este archivo **.img** se transfiere o elimina, la entrada correspondiente a esta carpeta en el menú **Medios virtuales** no funcionará. Por lo tanto, se recomienda no mover ni eliminar el archivo **.img** mientras se utiliza la **imagen**. Sin embargo, el archivo **.img** se puede eliminar después de que se anule la selección de la entrada correspondiente y, a continuación, se elimine mediante **Eliminar imagen** para eliminar la entrada.

Visualización de los detalles del dispositivo virtual

Para ver los detalles del dispositivo virtual, en el visor de la consola virtual, haga clic en **Herramientas** > **Estadísticas**. En la ventana **Estadísticas**, la sección **Medios virtuales** muestra los dispositivos virtuales asignados y la actividad de lectura/escritura de cada dispositivo. Si los medios virtuales están conectados, se muestra esta información. Si los medios virtuales no están conectados, aparecerá el mensaje “Los medios virtuales no están conectados”.

Si los medios virtuales se inician sin utilizar la consola virtual, la sección **Medios virtuales** se muestra como un cuadro de diálogo. Proporciona información sobre los dispositivos asignados.

Restablecimiento de USB

Para restablecer el dispositivo USB:

1. En el visor de la consola virtual, haga clic en **Herramientas** > **Estadísticas**.
   Se mostrará la ventana **Estadísticas**.
2. En **Medios virtuales**, haga clic en **Restablecimiento de USB**.
   Se muestra un mensaje que advierte al usuario que el restablecimiento de la conexión USB puede afectar todas las entradas al dispositivo de objetivo, incluidos los medios virtuales, el teclado y el mouse.
3. Haga clic en **Sí**.
   Se restablece el USB.

   NOTA: Los medios virtuales de iDRAC no finalizan incluso después de cerrar sesión en la interfaz web de iDRAC.

Asignación de la unidad virtual

Para asignar la unidad virtual:

NOTA: Mientras utiliza medios virtuales, 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
   - Asignar dispositivo externo

   La opción **Asignar DVD/CD** se puede usar para archivos ISO y la opción **Asignar disco extraíble** puede utilizarse para imágenes con medios virtuales basados en eHTML5. La opción **Asignar dispositivo externo** se puede usar para asignar unidades USB físicas.

   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 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, realice estos pasos:

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. Habilite los puertos que están realmente presentes y conectados al disco duro.
4. Acceda a la ventana **Cliente** de medios virtuales. Muestra las unidades correctas que se pueden asignar.

Borrado de la caché de Java

En caso de que se produzcan errores inesperados durante el uso de USB, borre la caché de Java. Siga los pasos que se indican a continuación para borrar la caché de Java:

1. En el panel de control de Java, en la pestaña **General**, haga clic en **Ajustes** en la sección **Archivos temporales de Internet**. Aparecerá el cuadro de diálogo **Ajustes de archivos temporales**.
2. Haga clic en **Eliminar archivos** en el cuadro de diálogo Ajustes de archivos temporales.

   Aparecerá el cuadro de diálogo **Eliminar archivos y aplicaciones**.
3. Haga clic en **Aceptar** en el cuadro de diálogo **Eliminar archivos y aplicaciones**. Con esto se eliminan todas las aplicaciones y los applets descargados de la caché.
4. Haga clic en **Aceptar** en el cuadro de diálogo **Ajustes de archivos temporales**. Si desea eliminar una aplicación y un applet específicos de la caché, haga clic en las opciones Ver aplicación y Ver applet respectivamente.

Anulación de asignación de la unidad virtual

Para anular la asignación de la unidad virtual:

1. En el menú **Consola virtual**, realice cualquiera de las siguientes acciones:
   - Haga clic en el tipo de dispositivo que desea anular la asignación.
   - Haga clic en **Desconectar medios virtuales**.

   Aparecerá un mensaje solicitando confirmación.
2. Haga clic en **Sí**.
   La marca de verificación para ese elemento de menú desaparecerá para indicar que no está asignado al servidor host.

   NOTA: Después de anular la asignación de 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 anular la asignación de una unidad de DVD virtual en el sistema operativo Linux, desmonte la unidad y expúlsela.

Habilitación del arranque único para medios virtuales

Puede cambiar el orden de arranque solo una vez cuando inicia después de conectar un dispositivo de medios virtuales remoto.

Antes de habilitar la opción de arranque único, asegúrese de lo siguiente:

- Cuenta con privilegios de **Configuración de usuario**.
- Asigne las unidades locales o virtuales (CD/DVD, disquete o dispositivo flash USB) con el medio o la imagen de arranque mediante las opciones de medios virtuales
- Los medios virtuales se encuentran en estado **Conectado** para que las unidades virtuales aparezcan en la secuencia de arranque.

Para habilitar la opción de arranque único e iniciar el sistema administrado desde los medios virtuales:

1. En la interfaz web de la iDRAC, vaya a **Visión general** > **Servidor** > **Medios conectados**.
2. En **Medios virtuales**, seleccione **Habilitar arranque una vez** y haga clic en **Aplicar**.
3. Encienda el sistema administrado y presione **<F2>** durante el arranque.
4. Cambie la secuencia de arranque para que se inicie desde el dispositivo de medios virtuales remoto.
5. Reinicie el servidor.
   El sistema administrado arranca una vez desde los medios virtuales.

Recurso compartido de archivos remotos

Esta función está disponible únicamente con la licencia de iDRAC Enterprise o Datacenter.

Los montajes de RFS son capaces de realizar cambios en los atributos de lectura/escritura y solo se soportan desde racadm/redfish.

NOTA: Antes de utilizar RFS, asegúrese de tener un ancho de banda de red mínimo de 1 MB/s.

Remote File Share 1 (RFS1)

La característica Recurso compartido de archivos remotos 1 (RFS1) utiliza la implementación de medios virtuales en iDRAC.

Cuando se monta un archivo de imagen con la característica RFS1, ambas unidades de disco virtual de medios virtuales se vuelven visibles para el sistema operativo del host. Si se asigna un archivo **.img** y, a continuación, se utiliza la unidad virtual de disquete/duro para presentar el archivo de imagen ante el sistema operativo. Si se asigna un archivo **.iso** y, a continuación, se utiliza la unidad virtual de CD/DVD para presentar el archivo de imagen ante el sistema operativo. La unidad virtual no usada aparecerá como unidad vacía ante el sistema operativo. El cliente de medios virtuales puede asignar imágenes o unidades de disco duro a ambas unidades virtuales, pero RFS solo puede usar una cada vez. Las funciones RFS y Medios virtuales son mutuamente exclusivas.

NOTA:

- RFS1 aparece como unidad óptica virtual o unidad de disquete cuando no existe ninguna sesión de medios virtuales activa, según la imagen adjunta.
- RFS1 aparece como archivo de red virtual 1 cuando existe una sesión de medios virtuales activa, ya que la unidad óptica virtual y las unidades de disquete virtual se consumen con los medios virtuales.

Ingrese la información requerida y haga clic en **Conectar** para conectarse al RFS1. Para desconectarse del RFS1, haga clic en **Desconectar**. Para obtener más información acerca de la información de campo obligatoria, consulte **Ayuda en línea** en la interfaz de usuario de iDRAC.

NOTA:

- El tiempo de espera agotado de la iDRAC para la conexión del RFS es de 55 segundos. Si la conexión tarda más de 55 segundos, aparece el error de tiempo de espera agotado.
- Se soportan la autenticación básica y la autenticación de síntesis para los recursos compartidos HTTP/HTTPS.
- **Conectar** está desactivado si la función RFS no tiene licencia. La opción **Desconectar** está siempre disponible, independientemente del estado de la licencia. Haga clic en **Desconectar** para desconectar una conexión RFS existente.

Casos

- Si el cliente de medios virtuales no se ejecutó, e intenta establecer una conexión con RFS, la conexión se establecerá y la imagen remota estará disponible para el sistema operativo del host.
- Si la conexión RFS no está activa, y si intenta ejecutar el cliente de medios virtuales, el cliente se ejecutará correctamente. Luego puede usar el cliente de medios virtuales para asignar dispositivos y archivos a las unidades virtuales de medios virtuales.
- Si la sesión de RFS1 está activa e intenta establecer una conexión a vMedia, se denegará la conexión a vMedia.
- Si el cliente de medios virtuales está activo e intenta establecer una conexión RFS, es posible que la unidad óptica virtual/disco flexible virtual asignado a los medios virtuales y el archivo de red virtual 1 se asignen al RFS.

Remote File Share 2 (RFS2)

El Recurso compartido de archivos remotos 2 (RFS2) es independiente del RFS1 y los medios virtuales. El RFS2 tiene su propia copia de atributos independiente del RFS1. La opción de imagen del RFS2 tiene el mismo comportamiento que el RFS1 existente en todas las

interfaces de iDRAC. Ambos se pueden conectar/desconectar de manera independiente. El RFS2 se controla a través de los atributos Activado/Desactivado y el modo Conectar del RFS2.

