Lenovo

Guía del usuario de XClarity Controller con Intel Xeon SP (1.ª, 2.ª Generación)

Nota: Antes de utilizar esta información, lea la información general incluida en el apartado Apéndice B “Avisos” en la página 217.

Décimoquinta edición (Mayo 2021)

Contenido

Capítulo 1. Introducción

El Lenovo XClarity Controller (XCC) es la siguiente generación de controlador de gestión, la cual viene a sustituir el controlador de gestión de placa base (BMC) para los servidores Lenovo ThinkSystem.

Es la próxima generación del procesador de servicio del Integrated Management Module II (IMM2) que consolida la funcionalidad del procesador de servicio, súper E/S, controlador de video y capacidades de presencia remota en un solo chip en la placa del sistema del servidor. Proporciona las siguientes funciones:

- Opción de una conexión Ethernet dedicada o compartida para la gestión de sistemas
- Soporte para HTML5
- Soporte para el acceso a través de XClarity Mobile
- XClarity Provisioning Manager
- Configuración remota utilizando XClarity Essentials o XClarity Controller CLI.
- Capacidad para que aplicaciones y herramientas tengan acceso al XClarity Controller local o remotamente
- Capacidades avanzadas de la presencia remota.
- Soporte para REST API (esquema Redfish) para servicios web adicionales y aplicaciones de software.

  Nota: XClarity Controller admite en la actualidad Redfish Scalable Platforms Management API especificación 1.0.2 y esquema 2016.2

Notas:

- En la interfaz web de XClarity Controller, se utiliza BMC para hacer referencia al XCC.
- Es posible que no haya un puerto de red de gestión de sistemas dedicado en algunos servidores ThinkSystem; para estos casos, solo se puede acceder al XClarity Controller mediante un puerto de red compartido con el sistema operativo del servidor.
- Para servidores Flex, el Chassis Management Module (CMM) es el módulo de gestión primario para las funciones de gestión. El acceso al XClarity Controller está disponible a través del puerto de red en el CMM.

Este documento explica cómo utilizar las funciones del XClarity Controller en un servidor ThinkSystem. XClarity Controller trabaja con el XClarity Provisioning Manager y UEFI para entregar capacidades de gestión de sistemas a los servidores ThinkSystem.

Para revisar si existen actualizaciones de firmware, lleve a cabo los pasos siguientes.

Nota: La primera vez que accede a Support Portal, debe elegir la categoría del producto, la familia de productos y los números de modelo para el servidor. La próxima vez que accede a Support Portal, los productos que seleccionó inicialmente se cargan previamente en el sitio web y solo se muestran los enlaces para sus productos. Para cambiar o añadir un producto a la lista, pulse el enlace **Gestionar mis listas de productos**. El sitio web se modifica periódicamente. Es posible que los procedimientos para localizar el firmware y la documentación sean ligeramente distintos de los que se describen en este documento.

1. Visite la página http://datacentersupport.lenovo.com.
2. Debajo de **Support (Soporte)**, seleccione **Data Center (Centro de datos)**.
3. Cuando se cargue el contenido, seleccione **Servers (Servidores)**.
4. En **Select Series (Seleccionar serie)**, primero seleccione la serie de hardware del servidor específico, después en **Select SubSeries (Seleccionar las subseries)**, seleccione las subseries del producto del

servidor específico y, finalmente, en **Select Machine Type (Seleccionar tipo de equipo)** seleccione el tipo de equipo específico.

Características de nivel estándar, avanzado y empresarial del XClarity Controller

Se ofrecen funciones de niveles estándar, avanzado y empresarial de XClarity Controller. Consulte la documentación de su servidor para obtener más información acerca del nivel de funcionalidad del XClarity Controller instalada en el servidor. Todos los niveles proporcionan lo siguiente:

- Acceso remoto y gestión del servidor de tiempo completo
- Gestión remota independiente del estado del servidor gestionado
- Control Remoto de hardware y de sistemas operativos

Nota: Algunas características pueden no aplicar a los servidores Flex System.

A continuación se muestra una lista de las características de nivel estándar del XClarity Controller:

Características de nivel estándar del XClarity Controller

A continuación se muestra una lista de las características de nivel estándar del XClarity Controller:

Interfaces de gestión estándar de la industria

- Interfaz IPMI 2.0
- Redfish
- CIM-XML
- DCMI 1.5
- SNMPv3
- SNMPv1 (solo interrupciones) requiere actualizaciones de firmware mínimas de v2.10 o v2.12 XCC según el tipo de servidor. Consulte el archivo de cambio de actualización de firmware XCC para obtener más detalles.

Otras interfaces de gestión

- Web
- CLI heredado
- Panel frontal USB: panel del operador virtual mediante dispositivo móvil

Control de encendido/reinicio

- Encender
- Apagado de software/brusco
- Control de alimentación programado
- Restablecer sistema
- Control de orden de arranque

Registros de sucesos

- IPMI SEL
- Registro legible humano
- Registro de auditoría

Control de medio ambiente

- Supervisión de agente libre
- Supervisión de sensor
- Control de ventilador
- Control de LED
- Errores de conjunto de chip (Caterr, IERR, etc.)
- Indicación del estado del sistema
- Supervisión de rendimiento OOB para adaptadores de E/S
- Visualizar y exportar inventario

RAS

- NMI virtual
- Recuperación automática de firmware
- Promoción automatizada de firmware de copia de seguridad
- Proceso de vigilancia de POST
- Vigilancia de cargador de SO
- Captura de pantalla azul (error de SO)
- Herramientas de diagnóstico integradas

Configuración de red

- IPv4
- IPv6
- Dirección IP, máscara de subred, puerta de enlace
- Modos de asignación de dirección IP
- Nombre de host
- Dirección MAC programable
- Selección MAC doble (si es admitida por el hardware del servidor)
- Reasignaciones de puerto de red
- Etiquetado VLAN

Protocolos de red

- DHCP
- DNS
- DDNS
- HTTP/HTTPS
- SNMPv3
- SNMPv1 (solo interrupciones)
- SSL
- SSH
- SMTP
- Cliente LDAP
- NTP

- SLP
- SSDP

Alertas

- Interrupciones PET
- Indicación de CIM
- Trampas SNMP
- Correo electrónico
- Sucesos de Redfish

Redirección serie

- IPMI SOL
- Configuración del puerto serie

Seguridad

- Raíz de núcleo del XClarity Controller de confianza para la medida (CRTM)
- Actualizaciones de firmware firmado digitalmente
- Control de acceso basado en roles (RBAC)
- Cuentas de usuarios locales
- Cuentas de usuarios LDAP/AD
- Reversión segura de firmware
- Detección de intrusión del chasis (solo disponible en algunos modelos de servidor)
- Declaración remota XCC de presencia física de TPM UEFI
- Registro de auditoría de cambios de configuración y acciones del servidor
- Autenticación de clave pública (PK)
- Retiro/reasignación del sistema

Presencia remota

- Disco remoto en tarjeta (RDOC): montaje de medio virtual de archivos ISO/IMG remotos mediante CIFS, NFS, HTTP, HTTPS, FTP, SFTP y LOCAL

Gestión de alimentación

- Medidor de alimentación en tiempo real

Gestión de licencia

- Validación y repositorio de clave de activación

Implementación y configuración

- Configuración remota
- Despliegue y herramientas de configuración y paquetes de controladores mediante XClarity Provisioning Manager integrado
- Copia de seguridad y restauración de la configuración

Actualizaciones de firmware

- Actualización de agente libre
- Actualización remota

Características de nivel avanzado del XClarity Controller

A continuación se muestra una lista de las características de nivel avanzado del XClarity Controller:

Todas las características de nivel estándar del XClarity Controller más:

Alertas

- Syslog

Presencia remota

- KVM remoto

Redirección serie

- Redirección serie sobre SSH

Seguridad

- Security Key Lifecycle Manager (SKLM)
- Bloqueo de dirección IP

Gestión de alimentación

- Gráficos de alimentación en tiempo real
- Contadores históricos de alimentación
- Gráficos de temperatura

Implementación y configuración

- Despliegue de SO remoto a través de XClarity Provisioning Manager incorporado mediante la característica de KVM remoto de XClarity Controller

Características de nivel empresarial del XClarity Controller

A continuación se muestra una lista de las características de nivel empresarial del XClarity Controller:

Todas las características de nivel estándar y avanzado del XClarity Controller más:

RAS

- Captura de arranque

Presencia remota

- Control de calidad/ancho de banda
- Colaboración de consola virtual (seis usuarios)
- Charla de consola virtual
- Medio virtual
  - Montaje de archivos ISO/IMG remotos a través de la consola remota
  - Archivo de montaje desde la red: monta un archivo de imagen ISO o IMG desde un servidor de archivo (HTTPS, CIFS, NFS) al host como una unidad de DVD o USB

Gestión de alimentación

- Limitación de alimentación
- Supervisión de rendimiento OOB: métricas de rendimiento del sistema

Implementación y configuración

- Implementación remota mediante Lenovo XClarity Administrator. Al utilizar Lenovo XClarity Administrator para el despliegue del sistema operativo, consulte https://pubs.lenovo.com/lxca/supported_operating_system_images para obtener detalles acerca de los sistemas operativos compatibles.

Actualización de XClarity Controller

Si el servidor se entregó con el nivel estándar o avanzado de la funcionalidad de firmware de XClarity Controller, es posible que pueda actualizar la funcionalidad de XClarity Controller en el servidor. Para obtener más información sobre los niveles disponibles de la actualización y cómo solicitarlos, consulte Capítulo 8 “Gestión de licencia” en la página 93.

Requisitos del navegador web y sistema operativo

Utilice la información en este tema para ver la lista de navegadores admisibles, de suites de cifrado y de sistemas operativos para el servidor.

La interfaz web del XClarity Controller requiere uno de los siguientes navegadores web:

- Chrome 48.0 o superior (55.0 o superior para consola remota)
- Firefox ESR 38.6.0 o superior
- Microsoft Edge
- Safari 9.0.2 o superior (iOS7 o posterior y OS X)

Nota: La compatibilidad con la función de consola remota no está disponible a través del navegador en sistemas operativos de dispositivos móviles.

Los navegadores que aparecen arriba corresponden a los admitidos actualmente por el firmware del XClarity Controller. El firmware del XClarity Controller se puede modificar periódicamente para incluir soporte para otros navegadores.

Dependiendo de la versión de firmware del XClarity Controller, el soporte de navegador web puede variar de los navegadores listados en esta sección. Para ver la lista de navegadores compatibles con el XClarity Controller, pulse la lista de menú **Navegadores admitidos** de la página de inicio de sesión del XClarity Controller.

Para una mayor seguridad, ahora solo son compatibles los cifrados de alto nivel cuando se usa HTTPS. Al usar HTTPS, la combinación del sistema operativo y el navegador de su cliente debe admitir una de las siguientes suites de cifrado:

- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-ECDSA-AES256-SHA
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-ECDSA-AES128-SHA
- ECDHE-RSA-AES256-GCM-SHA384

- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256

La memoria caché del navegador de Internet almacena información sobre las páginas web que se visite para que carguen más rápido en el futuro. Después de una actualización de utilidad flash del firmware del XClarity Controller, es posible que el navegador continúe utilizando la información de la memoria caché en lugar de recuperarlo del XClarity Controller. Después de actualizar el firmware del XClarity Controller es recomendable que borre la memoria caché del navegador para asegurarse de que las páginas web servidas por el XClarity Controller se visualicen correctamente.

Soporte de varios idiomas

Utilice la información en este tema para ver una lista de los idiomas soportados por el XClarity Controller.

De forma predeterminada, el idioma elegido para la interfaz web del XClarity Controller es el inglés. La interfaz es capaz de visualizar varios idiomas. Estos incluyen:

- Francés
- Alemán
- Italiano
- Japonés
- Coreano
- Portugués (Brasil)
- Ruso
- Chino simplificado
- Español (internacional)
- Chino tradicional

Para seleccionar el idioma de su preferencia, pulse la flecha junto a un idioma actualmente seleccionado. Un menú desplegable aparecerá para poder elegir el idioma preferido.

Las cadenas de texto generadas por el firmware del XClarity Controller se muestran en el idioma dictado por el navegador. Si el navegador especifica un idioma distinto de uno de los idiomas traducidos indicados anteriormente, el texto se muestra en inglés. Además, cualquier cadena de texto que se muestra por el firmware del XClarity Controller, pero que el XClarity Controller no genera (por ejemplo mensajes generados por UEFI, adaptadores PCIe, etc.) se visualizan en inglés.

La entrada del texto específico de un idioma distinto del inglés, como el **Mensaje de advertencia de intrusión** no se admite actualmente. Solo se admite texto escrito en inglés.

Introducción de MIB

Utilice la información de este tema para acceder a la Base de información de gestión.

Las MIB de SNMP pueden descargarse desde el https://support.lenovo.com/ (Buscar por tipo de equipo en el portal). Incluye las siguientes cuatro MIB.

- La **MIB de SMI** describe la Estructura de la información de gestión para el Grupo de centros de datos de Lenovo.
- La **MIB de producto** describe el identificador de objeto para los productos de Lenovo.

- La **MIB de XCC** proporciona la información de inventario y de supervisión para Lenovo XClarity Controller.
- La **MIB de alertas de XCC** define las interrupciones para las condiciones de alerta detectadas por Lenovo XClarity Controller.

Nota: El orden de importación para las cuatro MIB es **MIB de SMi** → **MIB de producto** → **MIB de XCC** → **MIB de alerta de XCC**.

Avisos utilizados en este documento

Utilice esta información para comprender los avisos que se utilizan en este documento.

En este documento se utilizan los siguientes avisos:

- **Nota:** estos avisos proporcionan consejos importantes, ayuda o consejos.
- **Importante:** estos avisos proporcionan información o consejos que pueden ayudarle a evitar situaciones inconvenientes o problemáticas.
- **Atención:** estos avisos indican daños potenciales a programas, dispositivos o datos. Inmediatamente antes de la indicación o situación en la que se puede producir el daño se coloca un aviso de atención.

Capítulo 2. Inicio y uso de la interfaz web de XClarity Controller

Este tema describe los procedimientos de inicio de sesión y las acciones que puede realizar desde la interfaz web del XClarity Controller.

El XClarity Controller combina funciones de procesador de servicios, controlador de video y la función de presencia remota en un único chip. Para acceder a XClarity Controller de forma remota mediante la interfaz web de XClarity Controller, primero debe iniciar sesión. Este capítulo describe los procedimientos de inicio de sesión y las acciones que puede realizar desde la interfaz web del XClarity Controller.

Acceder a la interfaz web de XClarity Controller

La información de este tema explica cómo acceder a la interfaz web del XClarity Controller.

XClarity Controller admite el direccionamiento IPv4 del protocolo de configuración de host dinámico y estático (DHCP). La dirección estática IPv4 predeterminada asignada al XClarity Controller es 192.168.70.125. XClarity Controller está configurado inicialmente para intentar obtener una dirección de un servidor DHCP y, si es posible, utilizar la dirección estática IPv4.

XClarity Controller también admite el direccionamiento IPv6, pero no tiene una dirección IP de IPv6 estática fija de manera predeterminada. Para el acceso inicial al XClarity Controller en un entorno IPv6, puede utilizar la dirección IP IPv4 o la dirección de enlace local IPv6. XClarity Controller genera una dirección de vínculo local IPv6 única, utilizando la dirección MAC de IEEE 802 insertando dos octetos, con los valores hexadecimales de 0xFF y de 0xFE en el centro de MAC de 48 bits, tal como se describe en RFC4291 y al invertir el 2do bit desde la derecha del primer octeto de la dirección MAC. Por ejemplo, si la dirección MAC es 08-94-ef-2f-28-af, la dirección de vínculo local será:
`fe80::0a94:efff:fe2f:28af`

Cuando accede al XClarity Controller, las siguientes condiciones de IPv6 se configuran de forma predeterminada:

- Se habilita la configuración automática de la dirección IPv6.
- Se deshabilita la configuración de la dirección IP estática de IPv6.
- Se habilita DHCPv6.
- Se habilita la configuración automática sin estado

XClarity Controller proporciona la opción de utilizar una conexión de red de gestión de sistemas **dedicada** (si procede) o una que es **compartida** con el servidor. La conexión predeterminada para los servidores montados en bastidor y servidores de torre es utilizar el conector de la red de gestión de sistemas **dedicado**.

La conexión de red de gestión de sistemas dedicada en la mayoría de los servidores se proporciona mediante un controlador separado de la interfaz de red de 1 Gbit. Sin embargo, en algunos sistemas la conexión de red de gestión de sistemas se puede proporcionar utilizando la interfaz de banda lateral del controlador de red (NCSI) a uno de los puertos de red de un controlador de interfaz de red de varios puertos. En este caso, la conexión de red de gestión de sistemas se limita a la velocidad de 10/100 de la interfaz de banda lateral. Para obtener información y conocer las limitaciones de la implementación del puerto de gestión en el sistema, consulte la documentación del sistema.

Nota: Un puerto de red **dedicado** de gestión de sistemas no puede estar disponible en el servidor. Si el hardware no tiene un puerto de red **dedicado**, la configuración **compartida** es la única de XClarity Controller disponible.