Para realizar el arranque con el archivo de red virtual 2 de RFS2, seleccione **Archivo de red virtual 2** en las opciones de arranque. El arranque de medios virtuales único no tiene ningún impacto en el RFS2 cuando está activado.

Ingrese la información necesaria, haga clic en **Conectar** para conectarse al RFS2 y haga clic en **Desconectar** para desconectarse del RFS2.

Cuando cargue o elimine el certificado HTTPS en el RFS1, el certificado también se cargará o eliminará en el RFS2. Esto se debe a que este certificado sirve a fin de identificar iDRAC, y sigue siendo el mismo para varios RFS o cualquier conexión compartida.

El estado de conexión de RFS se encuentra disponible en el registro de iDRAC. Una vez conectada, una unidad virtual montada mediante RFS no se desconecta aunque se cierre la sesión de iDRAC. La conexión de RFS se cierra si la iDRAC se reinicia o si se interrumpe la conexión de red.

Si actualiza el firmware de iDRAC mientras existe una conexión de RFS activa, y el modo de conexión de medios virtuales está establecido en **Conectar** o **Conectar automáticamente**, iDRAC intenta volver a establecer la conexión del RFS una vez finalizada la actualización del firmware e iDRAC se reinicia.

Si actualiza el firmware de iDRAC mientras existe una conexión de RFS activa, y el modo de conexión de medios virtuales está establecido en **Desconectar**, iDRAC no intenta volver a establecer la conexión del RFS una vez finalizada la actualización del firmware y el iDRAC se reinicia.

NOTA:

- CIFS y NFS soportan las direcciones IPv4 e IPv6.
- Cuando se realiza una conexión con un recurso compartido de archivo remoto con IPv6 mediante la entrega de un FQDN, IPv4 se debe deshabilitar en el servidor HTTPS.
- Cuando se configura iDRAC con IPv4 e IPv6, el servidor DNS puede contener registros en los que se asocie el hostname de iDRAC a ambas direcciones. Si se deshabilita la opción IPv4 en iDRAC, es posible que no se pueda acceder al recurso compartido IPv6 externo con iDRAC. Esto se debe a que el servidor DNS todavía podría contener registros de IPv4 y es posible que la resolución de nombres DNS devuelva la dirección IPv4. En tales casos, se recomienda eliminar los registros DNS de IPv4 del servidor DNS si se deshabilitó la opción IPv4 en iDRAC.
- Si está utilizando CIFS y es parte de un dominio de Active Directory, introduzca el nombre de dominio con la dirección IP en la ruta de acceso del archivo de imagen.
- Si desea acceder a un archivo desde un recurso compartido NFS, configure los siguientes permisos de recurso compartido. Se requieren estos permisos porque la iDRAC se ejecuta en modo no raíz.
  - Linux: asegúrese de que los permisos de recurso compartido se configuren al menos con el valor **Leer** para la cuenta **Otros**.
  - Windows: vaya a la ficha **Seguridad** de las propiedades de recurso compartido y agregue **Todos** en el campo **Nombres de usuario o grupos** con el privilegio **Leer y ejecutar**.
- Si ESXi se está ejecutando en el sistema administrado y monta una imagen de disco flexible (**.img**) mediante RFS, la imagen del disco flexible conectado no está disponible para el sistema operativo ESXi.
- Solo se admiten caracteres ingleses ASCII en las rutas de archivo de recurso compartido de red.
- No se soporta la característica de expulsión de unidad del sistema operativo cuando los medios virtuales se conectan mediante RFS.
- RFS puede desconectarse si no se puede acceder a la IP de iDRAC durante más de 1 minuto. Intente volver a realizar el montaje una vez que la red esté activa.
- Mientras se especifican los ajustes del recurso compartido de red, se recomienda evitar el uso de caracteres especiales en el nombre de usuario y la contraseña o codificar por porcentaje los caracteres especiales.
- Se admiten los siguientes caracteres para los campos **Nombre de usuario**, **Contraseña** y **Ruta de archivo de imagen**:
  - A-Z
  - a-z
  - Entre 0 y 9
  - Caracteres especiales: _ - ? < > / \ :* | @
  - Espacio en blanco
- Para HTTP, no utilice los siguientes caracteres: ! @ # % ^. Estos caracteres son compatibles con otros tipos de recursos compartidos. Sin embargo, para mantener la compatibilidad, utilice los caracteres recomendados.

Montaje de carpetas mediante RFS

La iDRAC admite el montaje de carpetas directamente a través del RFS. Esta característica permite adjuntar una carpeta directamente sin convertirla en un archivo ISO/IMG.

NOTA:

- Esta característica está disponible con la licencia iDRAC Enterprise o Datacenter.
- Solo es posible adjuntar carpetas a través del recurso compartido NFS y CIFS. El recurso compartido HTTP/HTTPS no se soporta.
- El tamaño de la carpeta NFS/CIFS que se adjuntará se limita a 1 GB y la cantidad máxima de subcarpetas se limita a 1000.
- No es posible asignar una carpeta vacía.

En las siguientes situaciones, se explica cómo se enumeran el RFS1 y el RFS2 en el orden de arranque del BIOS:

Escenario 1:

Si los medios virtuales ya están conectados mediante la consola virtual, los dispositivos se informan como **Unidad óptica virtual** o **Unidad de disquete virtual** en el orden de arranque del BIOS, según el tipo de imagen. Cuando se conecta el dispositivo RFS1, este se informa como **Archivo de red virtual 1** en el orden de arranque del BIOS. En el caso del dispositivo RFS2, este se informa como **Archivo de red virtual 2** en el orden de arranque del BIOS.

Escenario 2:

Cuando no hay medios virtuales conectados y se conecta un dispositivo RFS1, este se informa como **Unidad óptica virtual** o **Unidad de disco flexible virtual** en el orden de arranque del BIOS, según el tipo de imagen. Cuando se conecta un dispositivo RFS2, este se informa como **Archivo de red virtual 2** en el orden de arranque del BIOS.

Escenario 3

Cuando los medios virtuales no están conectados y el RFS1 sí lo está:

- Unidades ópticas virtuales para una imagen ISO
- Unidad de disquete virtual para una imagen IMG

La sesión de medios virtuales se bloqueará, ya que la sesión de RFS1 está activa.

Cuando los medios virtuales están conectados y RFS1 también lo está, este último aparece como Archivo de red virtual 1 para imágenes ISO e IMG. Esto es para mantener la compatibilidad con los vMedia y RFS existentes, que solo permiten una sesión a la vez. RFS2 aparece como **Archivo de red virtual 2**, independientemente de los medios virtuales y de RFS1.

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, las unidades ópticas virtuales, las unidades de disquete virtuales, el archivo de red virtual 1 y el archivo de red virtual 2 se muestran con los dispositivos de arranque estándar.
4. Asegúrese de que la unidad virtual esté habilitada y que aparezca como el primer dispositivo con medios de arranque. Si es necesario, siga las instrucciones que aparecen en la 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 iniciarse a partir de un dispositivo de arranque según el orden de arranque. Si el dispositivo virtual está conectado y hay un medio de arranque, el sistema se iniciará en el dispositivo virtual. De lo contrario, el sistema pasará por alto el dispositivo, como un dispositivo físico sin medios de arranque.

Cómo obtener acceso a los controladores

Los servidores Dell PowerEdge tienen todos los controladores de sistema operativo soportados 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 Página Soporte de Dell.

26

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 de un 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**, **.iso** o **ruta de carpeta**.

> **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.
2. Vaya a **Configuración** > **Configuración del sistema** > **Configuración de hardware** > **Primer dispositivo de inicio**.
3. Establezca el orden de inicio en la lista **Primer dispositivo de arranque** para seleccionar un medio virtual, como un disquete, un CD, un DVD, una imagen ISO, el archivo de red virtual 1 y el archivo de red virtual 2.
4. Seleccione la opción **Inicio único** para activar el sistema administrado de modo que se reinicie mediante el archivo de imagen solo para la instancia siguiente.
5. Haga clic en **Aplicar**.
6. Reinicie el sistema administrado y siga las instrucciones en pantalla para completar la implementación.

Administración de recursos compartidos de archivos remotos

Mediante la función de Remote File Share (RFS), puede establecer un archivo de imagen ISO o IMG en un recurso compartido de red y ponerlo a disposición del sistema operativo del servidor administrado como una unidad virtual. Para ello, móntelo como un CD o DVD a través de NFS, CIFS, HTTP o HTTPS. Esta función requiere licencia.

Los recursos compartidos de archivos remotos solo admiten los formatos de archivo de imagen **.img** o **.iso**. Un archivo **.img** se redirige como un disco flexible virtual y un archivo **.iso** se redirige como un CDROM virtual.

Debe tener privilegios de medios virtuales para realizar un montaje de RFS.

Esta función está disponible únicamente con la licencia de iDRAC Enterprise o Datacenter.

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 conectados**.
   Aparece la página **Medios conectados**.
2. En **Medios conectados**, seleccione **Conectar** o **Conectar automáticamente**.
3. En **Recurso compartido de archivos remoto**, especifique la ruta de acceso del archivo de imagen, el nombre de dominio, el nombre de usuario y la contraseña. Para obtener información acerca de los campos, consulte la **Ayuda en línea de iDRAC7**.

   Ejemplo de ruta de acceso de un archivo de imagen:

   - CIFS: `//<IP 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.

   NOTA: Los caracteres permitidos en los nombres de usuario y las contraseñas para los recursos compartidos de red están determinados por el tipo de recurso compartido de red. La iDRAC admite caracteres válidos para las credenciales del recurso compartido de red según lo definido por el tipo 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 recursos compartidos de archivos remotos mediante RACADM, use:

`racadm remoteimage`

`racadm remoteimage <options>`

Las opciones son:

`-c`: conectar imagen

`-d`: desconectar imagen

`-u` <username>: nombre de usuario para acceder a la carpeta compartida

`-p` <password>: contraseña para acceder a la carpeta compartida

`-l` <image_location>: ubicación de la imagen en el recurso compartido de red; use comillas dobles alrededor de la ubicación. Consulte los ejemplos de ruta de un archivo de imagen en la sección Configuración de recurso compartido de archivos remotos mediante la interfaz web.

`-s`: muestra el estado actual de la imagen remota

Ejemplos de uso

- RFS basado en CIFS:

```
racadm remoteimage -c -u "user" -p "pass" -l //shrloc/foo.iso
```

- RFS basado en NFS:

```
racadm remoteimage -c -u "user" -p "pass" -l <nfs ip>:/shrloc/foo.iso
```

- RFS basado en HTTP/HTTPS:

```
racadm remoteimage -c -u "user" -p "pass" -l http://url/shrloc/foo.iso
```

```
racadm remoteimage -c -l https://url/shareloc/foo.iso
```

- Desconectarse de la imagen remota:

```
racadm remoteimage -d
```

- Mostrar el estado actual de la imagen remota:

```
racadm remoteimage -s
```

NOTA: Este comando soporta los formatos IPV4 e IPV6. IPV6 se aplica a los recursos compartidos remotos de tipo CIFS y NFS.

NOTA: Las opciones -u y -p son obligatorias si el tipo de recurso compartido es CIFS.

NOTA: Todos los caracteres, incluidos los caracteres alfanuméricos y especiales, se permiten como parte del nombre de usuario, la contraseña y el image_location, excepto los siguientes caracteres: ' (comilla simple), "(comilla doble), ,(coma), < (menor que) y > (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`

Para obtener ayuda sobre cómo ver las propiedades de un grupo, ejecute el comando – `racadm help get`.

Para obtener ayuda sobre cómo configurar las propiedades de un grupo, ejecute el comando – `racadm help set`.

`racadm>>help remoteimage2`

NOTA: remoteimage2: permite que una imagen ISO remota esté disponible para el servidor. Requiere una licencia de recurso compartido de archivos remotos.

Uso

```
racadm remoteimage2 -c -u <user> -p <pass> -l <image_location>
racadm remoteimage2 -d
racadm remoteimage2 -s
```

Las opciones son:

`-c`: conectar imagen

`-d`: desconectar imagen

`-u` <username>: nombre de usuario para acceder a la carpeta compartida

`-p` <password>: contraseña para acceder a la carpeta compartida

`-l` <image_location>: ubicación de la imagen en el recurso compartido de red; use comillas dobles alrededor de la ubicación. Consulte los ejemplos de ruta de un archivo de imagen en la sección Configuración de recurso compartido de archivos remotos mediante la interfaz web.

`-s`: muestra el estado actual de la imagen remota

Ejemplos de uso

- RFS basado en CIFS:

```
racadm remoteimage2 -c -u "user" -p "pass" -l //shrloc/foo.iso
```

- RFS basado en NFS:

```
racadm remoteimage2 -c -u "user" -p "pass" -l <nfs ip>:/shrloc/foo.iso
```

- RFS basado en HTTP/HTTPS:

```
racadm remoteimage2 -c -u "user" -p "pass" -l http://url/shrloc/foo.iso
```

```
racadm remoteimage2 -c -l https://url/shareloc/foo.iso
```

- Desconectarse de la imagen remota:

```
racadm remoteimage2 -d
```

- Mostrar el estado actual de la imagen remota:

```
racadm remoteimage2 -s
```

NOTA: Este comando soporta los formatos IPV4 e IPV6. IPV6 se aplica a los recursos compartidos remotos de tipo CIFS y NFS.

NOTA: Las opciones -u y -p son obligatorias si el tipo de recurso compartido es CIFS.

Para obtener ayuda sobre cómo ver las propiedades de un grupo, ejecute el comando – `racadm help get`.

Para obtener ayuda sobre cómo configurar las propiedades de un grupo, ejecute el comando – `racadm help set`.

Implementación del sistema operativo mediante medios virtuales

Antes de implementar el sistema operativo mediante el medio virtual, asegúrese de lo siguiente:

- Los medios virtuales se encuentran en estado **Conectado** para que las unidades virtuales aparezcan en la secuencia de arranque.
- Si los medios virtuales están en modo de **Conexión automática**, la aplicación de medios virtuales se debe iniciar antes de arrancar el sistema.
- El recurso compartido de red contiene controladores y el archivo de imagen iniciable de sistema operativo tiene un formato estándar del sector, tal como **.img** o **.iso**.

Para implementar un sistema operativo mediante medios virtuales:

1. Realice uno de los siguientes pasos:
   - Inserte el CD o DVD de instalación del sistema operativo en la unidad de CD o DVD 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 siguientes métodos para arrancar en el dispositivo requerido:
   - Establezca el orden de arranque para que se inicie una sola vez desde el **Disquete virtual** o **CD/DVD/ISO virtual** mediante la interfaz web de iDRAC.
   - Establezca el orden de arranque a través de **Configuración del sistema** > **Ajustes del BIOS del sistema** presionando <F2> durante el arranque.
4. Reinicie el sistema administrado y siga las instrucciones en pantalla para completar la implementación.

Instalación del sistema operativo desde varios discos

1. Desasigne el CD/DVD existente.
2. Inserte el siguiente CD/DVD en la unidad óptica remota.
3. Reasigne la unidad de CD/DVD.

27

Solución de problemas de un sistema administrado mediante iDRAC

Puede diagnosticar y solucionar problemas de un sistema administrado remoto con lo siguiente:

- Consola de diagnóstico
- Código de la POST
- Videos de captura de inicio y bloqueo
- Pantalla de último bloqueo del sistema
- Registro de eventos del sistema
- Registros de Lifecycle
- Estado del panel frontal
- Indicadores de problemas
- Estado del sistema

Temas:

Uso de la consola de diagnósticos

iDRAC proporciona un conjunto estándar de herramientas de diagnóstico de red que son similares a las herramientas incluidas con los sistemas basados en Microsoft Windows o Linux. Mediante la interfaz web de iDRAC, puede acceder a las herramientas de depuración de red.

Para acceder a la consola de diagnósticos:

1. En la interfaz web de iDRAC, vaya a **Mantenimiento** > **Diagnósticos**.
   Se muestra la página **Comando de la consola de diagnósticos**.
2. En el cuadro de texto **Comando**, ingrese 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 los ajustes predeterminados**, se mostrará la

ventana **Restablecer el iDRAC a los ajustes predeterminados de fábrica**. Esta acción restablece el iDRAC a la configuración predeterminada de fábrica. Seleccione cualquiera de las opciones siguientes:

a. Conservar la 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`.

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.

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 diagnósticos automatizados remotos y exportación de los resultados 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 diagnóstico, asegúrese de que el servidor se encuentre en el estado **Fuera de POST** y que LC esté en el estado **Listo**. Para comprobar el estado de LC y del servidor, ejecute el siguiente comando:

```
racadm getremoteservicesstatus
```

- 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 RACADM de Integrated Dell Remote Access Controller.

Visualización de los códigos de la POST

Los códigos de la POST son indicadores de progreso del BIOS del sistema, que indican diversas etapas de la secuencia de arranque desde el restablecimiento del encendido y le permiten diagnosticar cualquier falla relacionada con el arranque del sistema. La página **Códigos de la POST** muestra el último código de la POST del sistema antes de arrancar el sistema operativo.

Para ver los códigos de la POST, vaya a **Mantenimiento** > **Solución de problemas** > **Código de la POST**.

La página **Código de la POST** muestra el indicador de estado del sistema, un código hexadecimal y una descripción del código.

Visualización de videos de captura de arranque y bloqueo

Puede ver las grabaciones de video de los siguientes elementos:

- **Últimos tres ciclos de arranque**: un video de ciclo de arranque registra la secuencia de eventos de un ciclo de arranque. Los videos de ciclos de inicio están organizados en el orden del más reciente al más viejo.
- **Video del último bloqueo**: un video de bloqueo registra la secuencia de eventos que provocan la falla.

NOTA: La característica de video de bloqueo está habilitada de manera predeterminada. Puede habilitar o deshabilitar esta característica según sus necesidades.