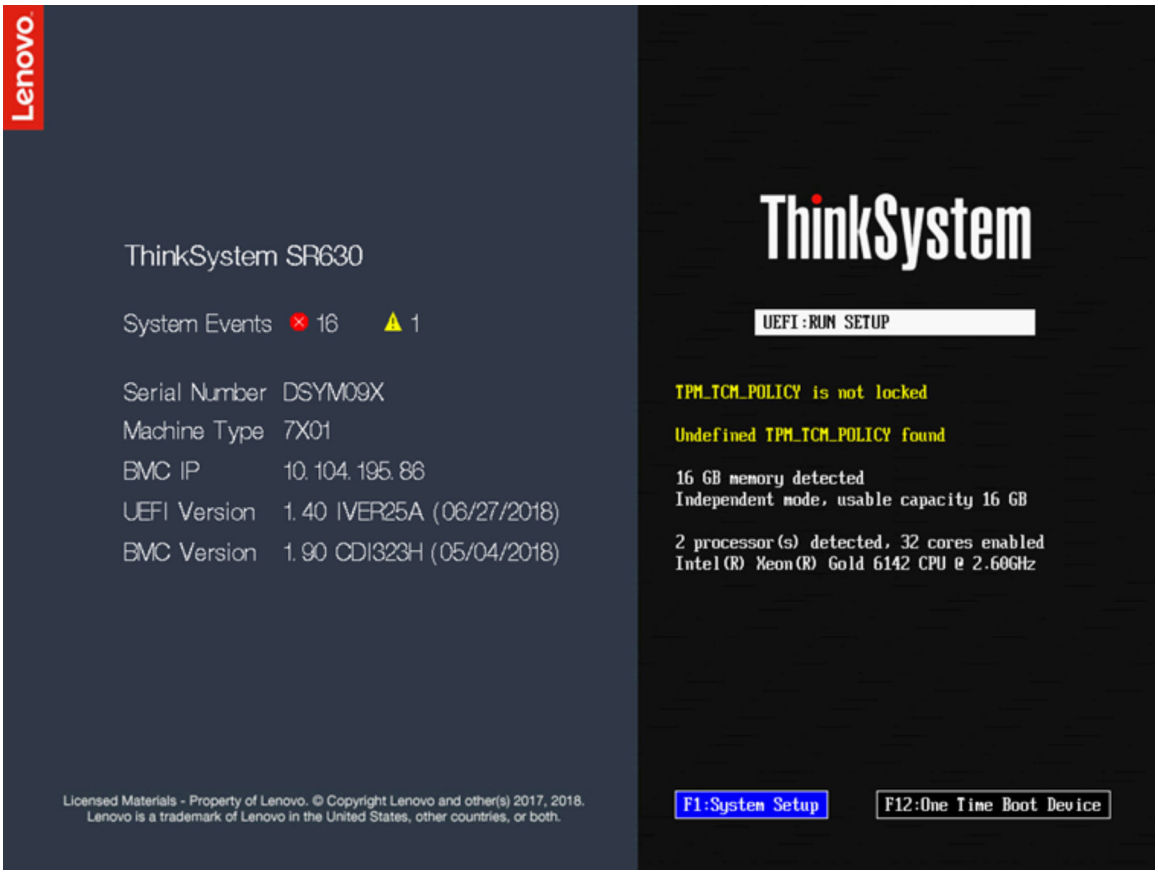
Configuración de conexión de red del XClarity Controller a través del XClarity Provisioning Manager

Use la información de este tema para configurar una conexión de red del XClarity Controller a través del XClarity Provisioning Manager.

Después de que se inicie el servidor, puede utilizar el XClarity Provisioning Manager para configurar la conexión de red del XClarity Controller. El servidor con XClarity Controller debe estar conectado a un servidor DHCP, o la red del servidor debe configurarse para utilizar la dirección IP estática del XClarity Controller. Para configurar la conexión de red del XClarity Controller con el programa de Setup Utility, complete los pasos siguientes:

Paso 1. Encienda el servidor. Se visualiza la pantalla de bienvenida a ThinkSystem.

Nota: Puede tardar hasta 40 segundos después de que el servidor se conecte a la alimentación de CA para que el botón de control de encendido pase a estar activo.



Paso 2. Cuando aparezca el mensaje `<F1> System Setup`, presione F1. Si ha establecido una contraseña de encendido y una contraseña de administrador, debe especificar la contraseña de administrador para acceder a XClarity Provisioning Manager.

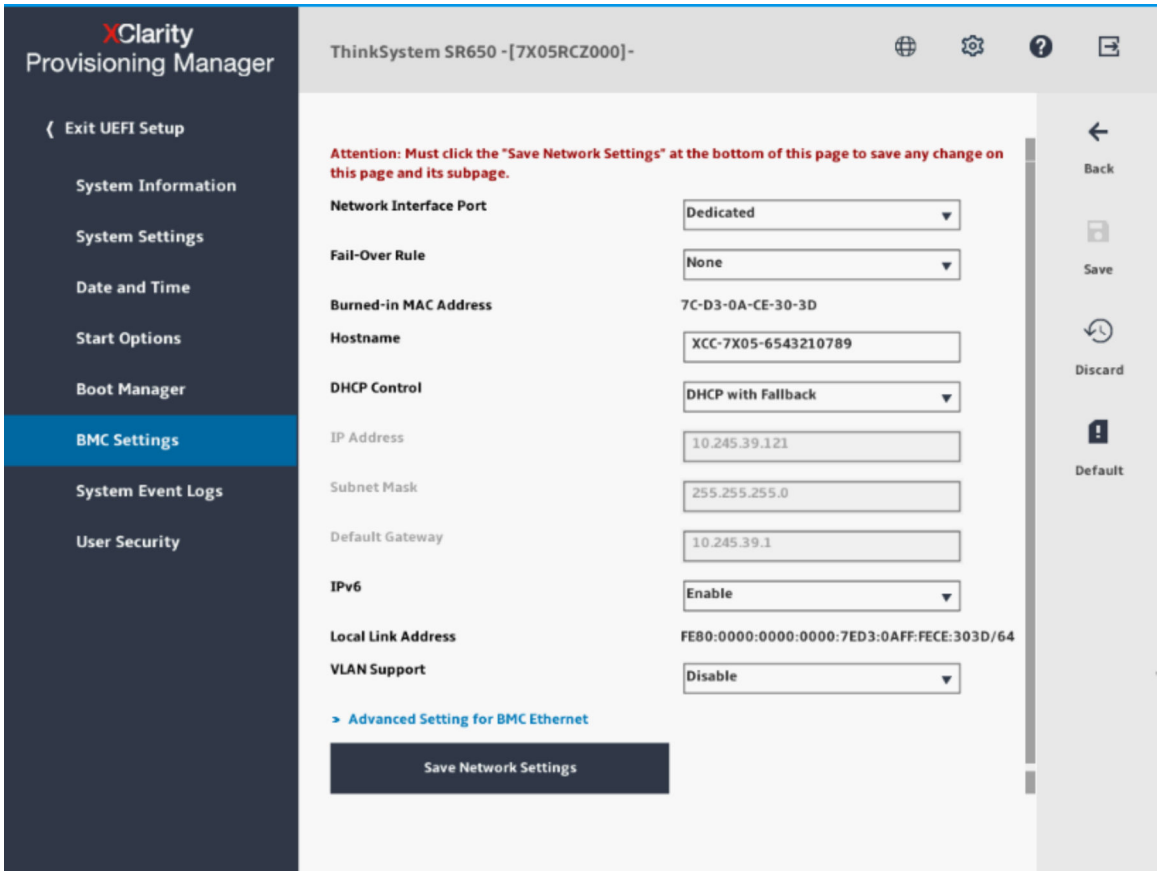
Paso 3. Desde el menú principal de XClarity Provisioning Manager, seleccione **UEFI Setup**.

Paso 4. En la siguiente pantalla, seleccione **BMC Settings**; a continuación, haga clic en **Network Settings**.

Paso 5. Existen tres opciones de conexión de red del XClarity Controller en el campo **DHCP Control**:

- IP estática
- DHCP habilitado

- DHCP con regreso



Paso 6. Seleccione una de las opciones de conexión de red.

Paso 7. Si elige utilizar una dirección IP estática, debe especificar la dirección IP, la máscara de subred y la puerta de enlace predeterminada.

Paso 8. También puede utilizar el Lenovo XClarity Controller Manager para seleccionar una conexión de red dedicada (si el servidor tiene un puerto de red dedicado) o una conexión de red compartida de XClarity Controller.

Notas:

- Un puerto de red dedicado de gestión de sistemas no puede estar disponible en el servidor. Si el hardware no tiene un puerto de red dedicado, la configuración **compartida** es la única de XClarity Controller disponible. En la pantalla **Network Configuration**, seleccione **Dedicated** (si procede) o **Shared** en el campo **Network Interface Port**.
- Para encontrar las ubicaciones de los conectores Ethernet en el servidor que utiliza el XClarity Controller, consulte la documentación incluida con el servidor.

Paso 9. Pulse **Guardar**.

Paso 10. Salga del XClarity Provisioning Manager.

Notas:

- Debe esperar aproximadamente 1 minuto para que los cambios surtan efecto antes de que el firmware de servidor funcione de nuevo.
- También puede configurar la conexión de red del XClarity Controller a través de la interfaz web o la interfaz de la línea de comandos (CLI) del XClarity Controller. En la interfaz web del XClarity Controller, las

conexiones de red se pueden configurar al pulsar **Configuración del BMC** en el panel de navegación izquierdo y luego seleccionar **Red**. En la CLI de XClarity Controller, las conexiones de red se configuran con varios comandos que dependan de la configuración de la instalación.

Inicio de sesión en el Xclarity Controller

Use la información de este tema para acceder al XClarity Controller mediante su interfaz web.

Importante: El XClarity Controller se establece inicialmente con un nombre de usuario de `USERID` y una contraseña de `PASSWORD` (con un cero, no con la letra O). Esta configuración de usuario predeterminada tiene acceso de supervisor. Con el fin de obtener una seguridad ampliada, cambie este nombre de usuario y esta contraseña durante la configuración inicial. Después de realizar el cambio, no puede volver a establecer `PASSWORD` como la contraseña de inicio de sesión.

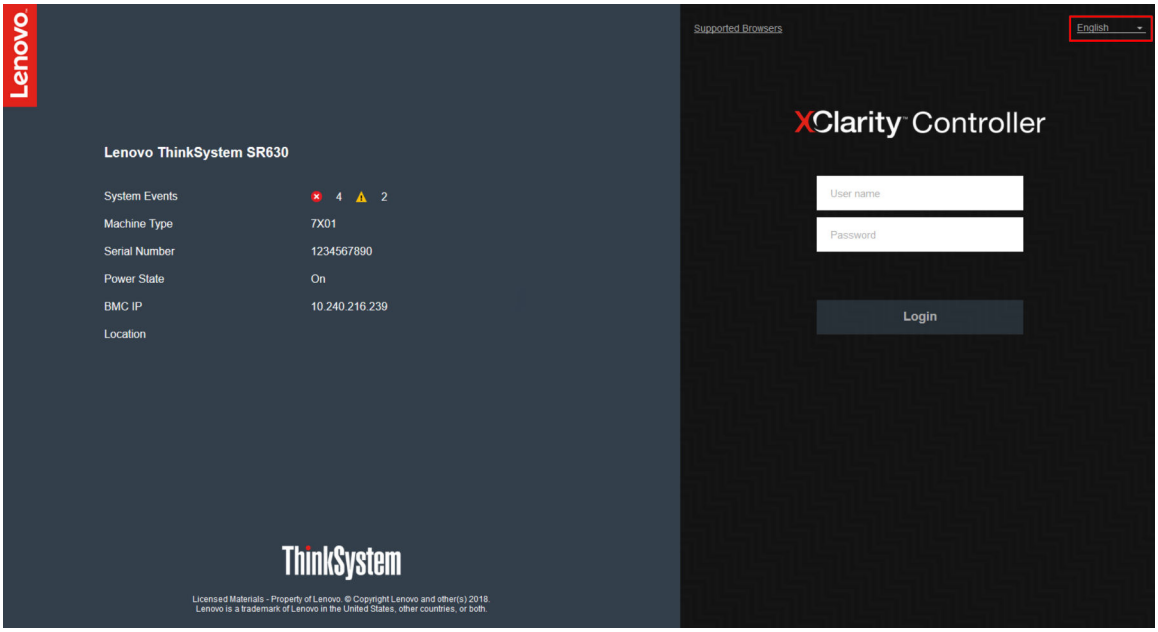
Nota: En Flex System, las cuentas de usuario del XClarity Controller se pueden gestionar mediante Flex System Chassis Management Module (CMM) y pueden ser diferentes que la combinación de USERID/ PASSW0RD descrita arriba.

Para acceder al XClarity Controller mediante su interfaz web, realice los siguientes pasos:

Paso 1. Abrir un navegador web. En el cuadro dirección o URL, escriba la dirección IP o el nombre de host del XClarity Controller con el que desea conectar.

Paso 2. Seleccione el idioma deseado en la lista desplegable de idioma.

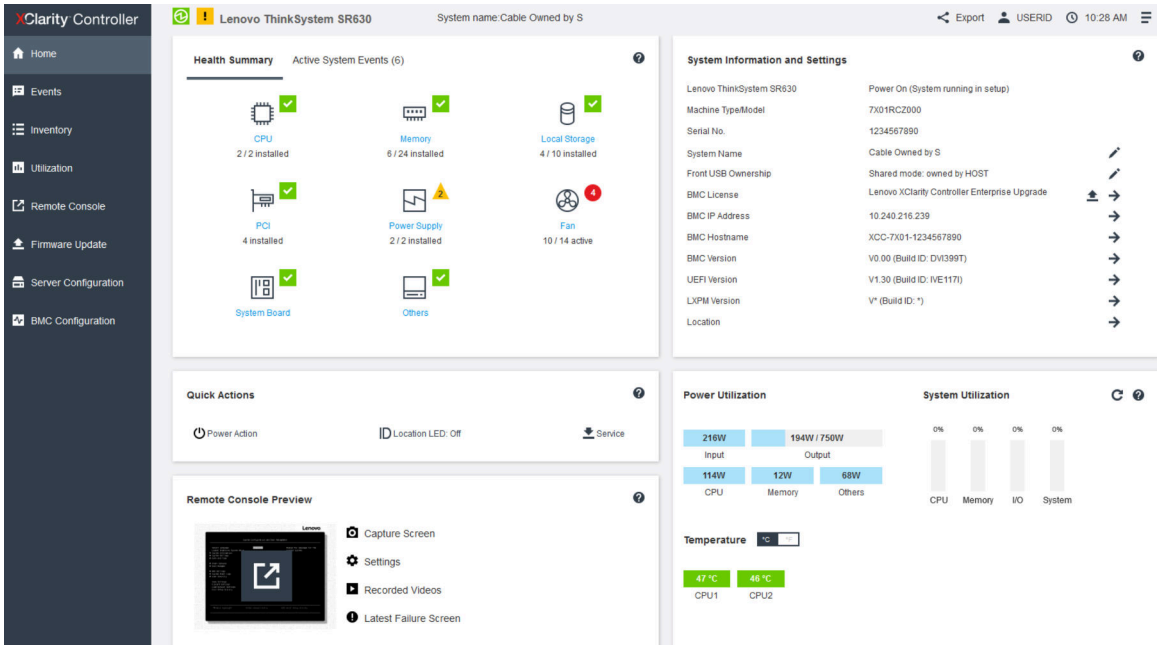
La siguiente ilustración muestra la ventana Inicio de sesión.



Paso 3. Escriba el nombre de usuario y la contraseña en la ventana de inicio de sesión del XClarity Controller. Si está utilizando XClarity Controller por primera vez, puede obtener el nombre de usuario y la contraseña del administrador del sistema. Todos los intentos de inicio de sesión quedan documentados en el registro de sucesos. En función de cómo el administrador del sistema ha configurado el Id. de usuario, es posible que necesite introducir una nueva contraseña después de iniciar sesión.

Paso 4. Presione **Iniciar sesión** para iniciar la sesión. El navegador abre la página inicial del XClarity Controller, tal como se muestra en la ilustración siguiente. La página de inicio muestra información

sobre el sistema que el XClarity Controller gestiona, más la indicación de los iconos de más que indican cuántos errores críticos 1 y cuántas advertencias 1 están actualmente en el sistema.



La página Inicio esencialmente se divide en dos secciones. La primera sección es el panel izquierdo de navegación, que es un conjunto de temas que permiten realizar las acciones siguientes:

- Supervisar el estado del servidor
- Configurar el servidor
- Configurar el XClarity Controller o BMC
- Actualización del firmware

La segunda sección es la información gráfica proporcionada a la derecha del panel de navegación. El formato modular le otorga una vista rápida del estado del servidor y de algunas acciones rápidas que se pueden realizar.

Descripción de las funciones de XClarity Controller en la interfaz web

La siguiente es una tabla donde se describen las funciones de XClarity Controller en el panel izquierdo de navegación.

Nota: Al navegar la interfaz web, también puede pulsar el icono de signo de interrogación para obtener ayuda en línea.

Tabla 1. Funciones de XClarity Controller

Tabla de tres columnas que contiene las descripciones de las acciones que puede realizar en la interfaz web de XClarity Controller.

Tab	Selección	Descripción
Inicio	Resumen de estado/sucesos activos del sistema	Muestra el estado actual de los componentes de hardware principales del sistema.

Tabla 1. Funciones de XClarity Controller (continuación)

Tab	Selección	Descripción
	Información del sistema y configuración	Proporciona un resumen de la información común del sistema.
	Acciones rápidas	Proporciona un enlace rápido para controlar el LED de alimentación del servidor y la ubicación y un botón de descargar datos de servicio.
	Utilización de alimentación/uso del sistema/temperatura	Proporciona una visión general rápida de utilización actual de alimentación, el uso del sistema y la temperatura general del servidor.
	Vista previa de consola remota	Controla el servidor en el nivel de sistema operativo. Puede ver y utilizar la consola del servidor desde su equipo. La sección de consola remota en la página inicial del XClarity Controller muestra una imagen un botón de arranque. La barra de herramientas derecha incluye las acciones rápidas siguientes: • Pantalla de captura • Valores • Videos grabados • Última pantalla de error
Sucesos	Registro de sucesos	Proporciona un listado histórico de todos los sucesos de hardware y de gestión.
	Registro de auditoría	Proporciona un historial de las acciones de los usuarios, tales como iniciar sesión en Lenovo XClarity Controller, crear un usuario nuevo o cambiar la contraseña de un usuario. Puede usar el registro de auditoría para efectuar el seguimiento y la documentación de la autenticación y de los controles en sistemas de TI.
	Historial de mantenimiento	Muestra todo el historial de actualización de firmware, la configuración y sustitución de hardware.
	Destinatarios de alerta	Gestionar a quién se le notificarán los sucesos del sistema. Le permite configurar a cada receptor y gestionar valores que se aplican a todos los destinatarios de sucesos. Puede también generar un suceso de prueba para verificar la configuración de las notificaciones.
Inventario		Muestra todos los componentes del sistema, junto con su estado e información clave. Puede pulsar un dispositivo para mostrar información adicional. **Nota:** Consulte la interfaz web de SMM2 para obtener más detalles sobre el estado de alimentación de la solución.
Utilización		Muestra la temperatura del ambiente o del componente, la utilización de alimentación, los niveles de voltaje, la utilización de subsistemas del sistema e información de la velocidad del ventilador del servidor y sus componentes en formatos gráficos o tabulares.
Almacenamiento	Detalle	Muestra la estructura física de los dispositivos de almacenamiento y la configuración de almacenamiento.
	Configuración de RAID	Vea o modifique la configuración RAID actual, incluyendo información de los discos virtuales y dispositivos de almacenamiento físicos.

Tabla 1. Funciones de XClarity Controller (continuación)

Tab	Selección	Descripción
Puerto remoto		Proporciona acceso a la funcionalidad de la consola remota. Puede utilizar la característica de medios virtual para montar los archivos de imágenes ISO o IMG que están ubicados en el sistema o en una ubicación de red al que el BMC puede acceder utilizando CIFS, NFS, HTTPS o SFTP. El disco montado aparece como una unidad de disco USB que está conectada al servidor.
Actualización de firmware		• Muestra los niveles de firmware. • Actualiza el firmware de XClarity Controller y el firmware del servidor.
Configuración del servidor	Adaptadores	Muestra la información de adaptadores de red instalados y los valores que se pueden configurar mediante el XClarity Controller.
	Opciones de arranque	• Seleccione el dispositivo de arranque para arranque único durante el siguiente reinicio del servidor. • Cambie el modo de arranque y la configuración del orden de arranque.
	Política de alimentación	• Configure la redundancia de alimentación durante el suceso de un error de fuente de alimentación. • Configure la política de limitación de alimentación. • Configure la política de restauración de alimentación. **Nota:** Consulte la interfaz web de SMM2 para obtener más detalles sobre el estado de alimentación de la solución.
	Propiedades del servidor	• Supervise las diferentes propiedades, condiciones de estado y valores de su servidor. • Gestione los tiempos de espera excedidos del servidor para detectar y para recuperarse de cuelgue del servidor. • Cree el mensaje de advertencia de intrusión. Un mensaje de advertencia de intrusión es un mensaje que puede crear para que los usuarios vean cuando se inicia sesión en el XClarity Controller.
Configuración BMC	Copia de seguridad y restauración	Restablezca la configuración del XClarity Controller a los valores predeterminados de fábrica, cree copias de seguridad de la configuración actual o restablezca la configuración desde un archivo de restauración.
	Licencia	Gestione las claves de activación para características opcionales del XClarity Controller.
	Red	Configure las propiedades, estado y los valores de red para el XClarity Controller.
	Seguridad	Configure las propiedades, estado y los valores de seguridad para el XClarity Controller.

Tabla 1. Funciones de XClarity Controller (continuación)

Tab	Selección	Descripción
	Usuario/LDAP	• Configure los perfiles de inicio de sesión del XClarity Controller y la configuración de inicio de sesión global. • Vea las cuentas de usuario que se registran actualmente al XClarity Controller. • La pestaña LDAP configura la autenticación del usuario para el uso con uno o más servidores LDAP. También le permite habilitar o deshabilitar la seguridad de LDAP y gestionar los certificados.

Capítulo 3. Configuración del XClarity Controller

Utilice la información de este capítulo para comprender las opciones disponibles para las configuraciones del XClarity Controller.

Al configurar el XClarity Controller están disponibles las siguientes opciones clave:

- Copia de seguridad y restauración
- Licencia
- Red
- Seguridad
- Usuario/LDAP

Configuración de las cuentas de usuario/LDAP

Utilice la información de este tema para comprender cómo se gestionan las cuentas de usuario.

Pulse **Usuario/LDAP** en **Configuración de BMC** para crear, modificar y ver cuentas de usuario y para configurar los valores de LDAP.

La pestaña **Usuario local** muestra las cuentas de usuario que se configuran en el XClarity Controller y que actualmente están conectadas al XClarity Controller.

La pestaña **LDAP** muestra la configuración LDAP para acceder a cuentas de usuario que se guardan en un servidor LDAP.

Método de autenticación del usuario

Utilice la información en este tema para comprender las modalidades que el XClarity Controller puede utilizar para autenticar los intentos de inicio de sesión.

Pulse **Habilitar inicios de sesión desde** para seleccionar cómo se autentican los intentos de inicio de sesión del usuario. Puede seleccionar uno de los métodos de autenticación siguientes:

- **Únicamente local:** los usuarios se autentican mediante una búsqueda de la cuenta de usuario local configurada en el XClarity Controller. Si no hay ninguna coincidencia de Id. de usuario y contraseña, se niega su acceso.
- **Únicamente LDAP:** XClarity Controller intenta autenticarse con el usuario con las credenciales guardadas en un servidor LDAP. Las cuentas de usuario locales del XClarity Controller **no** se buscan con este método de autenticación.
- **Primero local y después LDAP:** se intenta primero la autenticación local. Si la autenticación local falla; a continuación, se intentará la autenticación LDAP.
- **LDAP primero, a continuación usuario local:** se intenta primero la autenticación LDAP. Si la autenticación LDAP falla; a continuación, se intentará la autenticación local.

Notas:

- Solo se comparten las cuentas localmente administradas con las interfaces IPMI y SNMP. Estas interfaces no admiten la autenticación LDAP.
- Los usuarios IPMI y SNMP pueden iniciar sesión utilizando las cuentas administradas localmente cuando el campo **Habilitar inicios de sesión desde** es **Únicamente LDAP**.

Creación de una nueva cuenta de usuario

Utilice la información en este tema para crear un nuevo usuario local.

Crear usuario

Pulse **Crear** para crear una nueva cuenta de usuario.

Complete los campos siguientes: **Nombre de usuario**, **Contraseña**, **Confirmar la contraseña** y **Nivel de autoridad**. Para conocer más detalles sobre el nivel de autorización, consulte la sección siguiente.

Nivel de autoridad del usuario

Los siguientes niveles de autoridad de usuario están disponibles:

Supervisor
El nivel de autorización del usuario supervisor no tiene restricciones.

Solo lectura
El nivel de autoridad de usuario de solo lectura tiene acceso de solo lectura y no puede realizar las acciones como transferencias de archivos, acciones de alimentación y de reinicio o las funciones de presencia remota.

Personalizado
El nivel de autoridad de usuario personalizado permite personalizar la autoridad del usuario con valores para acciones que el usuario puede realizar.

Seleccione uno o varios de los niveles de autoridad personalizados siguientes.

Configuración del adaptador: redes y seguridad
Un usuario puede modificar los parámetros de configuración en las páginas de Seguridad, Red y Puerto de serie.

Gestión de cuenta de usuario
Un usuario puede añadir, modificar o eliminar usuarios y cambiar los valores de inicio de sesión globales.

Acceso a consola remota
Un usuario puede acceder a la consola remota.

Acceso a la consola remota y al disco remoto
Un usuario puede obtener acceso a la consola remota y a la característica de medios virtuales.

Alimentación de servidor remoto/Reiniciar
Un usuario puede realizar las funciones de encendido y reinicio del servidor.

Configuración del adaptador: aspectos básicos
Un usuario puede modificar los parámetros de configuración en las páginas de Propiedades del servidor y Sucesos.

Capacidad de borrar registros de sucesos
Un usuario puede borrar los registros de sucesos. Cualquiera puede ver los registros de sucesos, pero se requiere este nivel de autoridad para borrar los registros.

Configuración del adaptador: avanzado (actualización de firmware, reiniciar el BMC, restaurar la configuración)
Un usuario no tiene restricciones al configurar el XClarity Controller. Además, el usuario tiene acceso administrativo al XClarity Controller. El acceso administrativo incluye las siguientes funciones avanzadas: actualizaciones de firmware, arranque de la red PXE, restaurar el XClarity

Controller a los valores de fábrica, modificar y restaurar la configuración de XClarity Controller desde un archivo de configuración y reiniciar o restablecer el XClarity Controller.

Cuando un usuario establece el nivel de autoridad de un Id. de inicio de sesión de XClarity Controller, el nivel de privilegio de IPMI resultante del Id. de usuario de IPMI correspondiente se configura según las prioridades siguientes:

- Si un usuario establece el nivel de autoridad del Id. de inicio de sesión de XClarity Controller en **Supervisor**, el nivel de privilegio de IPMI se define como administrador.
- Si un usuario establece el nivel de autoridad del Id. de inicio de sesión de XClarity Controller en **Solo lectura**, el nivel de privilegio de IPMI se define como usuario.
- Si un usuario establece el nivel de autoridad del Id. de inicio de sesión de XClarity Controller a cualquiera de los tipos de acceso siguientes, el nivel de privilegio de IPMI se define como administrador:
  - Acceso de gestión de cuenta de usuario
  - Acceso a consola remota
  - Acceso a la consola remota y al disco remoto
  - Configuración del adaptador: redes y seguridad
  - Configuración del adaptador: avanzado
- Si un usuario establece el nivel de autoridad del Id. de inicio de sesión de XClarity Controller como **Acceso a Alimentación de servidor remoto/Reiniciar** o **Capacidad de borrar registros de sucesos**, el nivel de privilegio de IPMI se define como operador.
- Si un usuario establece el nivel de autoridad del Id. de inicio de sesión de XClarity Controller en **Configuración del adaptador: aspectos básicos**, el nivel de privilegio de IPMI se define como usuario.

Configuración de SNMPv3

Para habilitar el acceso de SNMPv3 para un usuario, seleccione la casilla al lado de **Configuración de SNMPv3**. Se explican las siguientes opciones de acceso del usuario:

Tipo de acceso
Solo se admiten las operaciones de **GET**. XClarity Controller no admite operaciones **SET** SNMPv3. SNMP3 solo puede realizar operaciones de consulta.

Dirección para interrupciones
Especifique el destino para el usuario. Este puede ser una dirección IP o nombre de host. Al usar interrupciones, el agente SNMP notifica la estación de gestión sobre los sucesos, (por ejemplo, cuando la temperatura del procesador ha excedido el límite).

Protocolo de autenticación
Solo **HMAC-SHA** se admite como protocolo de autenticación. El modelo de seguridad SNMPv3 utiliza este algoritmo para la autenticación.

Protocolo de privacidad
La transferencia de datos entre el cliente de SNMP y el agente se puede proteger mediante cifrado. Los métodos admitidos son **CBC-DES** y **AES**.

Notas: Incluso si un usuario de SNMPv3 usa cadenas repetitivas de una contraseña, aún se permitirá el acceso al XClarity Controller. Se muestran dos ejemplos para su referencia.

- Si se establece la contraseña en "**11111111**" (número de ocho dígitos con ocho 1), el usuario aún puede acceder el XClarity Controller, si la contraseña se ingresa accidentalmente con más de ocho 1. Por ejemplo, si la contraseña se ingresa como "**1111111111** (número de diez dígitos que contiene diez 1), aún se otorgará el acceso. Se considerará que la cadena repetitiva tiene la misma clave.

- Si la contraseña se establece en “**bertbert**”, el usuario aún podrá acceder al XClarity Controller si la contraseña se ingresa accidentalmente como “**bertbertbert**”. Se considerará que ambas contraseñas tienen la misma clave.

Para obtener más detalles, consulte la página 72 en el documento de Estándar Internet RFC 3414 (https://tools.ietf.org/html/rfc3414).

Clave SSH

XClarity Controller admite autenticación de clave pública SSH (tipo de clave RSA). Para añadir una clave SSH a una cuenta de usuario local, seleccione la casilla al lado de **Clave de SSH**. Se proporcionan las siguientes dos opciones:

Seleccionar archivo de clave
Seleccione el archivo de clave SSH para importar al XClarity Controller desde el servidor.

Ingresar clave en un campo de texto
Pegue o escriba los datos desde la clave SSH en el campo de texto.

Notas:

- Algunas de las herramientas de Lenovo pueden crear un usuario temporal para acceder al XClarity Controller, cuando la herramienta se ejecuta en el sistema operativo del servidor. Esta cuenta temporal no es visible y no utiliza ninguna de las 12 posiciones de cuentas de usuario locales. La cuenta se crea con un nombre de usuario aleatorio (por ejemplo, “20luN4SB”) y la contraseña. La cuenta solo se puede utilizar para acceder al XClarity Controller en la interfaz Ethernet sobre USB interna y solo para las interfaces CIM-XML y SFTP. La creación y la eliminación de esta cuenta temporal se registra en el registro de auditoría al igual que cualquier acción realizada por la herramienta con las credenciales.
- Para el Id. de motor de SNMPv3, el XClarity Controller usa una cadena hexadecimal para indicar el Id. Esta cadena hexadecimal se convierte en el nombre de host de XClarity Controller predeterminado. Consulte el siguiente ejemplo:

  El nombre de host “XCC-7X06-S4AHJ300” primero se convierte en el formato ASCII: 88 67 67 45 55 88 48 54 45 83 52 65 72 74 51 48 48

  La cadena hexadecimal está integrada con el formato ASCII (ignore los espacios intermedios): 58 43 43 36 de 2d 37 58 30 48 de 2d 53 34 41 4a 33 30 30

Eliminación de una cuenta de usuario

Utilice la información en este tema para eliminar una cuenta de usuario local.

Para eliminar una cuenta de usuario local, pulse el icono de papelera de reciclaje en la fila de la cuenta que desea eliminar. Si cuenta con la autorización, puede eliminar su propia cuenta o la cuenta de otros usuarios, incluso si inició sesión, a menos que sea la única cuenta restante con privilegios de gestión de cuentas de usuario. Las sesiones que ya están en progreso cuando se eliminan las cuentas de usuario no se finalizarán automáticamente.

Uso de contraseñas con hash para la autenticación

Utilice la información de este tema para comprender cómo utilizar las contraseñas con hash para la autenticación.

Además de la utilización de contraseñas y cuentas de usuario LDAP/AD, el XClarity Controller también admite contraseñas de terceros con hash para la autenticación. La contraseña especial usa un formato de hash unidireccional (SHA256) y es admitida por las interfaces web de XClarity Controller, OneCLI y CLI. Sin embargo, tenga en cuenta que la autenticación de las interfaces SNMP, IPMI y CIM de XCC no admiten las contraseñas de terceros con hash. Solo la herramienta OneCLI y la interfaz CLI de XCC pueden crear una

cuenta nueva con una contraseña con hash o realizar una actualización de la contraseña. El XClarity Controller también permite la herramienta OneCLI y la interfaz de CLI de XClarity Controller para recuperar la contraseña si está habilitada la capacidad de lectura de contraseña con hash.

Establecimiento de la contraseña con hash mediante la web de XClarity Controller

Haga clic en **Seguridad** en **Configuración de BMC** y desplácese hasta la sección **Security Password Manager** para habilitar o deshabilitar la función de la contraseña de terceros. Si se habilita, se utiliza una contraseña de terceros con hash para la autenticación de inicio de sesión. También se puede habilitar o deshabilitar la recuperación de contraseña de terceros con hash desde XClarity Controller.

Nota: De forma predeterminada, las funciones **Contraseña de terceros** y **Permitir recuperación de contraseña de terceros** están deshabilitadas.

Para comprobar si la contraseña del usuario es **Nativa** o una **Contraseña de terceros**, haga clic en **Usuario/LDAP** en **Configuración de BMC** para obtener más detalles. La información estará en la columna **Atributo avanzado**.

Notas:

- Los usuarios no podrán cambiar una contraseña si se trata de una contraseña de terceros y los campos **Contraseña** y **Confirmar contraseña** están desactivados.
- Si la contraseña de terceros caducó, se mostrará un mensaje de advertencia durante el proceso de inicio de sesión del usuario.

Establecimiento de la contraseña con hash mediante la función OneCLI

- Habilitar la función

  ```
  $ sudo OneCli config set IMM.ThirdPartyPassword Enabled
  ```

- Creación de contraseña con hash (Sin Salt). A continuación se muestra un inicio de sesión de ejemplo en XClarity Controller con la contraseña **password123**.

  ```
  $ pwhash = `echo -n password123 | openssl dgst -sha256 | awk '{print $NF}'`

  $ echo $pwhash 5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8

  $ sudo OneCli config set IMM.Loginid.2 admin

  $ sudo OneCli config set IMM.SHA256Password.2 $pwhash

  $ sudo OneCli config set IMM.SHA256PasswordSalt.2 ""
  ```

- Crear un usuario con la contraseña con hash (Con Salt). A continuación se muestra un inicio de sesión de ejemplo en XClarity Controller con la contraseña **password123**. Salt = abc.

  ```
  $ pwhash = `echo -n password123abc | openssl dgst -sha256 | awk '{print $NF}'`

  $ echo $pwhash 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee

  $ sudo OneCli config set IMM.Loginid.3 Admin

  $ sudo OneCli config set IMM.SHA256Password.3 $pwhash

  $ sudo OneCli config set IMM.SHA256PasswordSalt.3 'abc'
  ```

- Recuperar la contraseña con hash y salt.

  ```
  $ sudo OneCli config set IMM.ThirdPartyPasswordReadable Enabled

  $ sudo OneCli config show IMM.SHA256Password.3
  ```

```
$ sudo OneCli config show IMM.SHA256PasswordSalt.3
```

- Eliminar la contraseña con hash y salt.

  ```
  $ sudo OneCli config set IMM.SHA256Password.3 ""

  $ sudo OneCli config set IMM.SHA256PasswordSalt.3 ""
  ```

- Establecer la contraseña con hash para una cuenta existente.

  ```
  $ sudo OneCli config set IMM.Loginid.2 admin

  $ sudo OneCli config set IMM.Password.2 Passw0rd123abc

  $ sudo OneCli config set IMM.SHA256Password.2 $pwhash

  $ sudo OneCli config set IMM.SHA256PasswordSalt.2 ""
  ```

  Nota: Mientras se establece la contraseña con hash, esta contraseña entrará en efecto inmediatamente. La contraseña estándar original dejará de funcionar. En este ejemplo, la contraseña estándar original **Passw0rd123abc** no se puede utilizar más hasta que se elimine la contraseña con hash.

Establecimiento de la contraseña con hash mediante la función CLI

- Habilitar la función

  ```
  > hashpw -sw enabled
  ```

- Creación de contraseña con hash (Sin Salt). A continuación se muestra un inicio de sesión de ejemplo en XClarity Controller con la contraseña **password123**.

  ```
  $ pwhash = `echo -n password123 | openssl dgst -sha256 | awk '{print $NF}'`

  5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8

  > users -2 -n admin -shp 5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8 -a
  super
  ```

- Crear un usuario con la contraseña con hash (Con Salt). A continuación se muestra un inicio de sesión de ejemplo en XClarity Controller con la contraseña **password123**. Salt = abc.

  ```
  $ pwhash = `echo -n password123abc | openssl dgst -sha256 | awk '{print $NF}'`

  $ echo $pwhash 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee

  > users -3 -n Admin -shp 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee
  -ssalt 'abc' -a super
  ```

- Recuperar la contraseña con hash y salt.

  ```
  > hashpw -re enabled

  > users -3 -ghp -gsalt
  ```

- Eliminar la contraseña con hash y salt.

  ```
  > users -3 -shp "" -ssalt ""
  ```

- Establecer la contraseña con hash para una cuenta existente.

  ```
  > users -2 -n admin -p Passw0rd123abc -shp
  5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8 -a super
  ```

  Nota: Mientras se establece la contraseña con hash, esta contraseña entrará en efecto inmediatamente. La contraseña estándar original dejará de funcionar. En este ejemplo, la contraseña estándar original **Passw0rd123abc** no se puede utilizar más hasta que se elimine la contraseña con hash.

Después de configurar la contraseña, recuerde no utilizar estas credenciales para iniciar sesión en XClarity Controller. Al iniciar sesión, deberá usar la contraseña legible. En el ejemplo siguiente, la contraseña legible es “password123”.

```
$ pwhash = ‘echo –n password123 | openssl dgst –sha256 | awk '{print $NF}''

5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8

> users -2 -n admin -shp 5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8 -a super
```

Configuración de valores globales de inicio de sesión

Utilice la información en este tema para configurar las políticas de inicio de sesión y contraseñas que se aplican a todos los usuarios.