Esta es una función con licencia.

iDRAC registra 50 tramas durante el tiempo de inicio. La reproducción de las pantallas de inicio se produce a una velocidad de 1 trama por segundo. Si se restablece la iDRAC, el video de captura de inicio no está disponible debido a que se almacena en la RAM y se elimina.

NOTA:

- Debe tener privilegios de administrador o de Acceso a consola virtual para reproducir los videos de captura de arranque y captura de bloqueo.
- Es posible que el tiempo de captura de video que se muestra en el reproductor de videos de la GUI de la iDRAC difiera del tiempo de captura de video que se muestra en otros reproductores de video. El reproductor de videos de la GUI de la iDRAC muestra la hora en la zona horaria de la iDRAC mientras que todos los demás reproductores de video muestran la hora en las zonas horarias respectivas del sistema operativo.

NOTA:

- El motivo para el retraso en la disponibilidad de los archivos de captura de inicio se debe a que el búfer de captura de inicio no está completo después del inicio del host.
- Los reproductores de video predeterminados/de bandeja de entrada SLES/RHEL no son compatibles con el decodificador de video MPEG-1. Debe instalar un reproductor de video compatible con el decodificador MPEG y reproducir los archivos.
- Los videos en formato MPEG-1 no son compatibles con reproductores nativos de sistema operativo MAC.

Para ver la pantalla **Captura de inicio**, haga clic en **Mantenimiento** > **Solución de problemas** > **Captura de video**.

La pantalla **Captura de video** muestra las grabaciones de video. Para obtener más información, consulte la **Ayuda en línea de iDRAC**.

NOTA: Cuando la controladora de video incorporada está deshabilitada y el servidor tiene una controladora complementaria de video, se espera cierta latencia con respecto a la captura de inicio. Por lo tanto, en la siguiente captura se registrará la finalización de los mensajes de correo de un video.

Configuración de los ajustes de captura de video

Para configurar los ajustes de la captura de video:

1. En la interfaz web de iDRAC, vaya a **Mantenimiento** > **Solución de problemas** > **Captura de video**.
   Aparecerá la página **Captura de video**.
2. En el menú desplegable **Ajustes de la captura de video**, seleccione una de las siguientes opciones:
   - **Deshabilitar**: se deshabilita 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

Puede ver los registros de eventos del sistema (SEL) y los registros de ciclo de vida útil. Para obtener más información, consulte Visualización de los registros de eventos del sistema y Visualización de los registros 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

En Estado del sistema, se resume el estado de los siguientes componentes del sistema:

- Resumen
- Baterías
- Enfriamiento
- CPU
- Panel frontal
- Intrusión
- Memoria
- Dispositivos de red
- Fuentes de alimentación
- Voltajes

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: Indica que no hay errores presentes en el sistema administrado.
- Azul parpadeante: El modo de identificación está activado (independientemente de la presencia de error en el sistema administrado).

- Ámbar sólido: El sistema administrado está en el modo a prueba de fallos.
- Ámbar parpadeante: 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 solo para servidores en rack y en torre.

Para ver el estado de un LED de ID del sistema desde RACADM, utilice el comando `getled`.

NOTA: Durante la extracción en caliente de la unidad M.2 para la controladora BOSS N-1, el estado del panel de iDRAC se vuelve ámbar, pero el LED del indicador de estado frontal/posterior del servidor permanece en color azul.

Para obtener más información, consulte Guía de la CLI RACADM de Integrated Dell Remote Access Controller.

Indicadores de problemas de hardware

Los problemas relacionados con el hardware son los siguientes:

- Error al encender
- Ventiladores ruidosos
- Pérdida de conectividad de red
- Falla de disco duro
- Falla de medios USB
- Daños físicos

Según el problema, utilice los siguientes métodos para corregirlo:

- Vuelva a insertar el módulo o componente y reinicie el sistema
- Reemplace los discos duros o las unidades flash USB
- Vuelva a conectar o reemplace los cables de alimentación y de red

Si el problema persiste, consulte el *Manual de instalación y servicio* disponible en la página Manuales de PowerEdge para obtener información específica sobre 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 la iDRAC:

- Baterías
- CPU
- Enfriamiento
- Intrusión
- Memoria
- Fuentes de alimentación
- Medios flash extraíbles
- Voltajes
- Novedades variadas

Haga clic en cualquier nombre de componente de la sección **Condición del sistema** para ver los detalles acerca del componente.

Reinicio de iDRAC

Puede realizar un reinicio forzado o parcial de iDRAC sin apagar el servidor:

- Reinicio por hardware: en el servidor, mantenga presionado el botón LED durante 15 segundos.
- Reinicio por software: utilice la interfaz web de iDRAC o RACADM.

Reinicio de iDRAC mediante RACADM

Para reiniciar la iDRAC, utilice el comando **racreset**.

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`

Restablecimiento de iDRAC mediante la interfaz web

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.

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 de usuario para los siguientes componentes:

- Restablecimiento de los valores predeterminados del BIOS
- Diagnósticos incorporados
- Paquete de controladores para el sistema operativo integrado
- 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
- Borre discos duros, SSD y NVMe que soporten 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 toda la información que se genera cuando se reinicia iDRAC. 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: se restablece el BIOS a los valores predeterminados
- diag: diagnósticos integrados
- drvpack: paquete de controladores para el sistema operativo integrado
- lcdata: se borran los datos de Lifecycle Controller
- idrac: se restablece iDRAC a los valores predeterminados
- overwritepd: se sobrescriben los discos duros que no soportan el borrado seguro instantáneo (ISE)
- percnvcache: se restablece la memoria caché de la controladora
- secureerasepd: se borran los discos duros, SSD y NVMe que soportan ISE
- allapps: se borran todas las aplicaciones del sistema operativo

NOTA: El borrado seguro no borra el **firmware de reversión de iDRAC** de la partición cuando se utiliza el comando `racadm systemerase lcdata`.

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 RACADM de Integrated Dell Remote Access Controller.

NOTA: El enlace de Dell TechCenter aparece en la interfaz de usuario de iDRAC en los sistemas con la marca Dell.

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.

NOTA: En las versiones más recientes de iDRAC, el comando `LCWipe` quedó obsoleto. Para realizar la operación de borrado del sistema, ejecute el comando `systemerase`.

Restablecimiento de iDRAC a los ajustes predeterminados de fábrica

Puede restablecer iDRAC a los ajustes predeterminados de fábrica mediante la utilidad de configuración de iDRAC o la interfaz web de iDRAC.

Restablecimiento de iDRAC a los ajustes predeterminados de fábrica mediante la interfaz web de iDRAC

Para restablecer iDRAC a los ajustes predeterminados de fábrica mediante la interfaz web de iDRAC:

1. Vaya a **Mantenimiento** > **Diagnósticos**.
   Se muestra la página **Consola de diagnósticos**.
2. Haga clic en **Restablecer iDRAC a los ajustes predeterminados**.
   El estado de finalización se muestra en porcentaje. La iDRAC se reinicia y se restaura a los valores predeterminados de fábrica. La IP de iDRAC se restablece y no se puede acceder a ella. Puede configurar la IP mediante el panel frontal o el BIOS.

Restablecimiento de iDRAC a los ajustes predeterminados de fábrica mediante la utilidad de configuración de iDRAC

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

1. Vaya a **Restablecer la configuración de iDRAC a los ajustes predeterminados**.
   Se muestra la página **Restablecer la configuración de iDRAC a los ajustes predeterminados de Ajustes de iDRAC**.
2. Haga clic en **Sí**.
   Comienza el restablecimiento de iDRAC.
3. Haga clic en **Atrás** y vaya a la misma página **Restablecer la configuración de iDRAC a los ajustes predeterminados** para ver el mensaje de operación correcta.

28

Integración de SupportAssist en iDRAC

SupportAssist le permite crear recopilaciones de SupportAssist y utilizar otras funciones de SupportAssist para monitorear el sistema y el centro de datos. La iDRAC ofrece interfaces de aplicación para recopilar información de la plataforma que permite a los servicios de soporte resolver problemas de la plataforma y el sistema. La iDRAC le ayuda a generar una recopilación de SupportAssist del servidor y, a continuación, exportar la recopilación a una ubicación en la estación de administración (local) o a una ubicación de red compartida, como FTP, protocolo de transferencia de archivos trivial (TFS), HTTP, HTTPS, protocolo sistema de archivos de Internet común (CIFS) o sistema 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:

SupportAssist

NOTA: La iDRAC10 no es compatible con el registro de SupportAssist. Puede utilizar OpenManage Enterprise o el gateway de conexión segura para lo mismo.

Puede generar y guardar una recopilación localmente o en una red.

SupportAssist

Una vez que SupportAssist está configurado, puede revisar el panel de SupportAssist para ver el **registro de recopilación**. No es necesario estar registrado para ver o enviar el registro de recopilación.

Registro de recopilación

En el **Registro de recopilación**, se muestran los detalles de **Hora y fecha, Tipo de recopilación** (manual), **Datos recopilados** (selección personalizada, todos los datos), **Estado de recopilación** (completa con errores, completa) e **ID del trabajo**. Puede enviar la última recopilación persistente en iDRAC a Dell.

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.

Generación de SupportAssist

Para generar los registros del SO y de la aplicación, iDRAC Service Module debe estar instalado y en ejecución en el sistema operativo host.

NOTA: La recopilación de SupportAssist tarda más de 10 minutos en completarse cuando se realiza desde el SO/iDRAC mientras se ejecuta OMSA 10.1.0.0 con él.

Si debe trabajar con la Asistencia técnica en un problema con un servidor pero las políticas de seguridad restringen la conexión a Internet, puede proporcionarle a la Asistencia técnica los datos necesarios para facilitar la solución de problemas sin tener que instalar software o descargar herramientas de Dell y sin tener acceso a la Internet desde el sistema operativo del servidor o iDRAC.

Puede generar un informe de estado del servidor y luego exportar el registro de colección:

- A una ubicación en la estación de administración (local).
- A una ubicación de red compartida como el sistema de archivos de Internet comunes (CIFS) o el recurso compartido de archivos de red (NFS). Para exportar a un recurso compartido de red CIFS o NFS, se necesita conectividad de red directa al puerto de red compartido o dedicado del iDRAC.
- A Dell.

La recopilación de SupportAssist se genera en formato ZIP estándar. La recopilación puede contener la siguiente información:

- Inventario de hardware para todos los componentes (lo que incluye detalles del firmware y de la configuración de los componentes del sistema, registros de eventos del sistema de la placa base, información del estado de iDRAC y registros de Lifecycle Controller).
- Sistema operativo e información de las aplicaciones.
- Registros de la controladora de almacenamiento.
- Registros de depuración de iDRAC.
- Contiene un visor HTML5, al que se puede acceder una vez que la recopilación se haya completado.
- La recopilación proporciona una cantidad masiva de información detallada del sistema y registros en un formato fácil de usar, que se puede ver sin cargar la recopilación en el sitio de soporte técnico.

Después de que se generan los datos, puede ver los datos que contienen varios archivos XML y archivos de registro.

Cada vez que se recopilan datos, se graba un suceso en el registro de Lifecycle Controller. El evento incluye información como el usuario que inició el informe, la interfaz utilizada y la fecha y hora de la exportación.

En Windows, si se deshabilita WMI, la recopilación del recopilador del sistema operativo se detiene, y se muestra un mensaje de error.

Verifique que los niveles de privilegios sean los adecuados y asegúrese de que no haya ninguna configuración de seguridad o servidor de seguridad que impida la recopilación de los datos de software o de registro.

Antes de generar el informe de condición, compruebe lo siguiente:

- Lifecycle Controller está activado.
- Collect System Inventory On Reboot (Recopilar inventario del sistema al reiniciar) (CSIOR) está habilitada.
- Cuenta con privilegios de Inicio de sesión y Control del servidor.

Generación de SupportAssist Collection en forma manual mediante la interfaz web del iDRAC

Para generar la recopilación de SupportAssist manualmente:

1. En la interfaz web de la iDRAC, vaya a **Mantenimiento** > **SupportAssist**.
2. Haga clic en **Start a Collection**.
3. Seleccione los conjuntos de datos que se incluirán en la recopilación.
4. Puede optar por filtrar la recopilación para PII.
5. Seleccione el destino donde se debe guardar la recopilación.
   a. La opción **Guardar localmente** le permite guardar la recopilación generada en el sistema local.
   b. La opción **Guardar 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 **Guardar 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 **Guardar 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.
6. Haga clic en **Recopilar** para continuar con la generación de la recopilación.
7. Si se le solicita, acepte el acuerdo **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.

Registro de recopilación

En el **Registro de recopilación**, se muestran los detalles de **Hora y fecha, Tipo de recopilación** (manual), **Datos recopilados** (selección personalizada, todos los datos), **Estado de recopilación** (completa con errores, completa) e **ID del trabajo**. Puede enviar la última recopilación persistente en iDRAC a Dell.

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.

29

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
- Virtual console
- Medios virtuales
- Autenticación de SNMP
- Dispositivos de almacenamiento
- iDRAC Service Module
- RACADM
- Varios

Temas:

Sistema operativo

Cómo instalar el sistema operativo mediante las versiones iniciales de iDRAC10 (1.10.17.00, 1.20.05.00)

La interfaz de usuario de Lifecycle Controller no es compatible con iDRAC10. Puede instalar el sistema operativo mediante la licencia iDRAC10 Core.

A continuación, se indican los pasos para instalar el sistema operativo:

1. Cree un disco virtual en una controladora RAID de Dell:
   a. Presione **F2** durante el proceso de inicio del sistema y acceda a **System Setup**.
   b. Haga clic en **Device Settings** y seleccione la controladora RAID correspondiente.
   c. Haga clic en **Main Menu** > **Configuration Management**.
   d. Haga clic en **Crear disco virtual**.
   e. Seleccione las opciones adecuadas para definir los parámetros del disco virtual.

f. Haga clic en **Select Physical Disks** y seleccione las unidades adecuadas.
g. Haga clic en **Apply Changes** y, luego, en **OK**.
h. Haga clic en **Crear disco virtual**.
i. Seleccione **Confirm** y, luego, haga clic en **Yes**. El disco virtual se ha creado correctamente.

2. Instale el sistema operativo desde el DVD:
   a. Inserte el DVD de instalación del sistema operativo.
   b. Arranque desde el DVD para iniciar el proceso de instalación del sistema operativo.
3. Descargue las unidades faltantes e instale el sistema operativo:
   a. Descargue los controladores necesarios para el sistema operativo desde el sitio de soporte de Dell.
   b. Copie los controladores descargados en una unidad USB.
   c. Durante la instalación del sistema operativo, cuando se le soliciten los controladores, inserte la unidad USB y cargue los controladores desde ella.

Active Directory

Error de inicio de sesión en Active Directory. ¿Cómo se resuelve esto?

Para diagnosticar el problema, en la página **Configuración y administración de Active Directory**, haga clic en **Ajustes de prueba**. Revise los resultados de la prueba y corrija el problema. Cambie la configuración y ejecute la prueba hasta que el usuario de prueba supere el paso de autorización.

En general, compruebe lo siguiente:

- Durante el inicio de sesión, asegúrese de utilizar el nombre de dominio de usuario correcto y no el nombre de NetBIOS. Si tiene una cuenta de usuario local de iDRAC, inicie sesión en iDRAC con las credenciales locales. Después de iniciar sesión, asegúrese de que:
  - La opción **Active Directory habilitada** está seleccionada en la página **Configuración y administración de Active Directory**.
  - La configuración de DNS es correcta en la página de **Configuración de redes de iDRAC**.
  - El certificado de CA raíz de Active Directory correcto se carga en iDRAC si se activó 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 del grupo y el Nombre de dominio del grupo coinciden con la configuración de Active Directory si utiliza el esquema estándar.
  - Si el usuario y el objeto de iDRAC se encuentran en dominios diferentes, no seleccione la opción **Dominio de usuario en inicio de sesión**. En su lugar, seleccione la opción **Especificar un dominio** e ingrese el nombre de dominio donde reside el objeto de iDRAC.
- Compruebe los certificados SSL de la controladora de dominio para asegurarse de que la hora de iDRAC se encuentre dentro del período de validez del certificado.

El inicio de sesión de Active Directory falla 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 la validación de certificados está habilitada, cuando iDRAC establece la conexión SSL con el servidor de directorio, iDRAC utiliza el certificado de CA cargado para verificar el certificado del servidor de directorio. Las razones más comunes por las que no se supera la validación de la certificación son las siguientes:

- La fecha de iDRAC no se encuentra dentro del período de validez del certificado del servidor o del certificado de CA. Compruebe el tiempo de iDRAC y el período de validez del certificado.
- Las direcciones de la controladora de dominio configuradas en iDRAC no coinciden con el Sujeto o el Nombre alternativo del sujeto del certificado del servidor de directorio. Si está utilizando una dirección IP, lea la siguiente pregunta. Si utiliza FQDN, asegúrese de utilizar el FQDN de la controladora de dominio y no el dominio. Por ejemplo, **servername.example.com** en lugar de **example.com**.

La validación del certificado falla incluso si la dirección IP se utiliza como dirección de la controladora de dominio. ¿Cómo se resuelve esto?

Compruebe el campo Sujeto o Nombre alternativo del sujeto del certificado de la controladora de dominio. Normalmente, Active Directory usa el nombre de host y no la dirección IP de la controladora de dominio en el campo Sujeto o Nombre alternativo del sujeto del certificado de la controladora de dominio. Para resolver esto, realice cualquiera de las siguientes acciones:

- Configure el nombre de host (FQDN) de la controladora de dominio como **direcciones de la controladora de dominio** en iDRAC para que coincidan con el Sujeto o el Nombre alternativo del sujeto del certificado del servidor.
- Vuelva a emitir el certificado del servidor para utilizar una dirección IP en el campo Sujeto o Nombre alternativo del sujeto, de modo que coincida con la dirección IP configurada en iDRAC.
- Deshabilite la validación del certificado si decide confiar en esta controladora de dominio sin la validación del certificado durante el protocolo de enlace SSL.