Tiempo de espera por inactividad de sesión web

Utilice la información en este tema para establecer la opción de tiempo de espera por inactividad de sesión web.

En el campo **Tiempo de espera por inactividad de sesión web**, puede especificar cuánto tiempo, en minutos, el XClarity Controller espera antes de que desconecte una sesión web inactiva. El tiempo de espera máximo es de 1.440 minutos. Si se establece en 0, la sesión web no se cerrará nunca.

El firmware del XClarity Controller admite hasta seis sesiones web simultáneas. Para liberar sesiones para otros usuarios, se recomienda que cierre la sesión del web cuando haya terminado en vez de confiar que el tiempo de espera de inactividad cierre automáticamente su sesión.

Nota: Si deja el navegador abierto en una página web del XClarity Controller que se actualiza automáticamente, su sesión web no se apagará automáticamente debido a la inactividad.

Configuración de la política de seguridad de la cuenta

Utilice esta información para comprender y establecer la configuración de la política de seguridad de la cuenta del servidor.

Notas: En un Flex System, los valores de política de seguridad de cuenta son gestionados por el Flex System Chassis Management Module (CMM) y no pueden modificarse a través de XCC. Cuando el CMM se utiliza para configurar la política de seguridad de cuenta, tome nota de las siguientes acciones:

- A diferencia del XCC, el CMM no tiene el valor **Periodo de advertencia de caducidad de la contraseña (en días)**. Cuando el **Periodo de caducidad de la contraseña** está configurado para que sea superior a 5 días en el CMM, XCC configurará el periodo de advertencia de caducidad de la contraseña en 5 días. Por el contrario, si el valor es inferior a 5 días, el período de advertencia de caducidad de la contraseña será el mismo que el valor ingresado en **Periodo de caducidad de la contraseña**.
- Para el valor **Número máximo de errores de inicio de sesión (veces)**, el intervalo establecido en el CMM es de 0 a 100 veces. Sin embargo, el intervalo definido en el XCC es de 0 a 10 veces. Por lo tanto, cuando el usuario selecciona un valor que supera la cantidad de 10 veces en el CMM, XCC aún establecerá el número máximo de errores de inicio de sesión en 10 veces.
- Para la configuración **Intervalo de cambio de contraseña mínimo (horas)**, el intervalo establecido en el CMM es de 0 a 1440 horas. Sin embargo, el intervalo definido en el XCC es de 0 a 240 horas. Por lo tanto, cuando el usuario selecciona un valor que supera las 240 horas en el CMM, XCC aún configurará el intervalo mínimo de cambio de contraseña en 240 horas.

La información siguiente es una descripción de los campos de los valores de seguridad.

Obligar a cambiar la contraseña en el primer acceso

Después de configurar un usuario nuevo con una contraseña predeterminada, seleccione esta casilla de verificación para que el usuario cambie la contraseña la primera vez que inicie la sesión. El valor predeterminado para este campo tiene la casilla de verificación habilitada.

La contraseña de la cuenta predeterminada se debe cambiar en el próximo inicio de sesión
Una opción de fábrica se proporcionan para restablecer el perfil USERID predeterminado después del primer inicio de sesión satisfactorio. Cuando se habilita esta casilla de verificación, la contraseña predeterminada se debe cambiar antes de poder usar la cuenta. La nueva contraseña está sujeta a todas las reglas de cumplimiento de contraseñas activas. El valor predeterminado para este campo tiene la casilla de verificación habilitada.

Se requiere una contraseña compleja
El cuadro de opción está activado de manera predeterminada y la contraseña compleja debe seguir las siguientes reglas:

- Solo contener los siguientes caracteres (no se permiten caracteres de espacio en blanco): A-Z, a-z, 0-9, ~`!@#$%^&*()-+={}[]|:;"'<>,?/._
- Debe contener al menos una letra
- Debe contener al menos un número
- Deben contener al menos dos de siguientes combinaciones:
  - Al menos una letra mayúscula.
  - Al menos una letra minúscula.
  - Al menos un carácter especial.
- No se permiten otros caracteres (especialmente espacios o caracteres de espacio en blanco)
- Las contraseñas no pueden tener más de dos instancias consecutivas de caracteres idénticos (por ejemplo, “aaa”).
- La contraseña no puede ser idéntica al nombre de usuario, simplemente repetir el nombre de usuario una o más veces o ser el nombre de usuario en el orden inverso.
- Las contraseñas deben tener una longitud mínima de 8 y un máximo de 32 caracteres

Si el cuadro de opciones no está activado, el número especificado en la longitud mínima de la contraseña puede configurarse como de 0 a 32 caracteres. La contraseña de la cuenta puede estar en blanco si la longitud mínima de la contraseña está configurada en 0.

Periodo de caducidad de la contraseña (días)
Este campo contiene la duración máxima de contraseña que se permite antes de que la contraseña se debe modificar. Se admite un valor de 0 a 30 días. El valor predeterminado para este campo es 14 días.

Periodo de advertencia de caducidad de la contraseña (días)
Este campo contiene el número de días antes de que el usuario reciba una advertencia de que va a caducar la contraseña. Si se establece en 0, no se envían avisos. Se admite un valor de 0 a 30 días. El valor predeterminado para este campo es 14 días.

Longitud mínima de la contraseña
Este campo contiene la longitud mínima de contraseña. Este campo admite de 8 a 32 caracteres. El valor predeterminado para este campo es 10.

Ciclo mínimo de reutilización de la contraseña
Este campo contiene el número de contraseñas anteriores que no se pueden reutilizar. Se pueden comparar hasta diez contraseñas anteriores. Seleccione 0 para permitir la reutilización de todas las contraseñas anteriores. Se admite un valor de 0 a 10. El valor predeterminado para este campo es 5.

Intervalo mínimo de cambio de contraseña (horas)

Este campo contiene cuánto tiempo debe esperar un usuario entre los cambios de contraseña. Se admite un valor de 0 a 240 horas. El valor predeterminado para este campo es 1 hora.

Número máximo de errores de inicio de sesión (veces)
Este campo contiene el número de intentos de inicio de sesión fallidos que se permiten antes de que el usuario quede bloqueado durante un periodo de tiempo. Se admite un valor de 0 a 10. El valor predeterminado para este campo es de cinco errores de inicio de sesión.

Periodo de bloqueo tras superar el número máximo de errores de inicio de sesión (minutos)
Este campo especifica cuánto tiempo (en minutos), el subsistema del XClarity Controller deshabilitará los intentos de inicio de sesión remoto después de que el número máximo de fallos de inicio de sesión se haya alcanzado. Se admite un valor de 0 a 2.880 minutos. El valor predeterminado para este campo es 60 minutos.

Configuración de LDAP

Utilice la información en este tema para visualizar o cambiar la configuración de LDAP de XClarity Controller.

El soporte LDAP incluye:

- Soporte para la versión del protocolo LDAP 3 (RFC 2251)
- Soporte para las APi de cliente LDAP estándar (RFC-1823)
- Soporte para la sintaxis de filtros de búsqueda LDAP estándar (RFC-2254)
- Compatibilidad con la extensión de Lightweight Directory Access Protocol (v3) para la Seguridad de capa de transporte (RFC-2830)

La implementación de LDAP admite los siguientes servidores LDAP:

- Microsoft Active Directory (Windows 2003, Windows 2008, Windows 2012, Windows 2016, Windows 2019)
- Modo de aplicación de Microsoft Active Directory (servidor de Windows 2003)
- Servicio Microsoft Lightweight Directory (Windows 2008, Windows 2012)
- Novell eDirectory Server, versión 8.7, 8.8 y 9.4
- OpenLDAP Server 2.1, 2.2, 2.3 y 2.4

Pulse la pestaña **LDAP** para ver o para modificar la configuración de LDAP de XClarity Controller.

XClarity Controller puede autenticar remotamente el acceso de un usuario en un servidor LDAP central en vez de, o además de las cuentas locales de usuario que se almacenan en el propio XClarity Controller. Los privilegios se pueden designar para cada cuenta de usuario utilizando la cadena IBMRBSPermissions. También puede utilizar el servidor LDAP para asignar usuarios en grupos y para realizar la autenticación de grupo, además de autenticación normal del usuario (comprobación mediante contraseña). Por ejemplo, un XClarity Controller se puede asociar con uno o varios grupos, el usuario pasará la autenticación de grupo solo si el usuario pertenece al menos a un grupo que esté asociado con el XClarity Controller.

Para configurar un servidor LDAP, lleve a cabo los pasos siguientes:

1. En **Información del servidor LDAP**, las opciones siguientes están disponibles en la lista de elementos:
   - **Usar el servidor LDAP únicamente para autenticación (con autorización local)**: esta selección indica al XClarity Controller utilizar las credenciales únicamente para autenticar con el servidor LDAP y para recuperar información de membresía de grupo. Los nombres y privilegios de grupo se pueden configurar en la sección de Configuración de Active Directory.

- **Usar el servidor LDAP para autenticación y autorización**: esta selección indica al XClarity Controller utilizar las credenciales para autenticar con el servidor LDAP y para identificar el permiso del usuario.

Nota: Los servidores LDAP que se usan para autenticación se pueden configurar manualmente o se pueden descubrir dinámicamente mediante los registros de DNS SRV.

- **Usar servidores preconfigurados**: puede configurar hasta cuatro servidores LDAP al ingresar la dirección IP de cada servidor o nombre de host, si DNS esté habilitado. El número de puerto para cada servidor es opcional. Si este campo se deja en blanco, se usa el valor predeterminado de 389 para conexiones LDAP no seguras. Para conexiones seguras, el valor predeterminado puerto es 636. Debe configurar al menos un servidor LDAP.
- **Usar DNS para encontrar servidores**: puede optar por descubrir los servidores LDAP dinámicamente. Los mecanismos descritos en RFC2782 (A DNS RR para especificar la ubicación de los servicios) se utilizan para localizar los servidores LDAP. Esto se conoce como SRV DNS. Debe especificar un nombre de dominio completamente calificado (FQDN) que se usará como el nombre de dominio en la solicitud de DNS SRV.
  - **Bosque de AD**: en un entorno con grupos universales en varios dominios, el nombre de bosque (grupo de dominios) debe configurarse para detectar los catálogos globales requeridos (GC). En un entorno donde no se aplica la membresía de grupo entre dominios, este campo se puede dejar en blanco.
  - **Dominio AD**: deberá especificar un nombre de dominio completamente calificado (FQDN) que se usará como el nombre de dominio en la solicitud de DNS SRV.

Si desea habilitar el LDAP seguro, pulse la casilla de verificación **Habilitar LDAP seguro** . Para poder admitir LDAP seguro, debe existir primero un certificado SSL válido y se debe importar al menos un certificado de confianza del cliente SSL en XClarity Controller. El servidor LDAP debe admitir la versión 1.2 de seguridad de la capa de transporte (TLS) para que sea compatible con el cliente LDAP seguro de XClarity Controller. Para obtener más información sobre la administración de certificados, consulte “Gestión de certificado SSL” en la página 38.

2. Complete la información en **Parámetros adicionales**. A continuación aparecen explicaciones de los parámetros.

Método de vinculación

Antes de que pueda buscar o consultar el servidor LDAP, debe enviar una solicitud de vinculación. Este campo controla cómo se realiza esta vinculación inicial con el servidor LDAP. Los siguientes métodos de vinculación están disponibles:

- **No se necesitan credenciales**

  Utilice este método para vincular sin un nombre distinguido (DN) o una contraseña. Este método no se recomienda porque la mayoría de los servidores están configurados para rechazar solicitudes de búsqueda sobre registros de usuarios específicos.

- **Usar credenciales configuradas**

  Utilice este método para vincular con el cliente DN y la contraseña configurada.

- **Usar credenciales de inicio de sesión**

  Use este método para vincular con las credenciales proporcionadas durante el proceso de inicio de sesión. El Id. de usuario se puede proporcionar usando un DN, un DN parcial, un nombre de dominio completamente calificado o mediante un Id. de usuario que coincida con el atributo de búsqueda de UID configurado en el XClarity Controller. Si las credenciales presentadas se asemejan a un nombre distinguido parcial (por ejemplo cn=joe), este nombre distinguido parcial se presentará al DN raíz configurado en un intento de crear un nombre distinguido que coincida con el registro del usuario. Si el intento de vinculación falla, se intentará realizar un último intento

de vinculación al presentar cn= con la credencial de inicio de sesión y presentar la cadena resultante con el DN raíz configurado.

Si el enlace inicial se realiza correctamente, se realiza una búsqueda para buscar una entrada en el servidor LDAP que pertenezca al usuario que está iniciando sesión. De ser necesario, se realiza un segundo intento de enlace, esta vez con el DN que se recupera del registro LDAP del usuario y la contraseña que se ingresó durante el proceso de inicio de sesión. Si falla un segundo intento de vinculación, se rechaza el acceso al usuario. El segundo intento de vinculación solo se realiza cuando se utilizan los métodos de vinculación **No se requieren credenciales** o **Credenciales configuradas por el usuario**.

Nombre distinguido (DN) raíz

Este es el nombre distinguido (DN) de la entrada raíz de árbol de directorio en el servidor LDAP (por ejemplo, dn=mycompany,dc=com). Este DN se utiliza como el objeto base para todas las solicitudes de búsqueda.

Atributo de búsqueda UID

Cuando el método de vinculación está configurado como **No se requieren credenciales** o **Credenciales configuradas por el usuario**, una solicitud de búsqueda sigue el enlace inicial al servidor LDAP al recuperar la información específica acerca del usuario, incluyendo el DN de usuario, permisos de inicio y membresía de grupo. Esta solicitud de búsqueda debe especificar el nombre del atributo que representa a las Id. de usuario en ese servidor. Este nombre de atributo se configura en este campo. En los servidores de Active Directory, el nombre de atributo generalmente es **sAMAccountName**. En los servidores Novell eDirectory y OpenLDAP, el nombre del atributo es **uid**. Si este campo se deja en blanco, el valor predeterminado es **uid**.

Filtro del grupo

El campo **Filtro de grupo** se usa para la autenticación de grupos. Después de verificar las credenciales de usuario correctamente, se intentará la autenticación del grupo. Si falla una autenticación de grupo, se rechaza el intento de inicio de sesión del usuario. Cuando se configura el filtro de grupo, se utiliza para especificar a qué grupos pertenece XClarity Controller. Esto significa que el usuario deben pertenecer a, al menos, uno de los grupos configurados para que la autenticación de grupo se realice correctamente. Si el campo **Filtro de grupo** se deja en blanco, la autenticación de grupo se realiza correctamente de forma automática. Si el filtro de grupo está configurado, se realiza un intento de hacer coincidir al menos un grupo en la lista con un grupos al que el usuario pertenezca. Si no hay ninguna coincidencia, la autenticación de usuario falla y se niega el acceso. Si existe al menos una coincidencia, la autenticación de grupo se realiza correctamente.

Las comparaciones distinguen entre mayúsculas y minúsculas. El filtro tiene un límite de 511 caracteres y consiste en uno o más nombres de grupo. El carácter de dos puntos (:) debe utilizarse para delimitar nombres de grupo múltiples. Los espacios antes y después se omiten, pero cualquier otro espacio se trata como parte del nombre del grupo.

Nota: El carácter comodín (*) ya no se considera como comodín. El concepto de comodín se ha interrumpido para impedir que se produzcan exposiciones de seguridad. Un nombre de grupo se puede especificar como un DN completo o utilizando la parte del **cn**. Por ejemplo, un grupo con un DN de cn=adminGroup, dc=mycompany, dc=com se puede especificar utilizando el DN real o al utilizar adminGroup.

Únicamente en los entornos de Active Directory, se admite la membresía de grupo jerarquizada. Por ejemplo, si un usuario es un miembro del GroupoA y de GroupoB, y GroupoA también hay un miembro de GroupoC, el usuario se considera miembro de GroupoC también. Las búsquedas jerarquizadas se detienen si se han buscado 128 grupos. Los grupos en un nivel se buscan antes que los grupos en un nivel inferior. No se detectan los bucles.

Atributo de búsqueda de grupos

En un entorno Active Directory o Novell eDirectory, el campo **Atributo de búsqueda de grupos** especifica el nombre de atributo usado para identificar los grupos al que pertenece un usuario. En un entorno Active Directory, el nombre de atributo es **memberOf**. En un entorno eDirectory, el nombre de atributo es **groupMembership**. En un entorno de servidor OpenLDAP, los usuarios generalmente se asignan a grupos cuyo objectClass equivale a PosixGroup. En ese contexto, este campo especifica el nombre de atributo usado para identificar los miembros de un PosixGroup en particular. Este nombre de atributo es **memberUid**. Si este campo se deja en blanco, el nombre del atributo en el filtro usa **memberOf** de forma predeterminada.

Atributo de permiso de inicio de sesión

Cuando un usuario se autentica a través de un servidor LDAP satisfactoriamente, deben recuperarse los permisos de inicio de sesión para el usuario. Para poder recuperar los permisos de inicio de sesión, el filtro de búsqueda enviado al servidor debe especificar el nombre de atributo asociado con los permisos de inicio de sesión. El campo **Atributo de permiso de inicio de sesión** especifica el nombre de atributo. Si este campo se deja en blanco, al usuario se le asignan permisos predeterminados de solo lectura y se supone que el usuario pasa la autenticación de usuario y de grupo.

El valor del atributo que el servidor LDAP devuelve busca la cadena de palabra clave IBMRBSPermissions=. A esta cadena de palabra clave le debe seguir inmediatamente una cadena de bit ingresada como 12 0 o 1 consecutivos. Cada bit representa un conjunto de funciones. Los bits reciben una numeración de acuerdo con su posición. El bit más a la izquierda es la posición de bit 0 y el bit de más a la derecha es la posición de bit 11. Un valor de 1 en una posición en particular habilita esa función en especial que se asocia con la posición del bit. Un valor de 0 en una posición de bit deshabilita la función asociada a esa posición de bit.

La cadena IBMRBSPermissions=010000000000 es un ejemplo válido. La palabra clave IBMRBSPermissions= se utiliza para permitir que esté colocado en cualquier lugar en este campo. Esto le permite al administrador LDAP reutilizar un atributo existente y así evitar una extensión del esquema LDAP. Además, esto permite que se pueda usar el atributo para su propósito original. Puede añadir la cadena de palabras clave en cualquier lugar en este campo. El atributo utilizado puede permitir una cadena de formato libre. Cuando el atributo se recupera satisfactoriamente, el valor que el servidor LDAP devuelve se interpreta de acuerdo con la información en la tabla siguiente.

Tabla 2. Bits de permiso

Tabla de tres columnas que contiene las explicaciones de la posición de bit.

Posición de bit	Función	Explicación
0	Rechazar siempre	Un usuario siempre fallará la autenticación. Esta función puede utilizarse para bloquear a un usuario o usuarios asociados a un grupo específico.
1	Acceso de supervisor	Se le asignan privilegios de administrador a un usuario. El usuario tiene acceso de lectura/escritura a todas las funciones. Cuando establece este bit, no es necesario configurar individualmente los otros bits.
2	Acceso de solo lectura	El usuario posee acceso de solo lectura y no puede realizar ningún procedimiento de mantenimiento (por ejemplo, reiniciar, acciones remotas, actualizaciones de firmware) y nada se puede modificar (mediante las funciones de guardar, borrar o restaurar). La posición de bit 2 y todos los otros bits son mutuamente exclusivos y la posición de bit 2 posee la precedencia más baja. Cuando se establece cualquier otro bit, se ignorará este bit.
3	Redes y seguridad	Un usuario puede modificar la configuración en Seguridad, Protocolos de red, Interfaz de red, Asignaciones de puertos y Puerto de serie.

Tabla 2. Bits de permiso (continuación)

Posición de bit	Función	Explicación
4	Gestión de cuenta de usuario	Un usuario puede añadir, modificar o eliminar usuarios y cambiar la configuración de inicio de sesión global en la ventana de perfiles de inicio de sesión.
5	Acceso a consola remota	Un usuario puede acceder a la consola remota del servidor.
6	Acceso a la consola remota y al disco remoto	Un usuario puede acceder a la consola remota del servidor y a las funciones del disco remoto para el servidor remoto.
7	Acceso al encendido/ reinicio del servidor remoto	Un usuario puede acceder a las funciones de encendido y reinicio del servidor remoto.
8	Configuración de adaptador básico	Un usuario puede modificar los parámetros de configuración en las ventanas de configuración del sistema y alertas.
9	Capacidad de borrar registros de sucesos	Un usuario puede borrar los registros de sucesos. **Nota:** Todos los usuarios pueden ver los registros de sucesos; pero para borrar los registros de sucesos se pedirá al usuario tener este nivel de permiso.
10	Configuración de adaptador avanzado	Un usuario no tiene restricciones al configurar el XClarity Controller. Además, el usuario tiene acceso administrativo al XClarity Controller. El usuario también puede realizar las siguientes funciones avanzadas: actualizaciones de firmware, arranque de la red PXE, restaurar el XClarity Controller a los valores de fábrica, modificar y restaurar la configuración del adaptador desde un archivo de configuración y reiniciar o restablecer el XClarity Controller.
11	Reservado	Esta posición de bit está reservada para un uso futuro. Si ninguno de los bits está establecido, el usuario tiene autoridad de solo lectura. Se le da prioridad a los permisos de inicio de sesión recuperados directamente desde el registro del usuario. Si el atributo de permiso de inicio de sesión no está en el registro del usuario, se realiza un intento por recuperar los permisos de los grupos a los que el usuario pertenece. Esto se ejecuta como parte de la fase de la autenticación de grupo. Al usuario se le asigna el OR inclusivo para todos los bits para todos los grupos. El bit de acceso de solo lectura (posición 2) se establece si todos los demás bits están establecidos en cero. Si se establece el bit Rechazar siempre (posición 0) para cualquier de los grupos, el usuario no tendrá acceso. El bit Rechazar siempre (posición 0) posee precedencia siempre sobre cualquier otro bit.

Si no se establece ninguno de estos bits, el valor predeterminado se establece como **Solo lectura** para el usuario.

Tenga en cuenta que se le da prioridad a los permisos de inicio de sesión recuperados directamente desde el registro del usuario. Si el usuario no tiene el atributo de permiso de inicio de sesión en el registro, se intentará recuperar los permisos de los grupos a los que pertenece el usuario y, si está configurado, que coincidan con el filtro de grupo. En este caso, al usuario se le asignará el OR inclusivo para todos los bits para todos los grupos. Del mismo modo, el bit **Acceso solo de lectura** solo se establece si todo el resto de los bits son cero. Además, tenga presente que si se establece el bit **Rechazar siempre** para cualquier de los grupos, el usuario no tendrá acceso. El bit **Rechazar siempre** posee precedencia siempre sobre cualquier otro bit.

Nota: Si le otorga a un usuario la capacidad de modificar parámetros de configuración del adaptador básicos, de red o relacionados con la seguridad, debe considerar otorgar a este mismo usuario la capacidad de reiniciar el XClarity Controller (posición de bit 10). De lo contrario, sin esta capacidad, el usuario puede ser capaz de cambiar los parámetros (por ejemplo la dirección IP del adaptador), pero no podrá hacer que surtan efecto.

3. Elija **Habilitar seguridad basada en roles mejorada para usuarios de Active Directory** o no en **Configuración de Active Directory** (si se usa el modo **Usar servidores LDAP para autenticación y autorización**), o configure **Grupos para autorización local** (si se usa el modo **Usar servidores LDAP únicamente para autenticación** (**con autorización local**)).

   - **Habilitación de seguridad basada en roles mejorada para usuarios de Active Directory**

     Si está habilitada la configuración de seguridad avanzada basada en roles, se debe configurar un nombre de servidor libre de formato para que actúe como el nombre de destino para este XClarity Controller en particular. Se puede asociar el nombre de destino con uno o más roles en el servidor de Active Directory mediante el complemento de seguridad basada en roles (RBS). Esto se consigue al crear destinos gestionados y al otorgarles nombres específicos y luego asociarlos a los roles apropiados. Si se configura un nombre en este campo, proporciona la capacidad de definir roles específicos para usuarios y XClarity Controller (destinos) que pertenezcan al mismo rol. Cuando un usuario inicia sesión en el XClarity Controller y se autentica mediante Active Directory, los roles a los que pertenece el usuario se recuperan del directorio. Los permisos asignados al usuario se extraen de los roles que también tienen como miembro un destino cuyo nombre de destino coincida con el nombre de servidor que está configurado aquí, o con un destino que coincida con cualquier XClarity Controller. Múltiples XClarity Controller pueden compartir el mismo nombre de destino. Esto se puede utilizar para agrupar varios XClarity Controller y asignarles el mismo rol (o roles) al usar un destino gestionado único. Cada XClarity Controller puede recibir un nombre exclusivo.

   - **Grupos para autorización local**

     Se configuran nombres de grupos para proporcionar especificaciones de autorización local para grupos de usuarios. A cada nombre de grupo se le pueden asignar permisos (roles) que son iguales como se describe en la tabla arriba. El servidor LDAP asocia usuarios en un nombre de grupo. Cuando el usuario inicia la sesión, se asignan permisos que están asociados a la agrupación al que el usuario pertenece. Los grupos adicionales pueden configurarse al pulsar el icono “+” o se pueden eliminar al pulsar icono “x”.

Configuración de los protocolos de red

Utilice la información en este tema para visualizar o establecer los valores de red de XClarity Controller.

Configuración de los valores de Ethernet

Utilice la información en este tema para ver o cambiar cómo el XClarity Controller se comunica por una conexión Ethernet.

El XClarity Controller utiliza dos controladores de red. Un controlador de red está conectado al puerto de gestión dedicado y el otro controlador de red está conectado al puerto compartido. Cada uno de los controladores de red recibe su propia dirección MAC grabada. Si se va a utilizar DHCP para asignar una dirección IP para el XClarity Controller, cuando un usuario cambia entre los puertos de red o cuando se produce una conmutación por error desde el puerto de red dedicado para el puerto de red compartido, puede asignarse una dirección IP distinta por el servidor DHCP para el XClarity Controller. Se recomienda que, cuando se utiliza DHCP, los usuarios deben utilizar el nombre de host para acceder al XClarity Controller en lugar de usar una dirección IP. Aunque no se cambian los puertos de red de XClarity Controller, el servidor DHCP posiblemente pueda asignar una dirección IP distinta al XClarity Controller cuando caduque la concesión de DHCP, o cuando se reinicia el XClarity Controller. Si un usuario necesita acceder al XClarity Controller utilizando una dirección IP que no se cambia, debe configurarse el XClarity Controller para una dirección IP estática en lugar de DHCP.

Pulse **Red** en **Configuración de BMC** para modificar los valores de Ethernet del XClarity Controller.

Configuración del nombre del host de XClarity Controller

El nombre de host predeterminado de XClarity Controller se genera usando una combinación de la cadena "XCC - " seguida del tipo de máquina del servidor y el número de serie del servidor (por ejemplo "XCC-7X03-1234567890"). Puede cambiar el nombre de host de XClarity Controller al ingresar hasta un máximo de 63 caracteres en este campo. El nombre de host no debe incluir puntos (.) y puede contener solo caracteres alfabéticos, numéricos, guiones y guiones bajos.

Puertos Ethernet

Este valor controla la habilitación de los puertos Ethernet que utiliza el controlador de gestión, incluidos los puertos compartidos y dedicados.

Una vez están **deshabilitados**, no se asignará ninguna dirección IPv4 o IPv6 a todos los puertos Ethernet y se evitarán cambios adicionales a las configuraciones de Ethernet.

Nota: Este valor no afecta a la interfaz USB LAN o al puerto de gestión USB que se encuentra en la parte frontal del servidor. Esas interfaces tienen sus propios valores de habilitación dedicados.

Configurar valores de red IPv4

Para usar la conexión Ethernet IPv4, lleve a cabo los pasos siguientes:

1. Habilite la opción **IPv4**.

   Nota: Deshabilitar la interfaz Ethernet evita el acceso al XClarity Controller desde la red externa.
2. En el campo **Método**, seleccione una de las opciones siguientes:
   - **Obtener IP del DHCP**: XClarity Controller obtendrá su dirección IPv4 de un servidor DHCP.
   - **Utilizar dirección IP estática**: XClarity Controller utilizará el valor especificado por el usuario para su dirección IPv4.
   - **Primero DHCP, luego dirección IP estática**: XClarity Controller intentará obtener su dirección IPv4 desde un servidor DHCP, pero si ese intento falla, XClarity Controller utilizará el valor especificado por el usuario para su dirección IPv4.
3. En el campo **Dirección estática** escriba la dirección IP que desea asignar al XClarity Controller.

   Nota: La dirección IP debe contener cuatro enteros de 0 a 255 sin espacios y separados por puntos. Este campo no se puede configurar si el método se establece como **Obtener IP del DHCP**.
4. En el campo **Máscara de red**, escriba la máscara de subred utilizada por XClarity Controller.

   Nota: La máscara de subred debe contener cuatro enteros de 0 a 255 sin espacios ni puntos consecutivos y separados por puntos. El valor predeterminado es 255.255.255.0. Este campo no se puede configurar si el método se establece como **Obtener IP del DHCP**.
5. En el campo **Puerta de enlace predeterminada**, escriba su enrutador de puerta de enlace de red.

   Nota: La dirección de la puerta de enlace debe contener cuatro enteros de 0 a 255 sin espacios ni puntos consecutivos y separados por puntos. Este campo no se puede configurar si el método se establece como **Obtener IP del DHCP**.

Configurar los valores de Ethernet avanzados

Pulse la pestaña **Ethernet avanzado** para establecer los valores de Ethernet adicionales.

Nota: En un Flex System, un CMM de Flex System gestiona los valores de VLAN y no se pueden modificar desde el XClarity Controller.

Para habilitar el etiquetado de LAN virtual (VLAN) seleccione la casilla de verificación **Habilitar VLAN**. Cuando se habilita VLAN y se configura un Id. de VLAN, XClarity Controller solo acepta paquetes con los Id. de VLAN especificados. Los Id. de VLAN se pueden configurar con los valores numéricos entre 1 y 4094.

Desde la lista **Selección MAC** elija una de las selecciones siguientes:

- Usar dirección MAC grabada

  La opción de dirección MAC grabada es una dirección física única asignada a este XClarity Controller por el fabricante. La dirección es un campo de solo lectura.

- Usar dirección MAC personalizada

  Si se especifica un valor, la dirección administrada localmente anula la dirección MAC grabada. La dirección administrada localmente debe ser un valor hexadecimal entre `000000000000` y `FFFFFFFFFFFF`. Este valor debe estar en la forma de **xx:xx:xx:xx:xx:xx** donde **x** es un número hexadecimal de 0 a 9 o “a” hasta “f”. XClarity Controller no admite el uso de una dirección multidifusión. El primer byte de una dirección multidifusión es un número impar (el bit menos importante se establece en 1); por lo tanto, el primer byte debe ser un número par.

En el campo **Unidad de transmisión máxima**, especifique el tamaño máximo de un paquete (en bytes) para la interfaz de red. El rango de unidad de transmisión máximo es de 60 a 1500. El valor predeterminado para este campo es 1500.

Para usar la conexión Ethernet IPv6, lleve a cabo los pasos siguientes:

Configurar valores de red IPv6

1. Habilite la opción **IPv6**.
2. Puede asignar una dirección IPv6 a la interfaz utilizando uno de los siguientes métodos de asignación:
   - Usar la configuración automática de dirección sin estado
   - Usar la configuración de dirección con estado (DHCPv6)
   - Usar la dirección IP asignada estáticamente

     Notas: Cuando se elige **Utilizar la dirección IP asignada estáticamente**, se le solicitará la siguiente información:

     – Dirección IPv6
     – Longitud del prefijo
     – Puerta de enlace

Configuración de DNS

Utilice la información en este tema para visualizar o cambiar la configuración de sistema de nombres de dominio (DNS) de XClarity Controller.

Nota: En Flex System, los valores de DNS no se pueden modificar en el XClarity Controller. Las configuraciones DNS son manejadas por el CMM.

Pulse **Red** en **Configuración de BMC** para ver o modificar los valores de DNS del XClarity Controller.

Si pulsa la casilla de verificación **Usar servidores de dirección DNS adicionales**, especifique las direcciones IP de hasta tres servidores del sistema de nombres de dominio en la red. Cada dirección IP debe contener enteros de 0 a 255, separados por puntos. Estas direcciones de servidor DNS se añaden en la parte superior de la lista de búsqueda, por lo que la búsqueda de nombre de host se hace en estos servidores antes de que se asigne automáticamente por un servidor DHCP.

Configuración de DDNS

Utilice la información en este tema para habilitar o deshabilitar el protocolo del Sistema de nombres de dominio dinámico (DDNS) del XClarity Controller.

Pulse **Red** en **Configuración de BMC** para ver o modificar los valores de DDNS del XClarity Controller.

Pulse la casilla de verificación **Habilitar DDNS**, para habilitar DDNS. Cuando se habilita el DDNS, el XClarity Controller notifica a un servidor de nombres de dominio cambiar en tiempo real, la configuración del servidor de nombre de dominio activo de los nombres de host configurados en el XClarity Controller, las direcciones u otra información que se almacena en el servidor de nombres de dominio.

Elija una opción de la lista para seleccionar cómo desea que el nombre de dominio del XClarity Controller se seleccione.

- **Usar nombre de dominio personalizado**: puede especificar el nombre de dominio al que pertenece el XClarity Controller.
- **Usar nombre de dominio obtenido a través del servidor DHCP**: el nombre de dominio al que el XClarity Controller pertenece es especificado por el servidor DHCP.

Configuración de Ethernet sobre USB

Utilice la información en este tema para controlar la interfaz de Ethernet sobre USB que se utiliza para la comunicación en banda entre el servidor y el XClarity Controller.

Pulse **Red** en **Configuración de BMC** para ver o modificar los valores de Ethernet sobre USB del XClarity Controller.

Ethernet sobre USB se utiliza para las comunicaciones en banda del XClarity Controller. Pulse la casilla de verificación para habilitar o deshabilitar la interfaz Ethernet sobre USB.

Importante: Si deshabilita Ethernet sobre USB, no es posible realizar una actualización en banda del firmware del XClarity Controller o del firmware de servidor por medio de los programas de utilidad flash de Linux o Windows.

Seleccione el método que el XClarity Controller utiliza para asignar a las direcciones en los puntos finales de la interfaz de Ethernet sobre USB.

- **Usar dirección local de enlace IPv6 para Ethernet sobre USB**: Este método utiliza las direcciones IPv6 basadas en la dirección MAC que se han asignado a los puntos finales de la interfaz de Ethernet sobre USB. Normalmente, la dirección local de enlace IPv6 se genera utilizando la dirección MAC (RFC 4862), pero Windows 2008 y sistemas operativos más recientes del 2016 admiten una dirección IPv6 local de enlace estática en el extremo host de la interfaz. En su lugar, el comportamiento de Windows predeterminado regenera las direcciones locales de enlace aleatorias mientras se ejecuta. Si la interfaz de Ethernet sobre USB del XClarity Controller está configurado para utilizar la modalidad de dirección local de enlace IPv6, varias funciones que utilizan esta interfaz no funcionarán porque el XClarity Controller no conoce qué dirección Windows ha asignado a la interfaz. Si el servidor se está ejecutando Windows usa uno de los métodos de configuración de dirección de Ethernet sobre USB, o deshabilita el comportamiento de Windows predeterminado utilizando este comando: **netsh interface ipv6 set global randomizeidentifiers=disabled**
- **Usar dirección local de enlace IPv4 para Ethernet sobre USB**: Se asigna una dirección IP en el rango 169.254.0.0/16 al XClarity Controller y en el extremo del servidor de la red.
- **Configurar IPv4 para Ethernet sobre USB**: Con este método, especifica las direcciones IP y máscara de red que se asignan al XClarity Controller y al extremo del servidor de la interfaz de Ethernet sobre USB.

Notas:

1. Los valores de configuración de IP del sistema operativo no se utilizan para establecer la dirección IP del SO de la interfaz Ethernet sobre USB, pero se utiliza para notificar a BMC que la dirección IP del sistema operativo de Ethernet sobre USB cambió.
2. Antes de configurar los tres valores de IP para Ethernet sobre USB, debe configurar manualmente la dirección IP del SO de la interfaz de Ethernet sobre USB de su sistema operativo local.

La asignación de los números externos del puerto Ethernet a los números de puerto de Ethernet sobre USB es controlada pulsando la casilla de verificación **Habilitar reenvío de puerto externo de Ethernet a Ethernet sobre USB** y al completar la información de asignación para los puertos que desea reenviar desde la interfaz de red de gestión al servidor.

Configuración de SNMP

Utilice la información en este tema para configurar los agentes SNMP.

Lleve a cabo los pasos siguientes para configurar los valores de alerta SNMP del XClarity Controller.