¿Cómo configurar las direcciones de la controladora de dominio cuando se utiliza el esquema extendido en un entorno de varios dominios?

Debe ser el nombre de host (FQDN) o la dirección IP de las controladoras de dominio que prestan servicios al dominio en el que reside el objeto de iDRAC.

¿Cuándo configurar las direcciones de catálogo global?

Si utiliza un esquema estándar y los usuarios y grupos de funciones son de dominios diferentes, se necesitan direcciones de catálogo global. En este caso, solo puede usar un grupo universal.

Si utiliza un esquema estándar y todos los usuarios y grupos de funciones están en el mismo dominio, no se necesitan las direcciones de catálogo global.

Si utiliza un esquema extendido, no se utiliza la dirección de catálogo global.

¿Cómo funciona la consulta de esquema estándar?

iDRAC se conecta primero a las direcciones de controladora de dominio configuradas. Si el usuario y los grupos de funciones se encuentran en ese dominio, se guardan los privilegios.

Si se configuran las direcciones globales de la controladora, iDRAC continúa consultando el catálogo global. Si se recuperan privilegios adicionales del catálogo global, estos privilegios se acumulan.

¿iDRAC siempre utiliza 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, iDRAC realiza LDAP CONNECT solo para aislar el problema, pero no realiza un BIND de LDAP en una conexión insegura.

¿Por qué iDRAC habilita la validación de certificados de manera predeterminada?

iDRAC aplica una seguridad sólida para garantizar la identidad de la controladora de dominio a la que se conecta iDRAC. Sin la validación del certificado, un hacker puede suplantar una controladora de dominio y secuestrar la conexión SSL. Si decide confiar en todas las controladoras de dominio en el límite de seguridad sin validación de certificados, puede deshabilitarlo a través de la interfaz web o RACADM.

¿iDRAC soporta el nombre de NetBIOS?

No en esta versión.

¿Por qué se tarda hasta cuatro minutos en iniciar sesión en iDRAC mediante el Single Sign On de Active Directory o el inicio de sesión mediante tarjeta inteligente?

El Single Sign On de Active Directory o tarjeta inteligente normalmente tarda menos de 10 segundos, pero puede tardar hasta cuatro minutos si ha especificado el servidor DNS preferido y el servidor DNS alternativo, y el servidor DNS preferido ha fallado. Cuando un servidor del DNS está inactivo, se esperan tiempos de espera agotados del DNS. La iDRAC inicia sesión con el servidor del DNS alternativo.

Active Directory está configurado para un dominio presente en Windows Server 2008 Active Directory. Un subdominio o dominio secundario está presente para el dominio, el usuario y el grupo están presentes en el mismo dominio secundario y el usuario es miembro de ese grupo. Cuando se intenta iniciar sesión en iDRAC con el usuario presente en el dominio secundario, se produce un error de Single Sign On 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 le permiten administrar el acceso de usuarios y computadoras a recursos compartidos, así como filtrar los ajustes de políticas de grupo.
- Distribución: los grupos de distribución están diseñados para utilizarse solo como listas de distribución de correo electrónico.

Asegúrese siempre de que el tipo de grupo sea Seguridad. No puede usar grupos de distribución para asignar permisos en ningún objeto; sin embargo, úselos para filtrar los ajustes de la política de grupo.

iDRAC Service Module

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.

¿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 iDRAC Service Module 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 `esxcli software vib list|grep -i open` en el host. Se muestra el iDRAC Service Module.

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.

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 54. Ejemplo de una orden de enrutamiento

Destination	Gateway	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 qué parte del sistema operativo se encuentra disponible el registro de LifeCycle replicado?

Para ver los registros de Lifecycle replicados:

Tabla 55. 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**.

Tabla 55. Ubicación de los registros de Lifecycle (continuación)

Sistema operativo	Ubicación
	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 de iDRAC Service Module* disponible en la página Manuales de iDRAC..

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 de iDRAC del DNS registrado:

1. En la interfaz web de la iDRAC, vaya a **Descripción general** > **Configuración de la iDRAC** > **Red**. Aparecerá la página **Red**.
2. En la sección **Ajustes comunes**:
   - Seleccione la opción **Registrar iDRAC en DNS**.
   - En el campo **Nombre del iDRAC de DNS**, ingrese 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.

RACADM

Después de realizar un restablecimiento de iDRAC (mediante el comando racadm racreset), si se emite algún comando, aparecerá el siguiente mensaje. ¿Qué indica esto?

```
ERROR: Unable to connect to RAC at specified IP address
```

El mensaje indica que debe esperar hasta que iDRAC complete el restablecimiento antes de emitir otro comando.

Cuando se utilizan comandos y subcomandos de RACADM, algunos errores no están claros.

Es posible que vea uno o más de los siguientes errores cuando utilice los comandos de RACADM:

- Mensajes de error de RACADM local: problemas como sintaxis, errores tipográficos y nombres incorrectos.
- Mensajes de error de RACADM remoto: problemas como dirección IP incorrecta, nombre de usuario o contraseña incorrectos.

Durante una prueba de ping a iDRAC, si el modo de red se cambia entre los modos Dedicado y Compartido, no hay respuesta de ping.

Borre la tabla ARP del sistema.

El RACADM remoto no se puede conectar a iDRAC desde SUSE Linux Enterprise Server (SLES) 11 SP1.

Asegúrese de que las versiones oficiales de openssl y libopenssl estén instaladas. Ejecute el siguiente comando para instalar los paquetes RPM:

```
rpm -ivh --force < filename >
```

en el que, `filename` es el archivo del paquete rpm de OpenSSL o LibopenSSL.

Por ejemplo:

```
rpm -ivh --force openssl-0.9.8h-30.22.21.1.x86_64.rpm
rpm -ivh --force libopenssl0_9_8-0.9.8h-30.22.21.1.x86_64.rpm
```

¿Por qué el RACADM remoto y los servicios basados en la web no están disponibles después de un cambio de propiedad?

Es posible que los servicios remotos de RACADM y la interfaz basada en la web tarden un poco en estar disponibles después de que se reinicie el servidor web de iDRAC.

El servidor web de iDRAC se restablece cuando:

- La configuración de red o las propiedades de seguridad de red se cambian mediante la interfaz de usuario web de iDRAC.
- Se cambia la propiedad iDRAC.Webserver.HttpsPort, incluido cuando un comando `racadm set -f <config file>` la cambia.
- Se utiliza el comando `racresetcfg`.
- Se restablece iDRAC.
- Se carga un nuevo certificado de servidor SSL.

¿Por qué se muestra un mensaje de error si intenta eliminar una partición después de crearla mediante RACADM local?

Esto ocurre porque la operación de creación de partición está en curso. Sin embargo, la partición se elimina después de un tiempo y se muestra un mensaje que indica que la partición se eliminó. Si no es así, espere hasta que finalice la operación de creación de partición y, a continuación, elimine la partición.

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.

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 normal mediante tarjeta inteligente de Active Directory suele tardar menos de 10 segundos; sin embargo, puede demorar hasta cuatro minutos si especificó el servidor DNS preferido y el servidor DNS alternativo en la página **Red**, y el servidor DNS preferido falló. Cuando un servidor del DNS está inactivo, se esperan tiempos de espera agotados del DNS. La iDRAC inicia sesión con el servidor del DNS alternativo.

PIN incorrecto de la tarjeta inteligente.

Compruebe si la tarjeta inteligente se bloqueó debido a que se intentó ingresar un PIN incorrecto demasiadas veces. En tales casos, comuníquese con el emisor de tarjetas inteligentes en la organización para obtener una nueva.

Autenticación de SNMP

¿Por qué se muestra el mensaje "Acceso remoto: fallo de autenticación SNMP"?

Como parte del proceso de detección, IT Assistant intenta verificar los nombres de comunidad obtener y establecer del dispositivo. En IT Assistant, obtener nombre de comunidad = público y establecer nombre de comunidad = privado. De manera predeterminada, el nombre de comunidad del agente SNMP para el agente de iDRAC es público. Cuando IT Assistant envía una solicitud de establecer, el agente de iDRAC genera el error de autenticación de SNMP, ya que solo acepta solicitudes de comunidad= público.

Para evitar que se generen capturas de autenticación de SNMP, ingrese los nombres de comunidad que acepta el agente. Dado que iDRAC solo permite un nombre de comunidad, ingrese los mismos nombres de comunidad obtener y establecer para la configuración de detección de IT Assistant.

Inicio de sesión único

Error de SSO en Windows Server 2008 R2 x64. ¿Cuáles son los ajustes necesarios para resolver esto?

1. Ejecute **technet.microsoft.com/en-us/library/dd560670(WS.10).aspx** para la controladora de dominio y la política de dominio.
2. Configure las computadoras para utilizar el conjunto de cifrado DES-CBC-MD5.

   NOTA: Estos ajustes pueden afectar a la compatibilidad con los equipos cliente o los servicios y las aplicaciones de su ambiente. La opción Configurar tipos de cifrado permitidos para la política de Kerberos se encuentra en **Configuración de la computadora** > **Ajustes de seguridad** > **Políticas locales** > **Opciones de seguridad**.

3. Asegúrese de que los clientes de dominio tengan el GPO actualizado.
4. En la línea de comandos, escriba `gpupdate /force` y elimine la antigua keytab con el comando `klist purge`.
5. Después de actualizar el GPO, cree la nueva keytab.
6. Cargue la key-tab en iDRAC.

Ahora puede iniciar sesión en iDRAC mediante el SSO.

¿Por qué falla el SSO con 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 habilitar los tipos de cifrado:

1. Inicie sesión como administrador o como usuario con privilegios de administrador.
2. Vaya a **Inicio** y ejecute **gpedit.msc.** Aparecerá la ventana **Editor de políticas del grupo local**.

3. Vaya a **Ajustes de la computadora local** > **Ajustes de Windows** > **Ajustes de seguridad** > **Políticas locales** > **Opciones de seguridad**.
4. Haga clic con el botón secundario en **Seguridad de red: configurar tipos de cifrado permitidos para Kerberos** y seleccione **Propiedades**.
5. Habilite todas las opciones.
6. Haga clic en **Aceptar**. Ahora puede iniciar sesión en iDRAC mediante el SSO.

Realice los siguientes ajustes adicionales para el esquema extendido:

1. En la ventana **Editor de políticas del grupo local**, vaya a **Ajustes de la computadora local** > **Ajustes de Windows** > **Ajustes de seguridad** > **Políticas locales** > **Opciones de seguridad**.
2. Haga clic con el botón secundario en **Seguridad de red: restringir NTLM: tráfico NTLM saliente al servidor remoto** y seleccione **Propiedades**.
3. Seleccione **Permitir todo**, haga clic en **Aceptar** y cierre la ventana **Editor de políticas del grupo local**.
4. Vaya a **Inicio** y ejecute cmd. Aparecerá la ventana de símbolo del sistema.
5. Ejecute el comando `gpupdate /force`. Las políticas de grupo se actualizan. Cierre la ventana del símbolo del sistema.
6. Vaya a **Inicio** y ejecute regedit. Se mostrará la ventana **Editor del registro**.
7. Vaya a **HKEY_LOCAL_MACHINE** > **Sistema** > **CurrentControlSet** > **Control** > **LSA**.
8. En el panel derecho, haga clic con el botón secundario y seleccione **Nuevo** > **Valor DWORD (32-bit)**.
9. Asigne a la nueva llave el nombre **SuppressExtendedProtection**.
10. Haga clic con el botón derecho 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 iDRAC mediante el SSO.

Si activó el SSO para iDRAC y utiliza Internet Explorer a fin de iniciar sesión en iDRAC, el SSO fallará y se le solicitará que ingrese su nombre de usuario y contraseña. ¿Cómo se resuelve esto?

Asegúrese de que la dirección IP de iDRAC aparezca en **Herramientas** > **Opciones de Internet** > **Seguridad** > **Sitios de confianza**. Si no aparece en la lista, el SSO falla y se le solicita que ingrese su nombre de usuario y contraseña. Haga clic en **Cancelar** y continúe.

Dispositivos de almacenamiento

OpenManage Storage Management muestra más dispositivos de almacenamiento que iDRAC, ¿por qué?

iDRAC solo muestra información de los dispositivos soportados en Comprehensive Embedded Management (CEM).

Para JBODs/Insights externos detrás del HBA, el mensaje EEMI para la extracción del conector SAS/IOM se genera con el ID de mensaje EEMI ENC42. Sin embargo, no se generan los mensajes de EEMI ENC41 y ENC1 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** > **Visión general** > **Gabinetes**.
2. Seleccione el gabinete.
3. En las **Propiedades avanzadas**, asegúrese de que el valor de la **Ruta redundante** sea **Presente**.

¿Por qué existe una diferencia en el número de serie impreso en el dispositivo PCIe y en la GUI de iDRAC?

Los dispositivos basados en la clase base de PCIe pueden ser de diferentes tipos y factores de forma. En tales situaciones, es posible que los números de serie del formato del dispositivo no sean los mismos que los de un dispositivo PCIe base. Por ejemplo, formas derivadas de dispositivos PCIe, como unidades NVMe, tarjetas NIC, etc.

Registro de sucesos del sistema

Cuando se utiliza la interfaz web de iDRAC a través de Internet Explorer, ¿por qué SEL no guarda con la opción Guardar como?

Esto se debe a un ajuste del navegador. Para resolver esto:

1. En Internet Explorer, vaya a **Herramientas** > **Opciones de Internet** > **Seguridad** y seleccione la zona en la que está intentando descargar. Por ejemplo, si el dispositivo iDRAC está en la intranet local, seleccione **Intranet local** y haga clic en **Nivel personalizado...**.
2. En la ventana **Ajustes de seguridad**, en **Descargas**, asegúrese de que las siguientes opciones estén habilitadas:
   - Solicitud automática de descargas de archivos (si esta opción está disponible)

- Descarga de archivos

PRECAUCIÓN: Para asegurarse de que la computadora utilizada a fin de acceder a iDRAC sea segura, en Varios, no active la opción Iniciar aplicaciones y archivos no seguros.

Virtual console

¿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 **Aceleración del mouse**, seleccione **Linux**.
- En el menú **Herramientas**, seleccione la opción **Cursor único**.

¿Cómo se sincronizan los punteros del mouse en la ventana Visor de la consola virtual?

Antes de iniciar una sesión de consola virtual, asegúrese de seleccionar el mouse correcto para el sistema operativo.

Asegúrese de seleccionar la opción **Cursor único** en **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 **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.

¿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. Por diseño, el ratón PS/2 utiliza la posición relativa para el puntero del ratón, lo que provoca el retraso en la sincronización. La iDRAC tiene un controlador de ratón USB que permite una posición absoluta y un seguimiento más cercano del puntero del ratón. 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 mouse en USC/Diagnóstico en la pantalla 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 **Modo de mouse** se configura en **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.

¿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 SysRq, 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.

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 o el disco flexible virtual 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 asigna al 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 medios virtuales están conectados como un dispositivo USB compuesto al bus USB del host y comparten un puerto USB común. Siempre que algún medio virtual está conectado al bus USB del host o desconectado de él, todos los dispositivos de medios virtuales 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. 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.

Novedades variadas

Para las CPU de memoria de ancho de banda alto (HBM) en modo HBM, MemoryRollupStatus se muestra como Desconocido.

Para el modo solo HBM, los datos relacionados con la memoria informados en el inventario de hardware, los sensores, la telemetría, etc. no están disponibles. No debe considerar esto como una configuración defectuosa. En el caso de las interfaces que informan acerca de todos los sensores de ranuras DIMM individuales, se muestran con estado Desconocido. De manera similar, el sensor de temperatura máxima de DIMM también se puede seguir mostrando con estado Desconocido.

Cuando se intenta conectar la iDRAC a una red diferente, la iDRAC no obtiene una dirección IP diferente de la nueva subred.

Asegúrese de que el cable de red esté desconectado de la iDRAC durante al menos 5 s.

Después del restablecimiento de la iDRAC, es posible que no se muestren todos los valores en la IU de la 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:

- Situación 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.
- Situación 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 SO son capaces de actualizar el nombre de host en la iDRAC durante el primer inicio del SO.

La conexión de red de iDRAC no funciona.

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 estén activados en el sistema los ajustes de NIC, los de IPv4 e IPv6, y que además esté activada la modalidad estática o DHCP para su red.

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 del 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 del host para el adaptador de red antes de habilitar 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 del 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.

¿Cómo se recuperan un nombre de usuario y una contraseña administrativos de iDRAC?

Debe restaurar iDRAC a sus valores predeterminados. Para obtener más información, consulte Restablecer iDRAC a los valores predeterminados de fábrica.

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 la iDRAC mediante la interfaz web de la iDRAC.

No se puede iniciar sesión en la interfaz web de la iDRAC con el navegador 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. Use `/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.

Configuración del servidor proxy

¿Cómo se configuran los ajustes del servidor proxy en la CLI de RACADM y la API de Redfish?

En RACADM, se deben establecer los siguientes atributos de LC para configurar el servidor proxy:

- LifeCycleController.LCAttributes.UserProxyPassword
- LifeCycleController.LCAttributes.UserProxyPort
- LifeCycleController.LCAttributes.UserProxyServer
- LifeCycleController.LCAttributes.UserProxyType
- LifeCycleController.LCAttributes.UserProxyUserName

Para obtener más información sobre cómo ejecutar estos comandos, consulte la **Guía de CLI de Integrated Dell Remote Access Controller**.

Cuando se utiliza HTTP con un proxy, la conexión entre iDRAC y el proxy no es tan segura como la conexión entre iDRAC y el servidor HTTPS. `UserProxyServer` es un atributo importante. Si no se establece, no se pueden utilizar los otros atributos. El beneficio de usar RACADM y la API de Redfish es que no es necesario proporcionar la contraseña cada vez que utiliza el servidor proxy.