1. Pulse **Red** en **Configuración de BMC**.
2. Marque el recuadro de selección correspondiente para habilitar la **captura de SNMPv1**, la **captura de SNMPv2** o la **captura de SNMPv3**.
3. Si habilita la **captura de SNMPv1** o la **captura de SNMPv2**, complete los campos siguientes:
   a. En el campo **Nombre de comunidad**, introduzca el nombre de la comunidad; el nombre no puede estar vacío.
   b. En el campo **Host**, introduzca la dirección del host.
4. Si habilita la **captura de SNMPv3**, complete los campos siguientes:
   a. En el campo **ID de motor**, introduzca el ID del motor. El ID del motor no puede estar vacío.
   b. En el campo **Puerto del receptor de capturas**, introduzca el número de puerto. Número de puerto predeterminado es 162.
5. Si habilita las trampas SNMP, seleccione los siguientes tipos de sucesos para los que desea recibir alertas:
   - **Crítico**
   - **Atención**
   - **Sistema**

   Nota: Haga clic en cada categoría importante para seleccionar mejor los tipos de sucesos de subcategoría en los que desea recibir la alerta.

Habilitar o deshabilitar el acceso de red IPMI

Utilice la información en este tema para controlar el acceso de red al XClarity Controller.

Pulse **Red** en **Configuración de BMC** para ver o modificar los valores de IPMI del XClarity Controller. Complete estos campos para ver o para modificar los valores de IPMI:

Acceso de IPMI sobre LAN
Pulse el conmutador para habilitar o deshabilitar el acceso de red IPMI al XClarity Controller.

Importante:

- Si no está usando herramientas o aplicaciones que tienen acceso al XClarity Controller mediante la red usando el protocolo IPMI, se recomienda que se deshabilite el acceso de red a IPMI para una mayor seguridad.

- El acceso de IPMI sobre LAN al XClarity Controller está deshabilitado de manera predeterminada.

Configuración de los valores de red con comandos IPMI

Utilice la información de este tema para configurar los valores de red mediante los comandos IPMI.

Dado que cada valor de red del BMC se configura con solicitudes separadas de IPMI y en ningún orden determinado, el BMC no tiene la vista completa de todos los valores de red hasta que el BMC se reinicie para aplicar los cambios de red pendientes. La solicitud de cambiar un valor de red puede tener éxito en el momento de realizar la solicitud, pero luego se puede determinar que no es válida cuando se piden los cambios adicionales. Si los valores de red pendientes son incompatibles cuando se reinicie el BMC, los valores nuevos no serán implementados. Después de reiniciar el BMC, debe intentar acceder al BMC utilizando los valores nuevos para asegurarse de que se hayan aplicado correctamente.

Habilitación del servicio y asignación de puertos

Utilice la información en este tema para ver o cambiar los números de puertos utilizados por algunos servicios en el XClarity Controller.

Pulse **Red** en **Configuración de BMC** para ver o modificar los valores asignación de puertos del XClarity Controller. Complete estos campos para ver o para modificar las asignaciones de puertos:

Web
El número de puerto es 80. El usuario no puede configurar este campo.

Web sobre HTTPS
En este campo especifique el número de puerto para la web sobre HTTPS. El valor predeterminado es 443.

REST sobre HTTPS
El número de puerto cambiará automáticamente al especificado en el campo de web sobre HTTPS. El usuario no puede configurar este campo.

CIM sobre HTTP
En este campo especifique el número de puerto para CIM sobre HTTP. El valor predeterminado es 5989.

Nota: CIM está deshabilitado de forma predeterminada.

Presencia remota
En este campo especifique el número de puerto para la presencia remota. El valor predeterminado es 3900.

IPMI sobre LAN
El número de puerto es 623. El usuario no puede configurar este campo.

Nota: IPMI está deshabilitado de forma predeterminada.

SFTP
En este campo especifique el número de puerto utilizado para el Protocolo de transferencia de archivos SSH (SFTP). El número de puerto es 115. El usuario no puede configurar este campo.

Nota: IMM.SFTPPortControl=open es necesario para las actualizaciones en banda de OneCLI.

SLP
En este campo especifique el número de puerto utilizado para el SLP. El número de puerto es 427. El usuario no puede configurar este campo.

Notas: Hay dos tipos de servicio que XClarity Controller notifica:

- servicio: hardware de gestión. Lenovo: Lenovo-xclarity-controller
- servicio: wbem

SSDP
El número de puerto es 1900. El usuario no puede configurar este campo.

SSH
En este campo especifique el número de puerto que está configurado para acceder a la interfaz de línea de comandos mediante el protocolo SSH. El valor predeterminado es 22.

Agente de SNMP
En este campo especifique el número de puerto del agente SNMP que se ejecuta en el XClarity Controller. El valor predeterminado es 161. Los valores válidos del número de puerto son de 1 a 65535.

Trampas SNMP
En este campo especifique el número de puerto utilizado para las trampas SNMP. El valor predeterminado es 162. Los valores válidos del número de puerto son de 1 a 65535.

Configuración de restricciones de acceso

Utilice la información en este tema para visualizar o cambiar los valores que bloquean el acceso de direcciones IP o direcciones MAC del XClarity Controller.

Pulse **Red** en **Configuración de BMC** para ver o modificar los valores de control de acceso del XClarity Controller.

Lista de bloqueo y restricción de tiempo

Estas opciones le permiten bloquear determinadas direcciones IP/MAC específicas durante un periodo de tiempo específico.

- **Lista de direcciones IP bloqueadas**
  - Puede especificar hasta tres direcciones IPv4 o intervalos y tres direcciones o intervalos de IPv6 separados por comas, que no se permite que accedan al XClarity Controller. Consulte las ilustraciones de IPv4 abajo:
  - Ejemplo de dirección IPv4 única: 192.168.1.1
  - Ejemplo de dirección IPv4 de red superior: 192.168.1.0/24
  - Ejemplo de rango IPv4: 192.168.1.1–192.168.1.5
- **Lista de direcciones MAC bloqueadas**
  - Puede especificar hasta tres direcciones MAC separados por comas, que no se permite que accedan al XClarity Controller. Por ejemplo: 11:22:33:44:55:66.
- **Acceso restringido (una vez)**
  - Puede programar un intervalo de tiempo de un solo uso en el cual no se puede acceder a XClarity Controller. Para el intervalo de tiempo que se especifica:
  - La fecha y hora de inicio debe ser posterior a la hora actual de XCC.
  - La fecha y hora de término debe ser posterior que la fecha y hora de inicio.
- **Acceso restringido (diario)**
  - Puede programar uno o más intervalos diarios de uso en el cual no se puede acceder a XClarity Controller. Para cada intervalo de tiempo que se especifica:

– La fecha y hora de término debe ser posterior que la fecha y hora de inicio.

Lista de bloqueos desencadenados externamente

Estas opciones le permiten configurar el bloqueo automático de direcciones IP específicas (IPv4 e IPv6) desde las que el cliente intentó iniciar sesión sucesivamente en XClarity Controller con un nombre de usuario o contraseña incorrecto diferente.

El bloqueo automático determinará dinámicamente cuando se producen errores de inicio de sesión excesivos desde una dirección IP específica y bloquea el acceso de la dirección a XClarity Controller durante un periodo de tiempo predeterminado.

- **Número máximo de errores de inicio de sesión desde una IP específica**
  - El número máximo de veces indica el número de errores de inicio de sesión permitidos para un usuario con una contraseña incorrecta desde una dirección IP específica antes de que se bloquee.
  - Si se establece en 0, la dirección IP nunca se bloqueará debido a errores de inicio de sesión.
  - El contador de inicios de sesión erróneos para la dirección IP específica se restablecerá a cero después del inicio de sesión correcto desde esa dirección IP.
- **Periodo de bloqueo para bloquear un IP**
  - Cantidad mínima de tiempo (en minutos) que debe transcurrir antes de que un usuario pueda intentar volver a iniciar sesión desde una dirección IP bloqueada.
  - Si se establece en 0, el acceso desde la dirección IP bloqueada permanecerá bloqueado hasta que el administrador lo desbloquee expresamente.
- **Lista de bloqueo**
  - La lista de bloqueo de la tabla muestra todas las direcciones IP bloqueadas. Puede desbloquear una o todas las direcciones de IP desde la lista de bloqueo.

Configuración de puerto USB del panel frontal a gestión

Utilice la información en este tema para configurar la gestión del puerto USB del panel frontal del XClarity Controller.

En algunos servidores, el puerto USB del panel frontal se puede conmutar para que esté conectado al servidor o al XClarity Controller. La conexión al XClarity Controller está diseñada para utilizarla con un dispositivo móvil que ejecute la aplicación de dispositivos móviles de Lenovo XClarity. Cuando un cable USB está conectado entre el dispositivo móvil y el panel frontal del servidor, se establece la conexión de Ethernet sobre USB entre la aplicación móvil que se ejecuta en el dispositivo y el XClarity Controller.

Pulse **Red** en **Configuración de BMC** para ver o modificar los valores de la gestión del puerto USB del panel frontal de XClarity Controller.

Hay cuatro tipos de valores que se pueden elegir:

Modo de host único
El puerto USB del panel frontal está siempre conectado únicamente al servidor.

Modo de BMC único
El puerto USB del panel frontal está siempre conectado únicamente al XClarity Controller.

Modo compartido: propiedad de BMC
El puerto USB del panel frontal es compartido por el servidor y el XClarity Controller, pero el puerto se cambia al XClarity Controller.

Modo compartido: propiedad de host

El puerto USB del panel frontal es compartido por el servidor y el XClarity Controller, pero el puerto se cambia al host.

Para obtener información adicional sobre cómo acceder a la aplicación móvil, consulte el siguiente sitio:

https://pubs.lenovo.com/lxca/lxca_usemobileapp.html

Notas:

- Si el puerto USB del panel frontal está configurado para el modo compartido, el puerto se conecta al XClarity Controller cuando no recibe alimentación y se conecta al servidor cuando hay alimentación. Cuando recibe alimentación, el control del puerto USB del panel frontal puede cambiarse entre el servidor y el XClarity Controller. En el modo compartido, el puerto también puede cambiar entre el host y el XClarity Controller pulsando y sosteniendo el botón de identificación del panel frontal (para nodos de cálculo puede ser el botón de gestión USB) durante más de 3 segundos.
- Cuando está configurado en modo compartido y el puerto USB está conectado al servidor, el XClarity Controller puede admitir una solicitud de devolver el puerto USB del panel frontal al XClarity Controller. Cuando se ejecuta esta solicitud, el puerto USB del panel frontal seguirá conectado al XClarity Controller hasta que no haya actividad de USB al XClarity Controller para el periodo especificado por el tiempo de espera de inactividad.

Configuración de los valores de seguridad

Utilice la información de este tema para configurar los protocolos de seguridad.

Nota: La configuración mínima de la versión de TLS predeterminado es TLS 1.2, pero puede configurar el XClarity Controller para utilizar otras versiones de TLS si es necesario para sus aplicaciones de navegador o de gestión. Para obtener más información, consulte “Comando tls” en la página 157.

Pulse **Seguridad** en **Configuración de BMC** para acceder y para configurar las propiedades de seguridad, el estado y los valores del XClarity Controller.

Descripción general de SSL

Este tema es una visión general del protocolo de seguridad de SSL.

SSL es un protocolo de seguridad que ofrece privacidad de las comunicaciones. SSL permite que las aplicaciones cliente/servidor pueden comunicarse de una manera que está diseñada para evitar la interceptación, la alteración y la falsificación de mensajes. Puede configurar el XClarity Controller para utilizar el soporte SSL para distintos tipos de conexiones, tales como servidor web seguro (HTTPS), conexión LDAP segura (LDAPS), CIM sobre HTTPS y servidor SSH y gestionar los certificados que se requieren para SSL.

Gestión de certificado SSL

Este tema proporciona información sobre la gestión de certificados que se puede utilizar con el protocolo de seguridad de SSL.

Puede usar SSL con un certificado autofirmado o con un certificado firmado por una tercera entidad de certificación. Usar un certificado autofirmado es el método más sencillo para usar SSL, pero presenta un riesgo de seguridad ligeramente mayor. El riesgo se da porque el cliente SSL no tiene forma de validar la identidad del servidor DDL para la primera conexión que se intente entre el cliente y el servidor. Por ejemplo, es posible que terceros pueden suplantar al servidor web del XClarity Controller e interceptar datos que fluyan entre el verdadero servidor web del XClarity Controller y el navegador web de los usuarios. Si en el momento de la conexión inicial entre el navegador y el XClarity Controller se importa el certificado autofirmado al almacenamiento de certificados del navegador, todas las comunicaciones futuras serán seguras para ese navegador (suponiendo que la conexión inicial no sufrió algún ataque).

Para mayor seguridad, se puede usar un certificado firmado por una entidad de certificación (CA). Para obtener un certificado firmado, deberá seleccionar **Generar solicitud de firma de certificado (CSR)**. Seleccione **Descargar solicitud de firma de certificado (CSR)** y envíe la solicitud de firma de certificado (CSR) a una CA para obtener un certificado firmado. Cuando se reciba el certificado firmado, seleccione **Importar certificado firmado** para importarlo al XClarity Controller.

La función de la CA consiste en verificar la identidad del XClarity Controller. Un certificado contiene firmas digitales para la CA y el XClarity Controller. Si una CA reconocida emite un certificado o si el certificado de la CA ya se ha importado al navegador web, el navegador podrá validar el certificado e identificar correctamente el servidor web de XClarity Controller.

XClarity Controller requiere un certificado para utilizarlo con el servidor HTTPS, CIM sobre HTTPS y el cliente LDAP seguro. Además, el cliente LDAP seguro también requiere que se importe uno o más certificados de confianza. El certificado de confianza se utiliza por el cliente LDAP seguro para identificar positivamente el servidor LDAP. El certificado de confianza es el certificado de la CA que firmó el certificado del servidor LDAP. Si el servidor LDAP utiliza certificados autofirmados, el certificado de confianza puede ser el certificado del propio servidor LDAP. Se deben importar certificados de confianza adicionales si se utiliza más de un servidor LDAP en la configuración.

Gestión de certificados SSL

Este tema proporciona información algunas de las acciones que se pueden seleccionar para la gestión de certificados con el protocolo de seguridad SSL.

Pulse **Seguridad** en **Configuración de BMC** para configurar la gestión de certificados SSL.

Al gestionar los certificados del XClarity Controller, se le presentan las acciones siguientes:

Descargar certificado firmado
Utilice este enlace para descargar una copia del certificado instalado actualmente. El certificado se puede descargar en formato PEM o DER. El contenido del certificado se puede ver mediante una herramienta externa como OpenSSL (www.openssl.org). Un ejemplo de la línea de comandos para ver el contenido de certificado mediante OpenSSL se vería así:

```
openssl x509 -in cert.der -inform DER -text
```

Descargar una solicitud de firma de certificado (CSR)
Utilice este enlace para descargar una copia de la solicitud de firma de certificado. La CSR se puede descargar en formato PEM o DER.

Generar certificado firmado
Generar certificado autofirmado. Después de que se realice la operación, SSL se puede habilitar mediante el nuevo certificado.

Nota: Cuando se realiza la acción **Generar certificado firmado**, se abre una ventana Generar certificado autofirmado para HTTPS. Se le solicitará completar los campos necesarios y opcionales. **Debe** completar los campos necesarios. Una vez que se ha ingresado la información, pulse **Generar** para completar la tarea.

Generar una solicitud de firma de certificado (CSR)
Generar una solicitud de firma de certificado (CSR). Después de que se realice la operación, el archivo de CSR se puede descargar y enviar a una autoridad de certificación (CA) para que se firme.

Nota: Cuando se realiza la acción **Generar solicitud de firma de certificado (CSR)**, se abre una ventana Generar solicitud de firma de certificado para HTTPS. Se le solicitará completar los campos

necesarios y opcionales. **Debe** completar los campos necesarios. Una vez que se ha ingresado la información, pulse **Generar** para completar la tarea.

Importar un certificado firmado
Use esto para importar un certificado firmado. Para obtener un certificado firmado, primero se debe generar una solicitud de firma de certificado (CSR) y se debe enviar a una autoridad de certificación (CA).

Configuración del servidor Secure Shell

Utilice la información en este tema para comprender y habilitar el protocolo de seguridad de SSH.

Pulse **Red** en **Configuración de BMC** para configurar el servidor Secure Shell.

Para utilizar el protocolo SSH, se debe generar una clave primero para habilitar el servidor SSH.

Notas:

- No se requiere ninguna gestión de certificados para usar esta opción.
- XClarity Controller inicialmente creará una clave del servidor SSH. Si desea generar una nueva clave de servidor SSH, pulse **Red** en **Configuración del BMC**; a continuación, pulse **Regenerar clave**.
- Después de completar la acción, debe reiniciar el XClarity Controller para que los cambios entren en vigor.

Acceso a IPMI sobre estilo de controlador de teclado (KCS)

Utilice la información en este tema para controlar el acceso de IPMI sobre el estilo de controlador del teclado (KCS) al XClarity Controller.

XClarity Controller proporciona una interfaz IPMI a través del canal KCS que no requiere autenticación.

Pulse **Seguridad** en **Configuración de BMC** para habilitar o deshabilitar el acceso de IPMI sobre KCS.

Nota: Después de cambiar los valores, debe reiniciar el XClarity Controller para que los cambios entren en vigor.

Importante: Si no está ejecutando herramientas o aplicaciones en el servidor que tiene acceso al XClarity Controller mediante el protocolo IPMI, se recomienda que se deshabilite el acceso IPMI KCS para una mayor seguridad. XClarity Essentials usa la interfaz de IPMI sobre KCS para el XClarity Controller. Si deshabilita la interfaz de IPMI sobre KCS, vuelva a habilitarla antes de ejecutar XClarity Essentials en el servidor. A continuación, deshabilite la interfaz después de haber terminado.

Evitar firmware del sistema de nivel inferior

Utilice la información en este tema para evitar que el firmware del sistema cambie a niveles de firmware más antiguos.

Esta característica le permite decidir si desea permitir que el firmware del sistema vuelva a un nivel de firmware anterior.

Pulse **Red** en **Configuración de BMC** para evitar que el uso de firmware del sistema más antiguo

Para habilitar o deshabilitar esta función, pulse **Red** en **Configuración de BMC**. Cualquier cambio que se realice surtirá efecto inmediatamente sin la necesidad de reiniciar el XClarity Controller.

Declarar presencia física

Utilice la información en este tema para declarar y cancelar la declaración de presencia física desde la página web de XClarity Controller sin estar físicamente presente en el servidor.

Esta característica solo está disponible si se habilita **Política de presencia física** mediante UEFI. Una vez habilitada, puede acceder a la característica de presencia física al pulsar **Seguridad** en **Configuración de BMC**.

Configuración de la administración de claves de seguridad (SKM)

Utilice la información de este tema para crear y gestionar las claves de seguridad.

Este característica utiliza el servidor de administración de claves centralizado para proporcionar claves que desbloquean hardware de almacenamiento y así obtener acceso a datos almacenados en SED en un servidor ThinkSystem. El servidor de administración de claves incluye el servidor de administración de claves SKLM - IBM SED y los servidores de administración de claves KMIP - Thales/Gemalto SED (KeySecure y CipherTrust).

XClarity Controller utiliza la red para recuperar claves desde el servidor de administración de claves; por lo tanto, el servidor de administración de claves debe ser accesible para XClarity Controller. XClarity Controller proporciona el canal de comunicación entre el servidor de administración de claves y el servidor solicitante de ThinkSystem. El firmware de XClarity Controller intenta conectarse con cada servidor de administración de claves configurado y se detiene cuando se establece una conexión satisfactoria.

XClarity Controller establece la comunicación con el servidor de administración de claves si se cumplen las siguientes condiciones:

- Hay uno o más nombres de host de administración de claves/direcciones IP configuradas en XClarity Controller.
- Hay dos certificados (cliente y servidor) para la comunicación con el servidor de administración de claves instalados en XClarity Controller.

Nota: Configure al menos dos servidores de administración de claves (uno principal y uno secundario) con el mismo protocolo para su dispositivo. Si el servidor de administración de claves principal no responde al intento de conexión desde XClarity Controller; los intentos de conexión se inician con los servidores de administración de claves adicionales hasta que se establezca una conexión satisfactoria.

Se debe establecer una conexión de seguridad de la capa de transporte (TLS) entre XClarity Controller y el servidor de administración de claves. XClarity Controller autentica el servidor de administración de claves al comparar el certificado del servidor enviado por el servidor de administración de claves, con el certificado del servidor de administración de claves importado previamente en el repositorio de confianza de XClarity Controller. El servidor de administración de claves autentica a cada XClarity Controller que se comunique con él y verifica que XClarity Controller pueda acceder al servidor de administración de claves. Esta autenticación se logra comparando el certificado de cliente que XClarity Controller presenta, con una lista de certificados de confianza que se almacenan en el servidor de administración de claves.

Por lo menos un servidor de administración de clavesse conectará y el grupo de dispositivo se considera opcional. Se deberá importar el certificado del servidor de administración de claves y se debe especificar el certificado de cliente. De forma predeterminada, se utiliza el certificado HTTPS. Si desea sustituirlo, puede generar uno nuevo.

Nota: Para conectar el servidor KMIP (KeySecure y CipherTrust), se debe generar una solicitud de firma de certificado (CSR), y su nombre común debe coincidir con el nombre de usuario definido en el servidor KMIP. A continuación, se debe importar un certificado que haya sido firmado por la Entidad de certificación (CA) de confianza del servidor KMIP para la CSR.

Configuración de los servidores de administración de claves

Utilice la información en este tema para crear el nombre de host o dirección IP y la información de puerto asociada para el servidor de administración de claves.

La sección Configuración de los servidores de administración de claves consta de los siguientes campos:

Nombre de host o dirección IP
Escriba el nombre de host (si DNS si está habilitado y configurado) o la dirección IP del servidor de administración de claves en este campo. Se pueden añadir hasta cuatro servidores.

Puerto
Escriba el número de puerto del servidor de administración de claves en este campo. Si se deja en blanco este campo, se usa el valor predeterminado de 5696. Los valores válidos del número de puerto son 1 a 65535.

Configuración del grupo de dispositivos

Utilice la información de este tema para configurar el grupo de dispositivos utilizado en el servidor SKLM.

En el servidor SKLM, un grupo de dispositivos le permite a los usuarios gestionar las claves de unidad autocrifrada (SED) en múltiples servidores como un grupo. Un grupo de dispositivos con el mismo nombre también se debe crear en el servidor SKLM.

La sección de grupo de dispositivos contiene el campo siguiente:

Grupo de dispositivos
Un grupo de dispositivos le permite a los usuarios gestionar las claves de las SED en múltiples servidores como un grupo. Un grupo de dispositivos con el mismo nombre también se debe crear en el servidor SKLM. El valor predeterminado para este campo es IBM_SYSTEM_X_SED.

Establecer la gestión de certificados

Este tema proporciona información sobre la gestión de certificados de cliente y de servidor.

Los certificados de cliente y de servidor se utilizan para autenticar la comunicación entre el servidor SKLM y el XClarity Controller situados en el servidor ThinkSystem. En esta sección se explica la gestión de certificados de cliente y de servidor.

Gestión de certificados del cliente

Este tema proporciona información sobre la gestión de certificados de cliente.

Los certificados de cliente se clasifican como uno de los siguientes:

- Un certificado autoasignado de XClarity Controller.
- Un certificado generado de una solicitud de firma de certificado (CSR) del XClarity Controller y firmado (externamente) por una CA tercera.

Un certificado de cliente es necesario para la comunicación con el servidor SKLM. El certificado de cliente contiene firmas digitales para la CA y el XClarity Controller.

Notas:

- Los certificados se preservan a través de las actualizaciones de firmware.
- Si un certificado de cliente no se crea para la comunicación con el servidor SKLM, se utiliza el certificado de servidor HTTPS de XClarity Controller.
- La función de la CA consiste en verificar la identidad del XClarity Controller.

Para crear un certificado de cliente, haga clic en el icono más ( ) y seleccione uno de los siguientes elementos:

- Generar una nueva clave y un certificado autofirmado
- Generar una nueva clave y una solicitud de firma de certificado (CSR)

La acción **Generar una nueva clave y un certificado autofirmado** genera una nueva clave de cifrado privada y un certificado autofirmado. En la ventana Generar una nueva clave y un certificado autofirmado, escriba o seleccione la información en los campos obligatorios y opcionales que se apliquen a su configuración, (consulte la tabla siguiente). Pulse **Aceptar** para generar la clave de cifrado privada y el certificado. Aparece una ventana de progreso que indica que se está generando el certificado autofirmado. Aparece una ventana de progreso que indica cuando el certificado está instalado correctamente.

Nota: La nueva clave de cifrado privada y el certificado sustituye cualquier clave y certificado existentes.

Tabla 3. Generar una nueva clave y un certificado autofirmado

Tabla de dos columnas con los encabezados que documentan los campos obligatorios y opcionales para generar una nueva clave y una acción de certificado autofirmado. La fila inferior abarca ambas columnas.

Campo	Descripción
País[1]	En el elemento de lista, seleccione el país donde reside el BMC físicamente.
Estado o provincia[1]	Escriba el estado o la provincia donde reside el BMC físicamente.
Ciudad o localidad[1]	Escriba la ciudad o la localidad donde reside el BMC físicamente.
Nombre de la organización[1]	Escriba el nombre de la empresa u organización a la que pertenece el BMC.
Nombre de host del BMC[1]	Escriba el nombre de host del BMC que aparece en la barra de la dirección web.
Persona de contacto	Escriba el nombre de la persona de contacto que es responsable del BMC.
Dirección de correo electrónico	Escriba la dirección de correo electrónico de la persona de contacto que es responsable del BMC.
Unidad organizativa	Escriba la unidad en la empresa que posee el BMC.
Apellido	Escriba el apellido de la persona que es responsable del BMC. Este campo puede tener un máximo de 60 caracteres.
Nombre	Escriba el nombre de la persona que es responsable del BMC. Este campo puede tener un máximo de 60 caracteres.
Iniciales	Escriba las iniciales de la persona que es responsable del BMC. Este campo puede tener un máximo de 20 caracteres.
Calificador de DN	Escriba el calificador de nombre distinguido para el BMC. Este campo puede tener un máximo de 60 caracteres.
1. Este es un campo obligatorio.	

Después de que se haya generado el certificado de cliente puede descargar el certificado al almacenamiento en su XClarity Controller seleccionando la acción **Descargar certificado**.

La acción **Generar nueva clave y solicitud de firma de certificado (CSR)** genera una nueva clave de cifrado privada y una CSR. En la ventana Generar una nueva clave y una solicitud de firma de certificado, escriba o seleccione la información en los campos obligatorios y opcionales que se apliquen a su configuración, (consulte la tabla siguiente). Pulse **Aceptar** para generar la nueva clave de cifrado privada y la CSR.

Aparece una ventana de progreso mientras se está generando la CSR y una ventana de confirmación se visualiza ante la correcta finalización. Después de la generación de la CSR debe enviar la CSR a una CA para la firma digital. Seleccione la acción **Descargar solicitud de firma de certificado (CSR)** y pulse **Aceptar** para guardar la CSR en su servidor. Luego podrá enviar la CSR a su CA para la firma.

Tabla 4. Generar una nueva clave y una solicitud de firma de certificado

Tabla de dos columnas con los encabezados que documentan los campos obligatorios y opcionales para generar una nueva clave y una acción de solicitud de firma de certificado. La fila inferior abarca ambas columnas.

Campo	**Descripción**
País[1]	En el elemento de lista, seleccione el país donde reside el BMC físicamente.
Estado o provincia[1]	Escriba el estado o la provincia donde reside el BMC físicamente.
Ciudad o localidad[1]	Escriba la ciudad o la localidad donde reside el BMC físicamente.
Nombre de la organización[1]	Escriba el nombre de la empresa u organización a la que pertenece el BMC.
Nombre de host del BMC[1]	Escriba el nombre de host del BMC que aparece en la barra de la dirección web.
Persona de contacto	Escriba el nombre de la persona de contacto que es responsable del BMC.
Dirección de correo electrónico	Escriba la dirección de correo electrónico de la persona de contacto que es responsable del BMC.
Unidad organizativa	Escriba la unidad en la empresa que posee el BMC.
Apellido	Escriba el apellido de la persona que es responsable del BMC. Este campo puede tener un máximo de 60 caracteres.
Nombre	Escriba el nombre de la persona que es responsable del BMC. Este campo puede tener un máximo de 60 caracteres.
Iniciales	Escriba las iniciales de la persona que es responsable del BMC. Este campo puede tener un máximo de 20 caracteres.
Calificador de DN	Escriba el calificador de nombre distinguido para el BMC. Este campo puede tener un máximo de 60 caracteres.
Contraseña de desafío	Escriba la contraseña a la CSR. Este campo puede tener un máximo de 30 caracteres.
Nombre no estructurado	Escriba información adicional, como el nombre no estructurado que se asigna al BMC. Este campo puede tener un máximo de 60 caracteres.
1. Este es un campo obligatorio.	

La CA firma digitalmente la CSR utilizando la herramienta de procesamiento de certificado del usuario, como la herramienta de línea de comando **OpenSSL** o **Certutil**. Todos los certificados de cliente que se firman utilizando la herramienta de procesamiento de certificado de usuario tienen el mismo certificado **base**. Este certificado **base** también se debe importar al servidor SKLM de modo que todos los servidores firmados digitalmente por el usuario son aceptados por el servidor SKLM.

Después de que la CA ha firmado el certificado, debe importarlo en el BMC. Seleccione la acción **Importar un certificado firmado** y seleccione el archivo para cargar como el certificado de cliente; a continuación, pulse el botón **Aceptar**. Aparece una ventana de progreso que indica que se está cargando el certificado firmado por la CA. Aparece una ventana de carga de certificado si el proceso de carga es satisfactorio. Aparece una ventana de error de carga de certificado si el proceso de carga no es satisfactorio.

Notas:

- Para una mayor seguridad, use un certificado firmado digitalmente por la CA.
- El certificado que se importa al XClarity Controller debe corresponder a la CSR previamente generada.

Después de importar un certificado firmado por la CA al BMC, seleccione la acción **Descargar certificado**. Cuando selecciona esta acción, el certificado firmado por la CA se descarga del XClarity Controller al almacenamiento en su sistema.

Gestión de certificados del servidor

Este tema proporciona información sobre la gestión de certificados de servidor.

El certificado de servidor se genera en el servidor SKLM y se debe importar al XClarity Controller antes de que la funcionalidad de acceso seguro a la unidad funcione. Para importar el certificado que autentica el servidor SKLM con el BMC, pulse **Importar un certificado** en la sección Estado del certificado del servidor de la página Acceso a la unidad. Se visualiza un indicador de progreso a medida que se transfiere el archivo almacenamiento en el XClarity Controller.

Después de que el certificado de servidor se extrae correctamente en el XClarity Controller, el área de estado del certificado del servidor muestra el contenido siguiente: `A server certificate is installed.`

Si desea quitar un certificado de confianza, pulse el botón **Quitar** correspondiente.

Registro de auditoría extendido

Utilice la información de este tema para controlar el registro de auditoría extendido.

Esta función le permite decidir si va a incluir o no las entradas de registro del comando IPMI set (datos sin procesar) desde canales LAN y KCS en el registro de auditoría.

Haga clic en **Seguridad** en **Configuración de BMC** en XCC web para habilitar/deshabilitar el registro de auditoría extendido.

Nota: Si el comando de la configuración IPMI es del canal de LAN, el nombre de usuario y la dirección IP de origen se incluirán en el mensaje de registro. Y se excluyen todos los comandos IPMI con información de seguridad confidencial (por ejemplo, la contraseña).

Configuración de criptografía

Utilice la información de este tema para comprender las distintas configuraciones de criptografía.

Modo de seguridad alta

- Solo admite cifrados muy fuertes y muy fuertes.
- Compatible con NIST.
- Compatible con PFS (Perfect Forward Secrecy).

Modo de compatibilidad

- Admite una amplia gama de cifrados para mayor compatibilidad.

- No compatible con PFS y NIST.

Modo compatible con NIST

- Admite una amplia gama de cifrados para mayor compatibilidad.
- Compatible con NIST.
- Compatible con PFS.

Soporte de versión de TLS

- TLS 1.0 y superior
- TLS 1.1 y superior
- TLS 1.2 y superior
- TLS 1.3

El valor de criptografía de TLS es restringir las suites de cifrado TLS admitidas contra los servicios de BMC.

Consulte la siguiente tabla para ver los distintos valores en los que se admiten las suites de cifrado TLS

Modo de seguridad	Versión TLS	Suites de cifrado TLS
Modo de seguridad alta	TLS 1.3 e inferior	• TLS_AES_256_GCM_SHA384
Modo de seguridad alta	TLS 1.2 e inferior	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
Modo compatible con NIST	TLS 1.3 e inferior	• TLS_AES_256_GCM_SHA384 • TLS_AES_128_GCM_SHA256
Modo compatible con NIST	TLS 1.2 e inferior	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 • TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA256

Modo de seguridad	Versión TLS	Suites de cifrado TLS
Modo de compatibilidad	TLS 1.3 e inferior	• TLS_AES_256_GCM_SHA384 • TLS_AES_128_GCM_SHA256 • TLS_CHACHA20_POLY1305_SHA256
Modo de compatibilidad	TLS 1.2 e inferior	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 • TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA256
Modo de compatibilidad	TLS 1.1 e inferior	• TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA256

Copia de seguridad y restauración de la configuración del BMC

La información de este tema describe cómo restaurar o modificar la configuración del BMC.

Seleccione **Copia de seguridad y restauración** en **Configuración del BMC** para realizar las acciones siguientes:

- Ver un resumen de configuración del controlador de gestión
- Crear copia de seguridad o restaurar la configuración del controlador de gestión
- Ver el estado de copia de seguridad o de restauración
- Restablece la configuración del controlador de gestión a su configuración predeterminada de fábrica
- Accede al asistente de configuración inicial del controlador de gestión

Copia de seguridad de la configuración del BMC

La información de este tema describe cómo crear una copia de seguridad de la configuración del BMC.

Seleccione **Copia de seguridad y restauración** en **Configuración del BMC**. En la parte superior está la sección **Configuración de copia de seguridad de BMC**.

Si se realizó una copia de seguridad anteriormente, verá los detalles en el campo **Última copia de seguridad**.

Para realizar una copia de seguridad de la configuración actual del BMC, siga los pasos siguientes:

1. Especifique la contraseña para el archivo de copia de seguridad del BMC.
2. Seleccione si desea cifrar el archivo o únicamente datos confidenciales.
3. Inicie el proceso de copia de seguridad pulsando **Iniciar copia de seguridad**. Durante el proceso, no podrá realizar ninguna acción de restauración o reinicio.
4. Cuando se completa el proceso, aparecerá un botón para descargar y guardar el archivo.

Nota: Cuando el usuario establece un nuevo usuario y contraseña de XClarity Controller y realiza una copia de seguridad de la configuración, la cuenta y la contraseña predeterminada (`USERID/PASSWORD`) también se incluyen. Si se borra posteriormente la cuenta/contraseña predeterminada desde la copia de seguridad, el sistema mostrará un mensaje que notificar al usuario de que hay un error para restaurar la cuenta/contraseña de XClarity Controller. Usuarios pueden ignorar este mensaje.

Restablecimiento de la configuración del BMC

La información de este tema describe cómo restaurar la configuración del BMC.

Seleccione **Copia de seguridad y restauración** en **Configuración del BMC**. Debajo de **Crear copia de seguridad de la configuración del BMC** está la sección **Restaurar BMC desde el archivo de configuración**.

Para restaurar el BMC a una configuración guardada anteriormente, siga los pasos siguientes:

1. Navegue para seleccionar el archivo de copia de seguridad y escriba la contraseña cuando se le solicite.
2. Verifique el archivo al pulsar **Ver contenido** para ver los detalles.
3. Después de verificar el contenido, pulse **Iniciar la restauración**.

Restablecimiento de BMC a los valores predeterminados de fábrica

La información de este tema describe cómo restablecer el BMC a los valores de fábrica.

Seleccione **Copia de seguridad y restauración** en **Configuración del BMC**. Debajo de **Restaurar BMC desde el archivo de configuración** está la sección **Restablecer el BMC a los valores predeterminados de fábrica**.

Para restablecer el BMC a los valores predeterminados de fábrica, siga los pasos siguientes:

1. Pulse **Comenzar a restablecer el BMC a los valores predeterminados de fábrica**.

   Notas:

   - Solo los usuarios con el nivel de autorización de supervisor pueden realizar esta acción.
   - La conexión Ethernet se desconecta temporalmente. Debe iniciar la sesión en la interfaz web del XClarity Controller de nuevo después de que se realice la operación de restablecimiento.
   - Una vez que pulse **Comenzar a restablecer el BMC a los valores predeterminados de fábrica**, se perderán todos los cambios de configuración anteriores. Si desea habilitar LDAP al restaurar la configuración de BMC, antes de ello debe importar un certificado de seguridad de confianza.
   - Después de que se realice el proceso, el XClarity Controller se reiniciará. Si se trata de un servidor local, su conexión TCP/IP se interrumpe y debe volver a configurar la interfaz de red para restaurar la conectividad.
   - El restablecimiento del BMC a los valores predeterminados de fábrica no afecta a los valores de UEFI.

Reinicio de XClarity Controller

La información de este tema explica cómo reiniciar el XClarity Controller.

Para conocer más detalles sobre cómo reiniciar el XClarity Controller, consulte “Acciones de alimentación” en la página 64

Capítulo 4. Supervisar el estado del servidor

Utilice la información en este tema para comprender cómo ver y supervisar la información del servidor al que va a acceder.

Una vez que se registra en XClarity Controller, se muestra una página de estado del sistema. En esta página, puede ver el estado de hardware del servidor, registros de sucesos y de auditoría, el estado del sistema, el historial de mantenimiento y los destinatarios de alertas.