En la API de Redfish, realice una operación de parches mediante el URI `/redfish/v1/Managers/<Manager-ID>/Oem/Dell/DellAttributes/<Dell-attributes-ID>` para configurar el servidor proxy.

¿Cómo se configuran los ajustes del servidor proxy en la IU de iDRAC?

En la UI de iDRAC, puede actualizar la configuración de proxy en todas las páginas donde se requiere el servidor proxy. Incluso si estableció la configuración del proxy mediante RACADM y la API de Redfish, aún puede actualizar la configuración del proxy en la UI de iDRAC. Para configurar los ajustes de proxy en la página **Actualización del sistema**:

1. Vaya a **Mantenimiento** > **Actualización del sistema** > **Actualización manual**.
2. En **Actualización manual**, seleccione **HTTPS** en **Tipo de ubicación**.
3. Seleccione **Habilitado** en **Habilitar servidor proxy**.
4. Ingrese el **Servidor**, el **Puerto**, el **Nombre de usuario** y la **Contraseña**.
5. Seleccione el **Tipo** y haga clic en **Guardar configuración de proxy como predeterminada**.

NOTA: Puede configurar los ajustes de proxy en cualquiera de las páginas, como **Exportar registro de Lifecycle**, **Actualización automática**, **Ajustes de recopilación de SupportAssist**, **Importación del perfil de configuración del servidor** y **Exportación del perfil de configuración del servidor**.

NOTA: De manera predeterminada, la opción **Activar configuración de proxy** en la IU de iDRAC está desactivada. Se restablecerá a un estado deshabilitado después de cada uso. Para obtener más información, consulte **Ayuda en línea de Integrated Dell Remote Access Controller o iDRAC**.

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 Página Soporte de Dell.

30

Situaciones de casos de uso

Esta sección lo ayuda a navegar a secciones específicas de la guía para realizar situaciones de casos de uso típicos.

Temas:

Solución de problemas de un sistema administrado inaccesible

Después de recibir alertas de OpenManage Essentials, Dell Management Console o un recopilador de capturas local, no se puede acceder a cinco servidores en un centro de datos con problemas como el sistema operativo o el servidor bloqueados. Es necesario identificar la causa para solucionar el problema y poner en funcionamiento el servidor mediante iDRAC.

Antes de solucionar el problema del sistema inaccesible, asegúrese de que se cumplen los siguientes requisitos:

- Habilite la pantalla de último bloqueo del sistema
- Las alertas están habilitadas en iDRAC

Para identificar la causa, compruebe lo siguiente en la interfaz web de iDRAC y restablezca la conexión con el sistema:

- Estado del LED del servidor: amarillo fijo o intermitente.
- La imagen del sistema operativo se ve en la consola virtual. Si puede ver la imagen, restablezca el sistema (arranque en caliente) y vuelva a iniciar sesión. Si puede iniciar sesión, el problema se solucionó.
- Pantalla de último bloqueo.
- Video de captura de arranque.
- Video de captura de bloqueo.
- Estado del servidor: iconos de **X** rojas para los componentes del sistema con problemas.
- Estado del arreglo de almacenamiento: posible arreglo offline o fallido
- Registro de ciclo de vida útil para eventos críticos relacionados con el hardware y firmware del sistema y las entradas de registro que se registraron en el momento del bloqueo del sistema.
- Genere un informe de soporte técnico y ver los datos recopilados.
- Utilice las características de monitoreo proporcionadas por iDRAC Service Module

Obtención de información del sistema y evaluación del estado del sistema

Para obtener información del sistema y evaluar su estado:

- En la interfaz web de iDRAC, vaya a **Visión general** > **Resumen** para ver la información del sistema y acceder a diversos enlaces en esta página para evaluar el estado del sistema.
- Si iDRAC Service Module está instalado, se muestra la información del host del sistema operativo.

Configuración de alertas y 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 la alerta de prueba.

Visualización y exportación del registro de eventos del sistema y del registro de ciclo de vida útil

Para ver y exportar el registro de ciclo de vida útil y el registro de eventos del sistema (SEL):

1. En la interfaz web de la iDRAC, vaya a **Mantenimiento** > **Registro de eventos del sistema** para ver SEL y **Registro de ciclo de vida útil** a fin de visualizar el registro de ciclo de vida útil.

   NOTA: El SEL también se registra en el registro de ciclo de vida útil. Uso de las opciones de filtrado para ver el SEL.

2. Exporte el registro de SEL o ciclo de vida útil en formato XML a una ubicación externa (estación de administración, USB, recurso compartido de red, etc.). Como alternativa, puede habilitar el registro del sistema remoto, de modo que todos los registros escritos en el registro de ciclo de vida útil también se escriban simultáneamente en los servidores remotos configurados.
3. Si utiliza iDRAC Service Module, exporte el registro de ciclo de vida útil 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
- CLI de RACADM
- Dell Update Package (DUP)
- Lifecycle Controller
- Dell Remote Access Configuration Tool (DRACT)

Realización de un apagado ordenado

Para iniciar un apagado ordenado, el software desactiva el servidor, lo que permite que el sistema operativo cierre los procesos de manera segura. También apaga las ranuras PCIe. Como resultado, los adaptadores en las ranuras PCIe no responden a los comandos de control de NC-SI.

Si los comandos no responden, el módulo NIC-CEM trata a los adaptadores como sin capacidad de respuesta y registra los registros de Lifecycle Controller (LCLOG) de HWC8607 para indicar que se perdió la comunicación con los adaptadores.

Para realizar un apagado ordenado, en la interfaz web de iDRAC, vaya a una de las siguientes ubicaciones:

- En **Panel**, seleccione **Apagado ordenado** y haga clic en **Aplicar**.

NOTA: Después de que la solicitud se envía al host, este debe atenderla y ejecutarla. La ejecución correcta de un apagado ordenado depende del estado del host.

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 administrador local predeterminada o crear una nueva cuenta de usuario administrador. Para modificar la cuenta de usuario de administrador local, consulte Modificación de los ajustes de la cuenta de administrador local.

Para crear una nueva cuenta de administrador, consulte las siguientes secciones:

- Configuración de usuarios locales
- Configuración de usuarios de Active Directory
- Configuración de usuarios LDAP genéricos

Inicio de la consola remota de servidores y montaje de una unidad USB

Para iniciar la consola remota y montar una unidad USB:

1. Conecte una unidad flash USB (con la imagen requerida) a la estación de administración.
2. Utilice el siguiente método para iniciar la consola virtual a través de la interfaz web de iDRAC:
   - Vaya a **Panel** > **Consola virtual** y haga clic en **Iniciar la consola virtual**.

   Aparecerá el **Visor de consola virtual**.
3. En el menú **Archivo**, haga clic en **Medios virtuales** > **Iniciar medios virtuales**.
4. Haga clic en **Agregar imagen** y seleccione la imagen que se encuentra en la unidad flash USB.
   La imagen se agregará a la lista de unidades disponibles.
5. Seleccione la unidad que desea asignar. La imagen en la unidad flash USB se asigna al sistema administrado.

Instalación de un sistema operativo de bajo nivel mediante medios virtuales conectados y recursos compartidos de archivos remotos

Consulte la sección Implementación del sistema operativo mediante recursos compartidos de archivos remotos.

Administración de la densidad del rack

Antes de instalar servidores adicionales en un rack, debe determinar la capacidad restante en el rack.

Para evaluar la capacidad de un rack a fin de agregar servidores adicionales:

1. Vea los datos de consumo de energía actual y los datos históricos de consumo de energía de los servidores.
2. Según los datos, la infraestructura de alimentación y las limitaciones del sistema de enfriamiento, habilite la política de límite de alimentación y establezca los valores de límite de alimentación.

   NOTA: Se recomienda establecer un límite cerca del pico y, a continuación, utilizar ese nivel limitado a fin de determinar cuánta capacidad queda en el rack para agregar más servidores.

Instalación de una nueva licencia electrónica

Consulte Operaciones de licencia para obtener más información.

Aplicación de los ajustes de configuración de identidad de I/O para varias tarjetas de red en un solo reinicio del sistema host

Si tiene varias tarjetas de red en un servidor que forma parte de un entorno de red de área de almacenamiento (SAN) y desea aplicar diferentes direcciones virtuales, iniciadores y ajustes de configuración de objetivo a esas tarjetas, utilice la función de optimización de identidad de I/O a fin de reducir el tiempo necesario para configurar los ajustes. Para hacerlo, realice estos pasos:

1. Asegúrese de que el BIOS, iDRAC y las tarjetas de red estén actualizados a la versión de firmware más reciente.
2. Habilite la optimización de identidad de I/O.
3. Exporte el archivo de perfil de configuración del servidor (SCP) desde iDRAC.
4. Edite la configuración de optimización de la identidad de I/O en el archivo SCP.
5. Importe el archivo SCP a iDRAC.

Índice