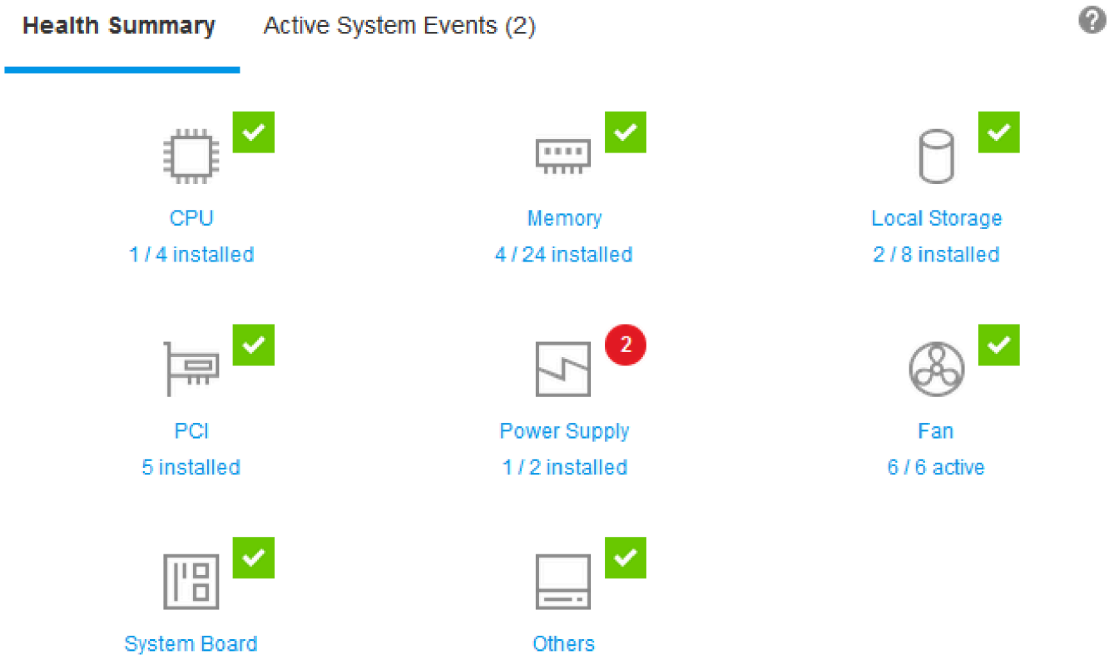
Visualización del resumen de estado/sucesos activos del sistema

Utilice la información de este tema para entender cómo ver el resumen de estado/sucesos activos del sistema.

Cuando accede a la página de inicio del XClarity Controller, **Resumen de estado** se muestra de forma predeterminada. Se proporciona una representación gráfica, que muestra el número de componente de hardware que se han instalado y su estado respectivo. Los componentes de hardware que se están supervisando incluyen:

- Procesador (CPU)
- Memoria
- Almacenamiento local
- Adaptadores PCI
- Fuente de alimentación
- Ventilador
- Placa del sistema
- Otros

Nota: Es posible que el **almacenamiento local** muestre “not available” (no disponible) en el icono de estado en sistemas con una configuración de copia de seguridad de intercambio simple.



Si los componentes de hardware no están funcionando normalmente, se marca por un icono crítico o de aviso. Un estado crítico se indica mediante un icono de círculo rojo, mientras que una condición de advertencia se indica con un icono de triángulo amarillo. Al pasar sobre el icono del mouse sobre la señal crítica o de advertencia, se muestran hasta tres sucesos activos para ese componente.

Para ver los otros sucesos, pulse la pestaña **Sucesos activos del sistema**. Una ventana aparecerá que muestra los sucesos que activos en el sistema. Pulse **Ver todos los registros de sucesos** para ver todo el historial de sucesos.

Si el componente de hardware está marcado con una marca de verificación verde, está funcionando normalmente y no hay sucesos activos.

El texto debajo del componente de hardware indica el número de componentes instalados. Si pulsa el texto, se le dirigirán a la página **Inventario**.

Visualización de la información del sistema

Este tema explica cómo obtener un resumen de información común del servidor.

El panel **Información y valores de sistema** que se encuentra a la izquierda de la página de inicio proporciona un resumen de información común del servidor, que incluye lo siguiente:

- Nombre del equipo, alimentación y estado del sistema operativo
- Tipo/modelo de equipo
- Número de serie
- Nombre de sistema
- Propiedad de USB frontal
- Licencia de BMC
- Dirección IP de BMC
- Nombre de host de BMC
- Versión UEFI
- Versión BMC
- Versión LXPM
- Ubicación

El servidor puede estar en uno de los estados del sistema enumerados en la siguiente tabla.

Tabla 5. Descripciones de estado del sistema

Tabla de dos columnas con encabezados que documentan los estados del sistema del servidor.

Estado	**Descripción**
Alimentación del sistema encendida/estado desconocido	El servidor se apaga.
Sistema encendido/iniciando UEFI	El servidor se enciende, pero UEFI no está funcionando.
Sistema ejecutando UEFI	El servidor se enciende y UEFI está en funcionamiento.
Sistema detenido en UEFI	El servidor está encendido; UEFI ha detectado un problema y ha dejado de funcionar.
Arrancando sistema operativo o en sistema operativo no admitido	El servidor se encuentra en este estado debido a una de las siguientes razones: • El cargador del sistema operativo se ha iniciado; pero el sistema operativo no se ejecuta • La interfaz Ethernet sobre USB del BMC está deshabilitado • El sistema operativo no tiene los controladores cargados que admiten la interfaz Ethernet sobre USB.
Sistema operativo arrancado	El sistema operativo del servidor se está ejecutando.
Suspensión a RAM	El servidor se ha colocado en el estado de espera o de reposo.
El sistema se está ejecutando en la prueba de memoria	El servidor está encendido y está ejecutando herramientas de diagnóstico de memoria.
El sistema está ejecutándose en modo de configuración	El servidor está encendido y el sistema ha arrancado en el menú de configuración F1 de UEFI o menú de LXPM.
El sistema está ejecutándose en el modo de mantenimiento de LXPM	El servidor está encendido y el sistema ha iniciado en el modo de mantenimiento de LXPM en el que los usuarios no pueden navegar en el menú de LXPM.

Si desea cambiar el nombre del sistema, pulse el icono de lápiz. Escriba el nombre del sistema que desea utilizar; a continuación, pulse la marca de verificación verde.

Si desea cambiar la propiedad de USB frontal, pulse el icono de lápiz y seleccione el modo **Propiedad del panel frontal USB** que desea del menú desplegable. A continuación, pulse la marca de verificación verde.

Si el servidor tiene una licencia que no sea la licencia empresarial del XClarity Controller, puede comprar una actualización de la licencia para habilitar funciones ampliadas. Para instalar la licencia de una actualización después de haber obtenido una licencia de actualización, pulse el icono de flecha hacia arriba.

Para agregar, eliminar o exporte una licencia, pulse el icono de flecha hacia la derecha.

Para cambiar los valores de dirección IP del BMC, el nombre de host del BMC, la versión de UEFI, la versión de BMC y los elementos de ubicación, pulse la flecha hacia la derecha.

- Para la dirección IP y el nombre de host, irá a la sección **Configuración de Ethernet** en **Red**.
- Para los elementos de la versión de UEFI y de BMC, irá a la página **Actualización de firmware**.
- Para el elemento de ubicación, irá a la sección **Propiedades del servidor** en la página **Configuración de servidor**.

Visualización del uso del sistema

Al hacer clic en **Utilización** en el panel izquierdo, se proporciona un resumen de información de utilización común del servidor.

Utilización del sistema es una medición compuesta basada en la utilización en tiempo real de los procesadores, la memoria y los subsistemas de E/S. Los datos de utilización se obtienen del lado de ME (administrador de nodo), lo que incluye lo siguiente:

- **Utilización de CPU**
  - Residencia de estado C agregada
  - Tiempo medido en C0 como porcentaje de residencia usada y máxima de C0 (por segundo).
- **Utilización de memoria**
  - Lectura/escritura agregada de todos los canales de memoria.
  - Ancho de banda medida calculada como porcentaje del ancho de banda usada y máxima disponible (por segundo).
- **Utilización de E/S**
  - Volumen de lectura/escritura agregada de los puertos de raíz en el Bus PCIe*.

– Ancho de banda medida calculada como porcentaje del ancho de banda de E/S usada y máxima disponible (por segundo).

Visualización de los registros de sucesos

El **Registro de sucesos** proporciona un listado histórico de todos los sucesos de hardware y de gestión.

Seleccione la pestaña **Registro de sucesos** en **Sucesos** para visualizar la página **Registro de sucesos**. Se marca el tiempo de todos los sucesos en el registro por medio del uso de los valores de fecha y hora del XClarity Controller. Algunos sucesos también generan alertas cuando suceden, si se los configura para hacerlo en **Destinatarios de alerta**. Puede clasificar y filtrar sucesos en el registro de sucesos.

A continuación se encuentra una descripción de las acciones que se pueden realizar en la página **Registro de sucesos**.

- **Personalizar tabla**: seleccione esta acción para elegir el tipo de información que desea mostrar en la tabla. Se puede mostrar un número de secuencia para ayudar a determinar el orden de sucesos cuando hay más de un suceso en la misma hora.

  Nota: Algunos números de secuencia utilizan procesos internos de BMC, de modo que es normal que puede haber espacios en los números de secuencia cuando los sucesos son clasificados por número de secuencia.
- **Borrar registros**: seleccione esta acción para eliminar los registros de sucesos.
- **Actualizar**: seleccione esta acción para actualizar la pantalla con cualquier entrada del registro de sucesos que pueda haberse producido desde la última visualización de la página.
- **Tipo**: seleccione qué tipos de sucesos se van a mostrar. Los tipos de sucesos incluyen lo siguiente:

   Muestra las entradas de errores en el registro

   Muestra las entradas de advertencia en el registro

   Muestra las entradas informativas en el registro

  Pulse cada icono para apagar o encender los tipos de errores que aparecen. Al pulsar el icono varias veces alternará entre mostrar y no mostrar los sucesos. Una caja azul que rodea el icono indica qué tipo de suceso se mostrará.
- **Filtro de tipo de fuente**: seleccione un elemento del menú desplegable para mostrar solo el tipo de entradas de registro de sucesos que desee mostrar.
- **Filtro de tiempo**: seleccione esta acción para especificar el intervalo de los sucesos que desea mostrar.
- **Buscar**: para buscar tipos específicos de sucesos o de palabras clave, pulse el icono de lupa y escriba una palabra para buscar en el cuadro **Buscar**. Tenga en cuenta que la entrada distingue entre mayúsculas y minúsculas.

Nota: El número máximo de entradas del registro de sucesos es 1024. Cuando los registros de sucesos estén llenos, la nueva entrada de registro sobrescribirá automáticamente la más antigua.

Visualización de los registros de auditoría

El **Registro de auditoría** proporciona un historial de las acciones de los usuarios, tales como iniciar sesión en XClarity Controller, crear un usuario nuevo o cambiar la contraseña de un usuario.

Puede usar el registro de auditoría para efectuar el seguimiento y la documentación de la autenticación, de los cambios y las acciones del sistema.

El registro de sucesos y el registro de auditoría admiten acciones similares de mantenimiento y visualización. Para ver la descripción de la pantalla y las acciones de filtrado que se pueden realizar en la página de Registro de auditoría, consulte "Visualización de los registros de sucesos" en la página 55.

Notas:

- Una vez ejecutadas las herramientas de Lenovo en el sistema operativo del servidor, el registro de auditoría puede contener registros que muestran las acciones realizadas por un nombre de usuario (por ejemplo usuario "20luN4SB") que pueda no reconocer. Cuando algunas de las herramientas se ejecutan en el sistema operativo del servidor, puede crear un usuario temporal para acceder al XClarity Controller. La cuenta se crea con un nombre de usuario y una contraseña aleatoria y solo se puede utilizar para acceder al XClarity Controller en la interfaz Ethernet sobre USB interna. La cuenta solo se puede utilizar para acceder a CIM-XML de XClarity Controller y a interfaces SFTP. La creación y la eliminación de esta cuenta temporal se registra en el registro de auditoría al igual que cualquier acción realizada por la herramienta con las credenciales.
- El número máximo de entradas del registro de auditoría es 1024. Cuando los registros de auditoría estén llenos, la nueva entrada de registro sobrescribirá automáticamente la más antigua.

Visualización del historial de mantenimiento

La página **Historial de mantenimiento** incluye información sobre el historial de actualización de firmware, la configuración y la sustitución del hardware.

El contenido del historial de mantenimiento se puede filtrar para mostrar ciertos tipos de sucesos o ciertos intervalos de tiempo.

Nota: El número máximo de entradas del historial de mantenimiento es 250. Cuando los registros del historial de mantenimiento estén llenos, la nueva entrada de registro sobrescribirá automáticamente la más antigua.

Configuración de los destinatarios de las alertas

Para añadir y modificar las notificaciones de correo electrónico y Syslog o los destinatarios de SNMP TRAP, utilice la información de este tema.

A continuación se encuentra una descripción de las acciones que se pueden realizar en la pestaña **Destinatarios de alertas**.

Las siguientes acciones se pueden realizar en la sección de los destinatarios **Correo electrónico/Syslog**.

- **Crear**: seleccione esta acción para crear los nuevos destinatarios adicionales de correo electrónico y de Syslog. Se pueden configurar hasta 12 destinatarios de correo electrónico y Syslog.
  - **Crear destinatario de correo electrónico**: seleccione esta acción para crear un destinatario de correo electrónico.
    - Escriba el nombre y la dirección de correo electrónico del destinatario.

  - Seleccione para habilitar o deshabilitar la notificación de sucesos. Si selecciona deshabilitar, la cuenta seguirá configurada, pero no se enviarán notificaciones por correo electrónico.
  - Seleccione los tipos de sucesos que se notificarán al destinatario. Si pulsa el menú desplegable junto a las etiquetas de categoría Crítico, Atención o Sistema, puede seleccionar o cancelar la selección de las notificaciones para los componentes específicos en la categoría.
  - Puede elegir incluir o no los contenidos del registro de eventos en la alerta de correo electrónico.
  - El índice especifica cuál de las 12 ranuras receptoras se asignan.
  - Aquí puede configurar el servidor de correo electrónico al que se enviarán los sucesos o puede pulsar la acción del servidor SMTP en la parte superior de la sección. Consulte el servidor SMTP a continuación para conocer los detalles de la configuración.
- **Crear destinatario de Syslog**: seleccione esta acción para crear destinatarios de Syslog.
  - Escriba el nombre y la dirección IP o el nombre de host del servidor Syslog.
  - Seleccione para habilitar o deshabilitar la notificación de sucesos. Si selecciona deshabilitar, la cuenta seguirá configurada, pero no se enviarán notificaciones por correo electrónico.
  - El índice especifica cuál de las 12 ranuras receptoras se asignan.
  - Seleccione los tipos de sucesos que se enviarán al servidor Syslog. Si pulsa el menú desplegable junto a las etiquetas de categoría Crítico, Atención o Sistema, puede seleccionar o cancelar la selección de las notificaciones para los componentes específicos en la categoría.

- **Servidor SMTP**: seleccione esta acción para configurar los valores pertinentes para el servidor de correo electrónico de SMTP. Solo se puede configurar un servidor de correo electrónico. Se usa la misma configuración de correo electrónico al enviar alertas a todos los destinatarios de correo electrónico configurados. El BMC cambia automáticamente de una conexión segura a una conexión cifrada para la transferencia de correo usando el comando STARTTLS de forma uniforme a través del puerto 587, si el servidor de correo de destino lo admite.
  - Escriba el nombre de host o la dirección IP y el número de puerto de red del servidor de correo electrónico.
  - Si el servidor de correo electrónico requiere autenticación, seleccione la casilla de verificación **Requiere autenticación** y especifique el nombre de usuario y la contraseña. Seleccione el tipo de autenticación requerido por el servidor de correo electrónico, ya sea un método de desafío y respuesta (**CRAM-MD5**) o de credenciales simples (**LOGIN**).
  - Algunas redes pueden bloquear notificaciones por correo electrónico salientes si el valor de la ruta inversa no es la esperada. De forma predeterminada, XClarity Controller utilizará alertmgr@dominio, donde el dominio es el nombre de dominio como se especifica en la sección del DDNS de la página web de la red del XClarity Controller. Puede especificar su propia información de remitente en lugar de la opción predeterminada.
  - Puede comprobar la conexión con el servidor de correo electrónico para asegurarse de que los valores de correo electrónico se han configurado correctamente. XClarity Controller mostrará un mensaje que indica si la conexión se realiza correctamente o no.
- **Volver a intentar y retrasar**: seleccione esta acción para configurar los valores relevantes para las opciones de reintento y retraso.
  - El límite de reintentos especifica el número de veces que XClarity Controller volverá a intentar enviar una alerta, si el intento inicial falla.
  - El retraso entre las entradas especifica el tiempo que XClarity Controller esperará después de enviar una alerta a un destinatario para enviar una alerta al destinatario siguiente.
  - El retraso entre los intentos especifica el tiempo que XClarity Controller esperará después de un intento fallido antes de volver a intentar enviar la alerta.
- **Protocolo**: seleccione esta acción para configurar los valores pertinentes para el protocolo de conexión.

  - Puede elegir entre el **protocolo TCP** o el **protocolo UDP**, tenga en cuenta que este valor se aplicará a todos los destinatarios de syslog.
- Si se han creado destinatarios de correo electrónico o de Syslog, serán listados en esta sección.
  - Para editar los valores del destinatario de correo electrónico o de Syslog, pulse el icono de lápiz debajo del encabezado de la acción en la fila junto al destinatario que desea configurar.
  - Para eliminar un destinatario de correo electrónico o de Syslog, pulse el icono de papelera de reciclaje.
  - Para enviar una alerta de prueba a un destinatario de correo electrónico o de Syslog, pulse el icono de avión de papel.

Las siguientes acciones se pueden realizar en el segmento de usuario **SNMPv3**.

- **Crear**: seleccione esta acción para crear destinatarios de SNMPv3 TRAP.
  - Seleccione la cuenta de usuario que se debe asociar con SNMPv3 TRAP. La cuenta de usuario debe contener una de las doce cuentas de usuario locales.
  - Especifique el nombre de host o la dirección IP del gestor SNMPv3 que recibirá las SNMPv3 TRAP.
  - XClarity Controller utiliza el algoritmo hash HMAC-SHA para autenticarse con el gestor de SNMPv3. Este es el único algoritmo compatible.
  - La contraseña de privacidad se utiliza con el protocolo de privacidad para cifrar los datos de SNMP.
  - La **Configuración global de SNMPv3** se aplica a todos los destinatarios de SNMPv3 TRAP. Estos valores se pueden configurar al crear un destinatario de SNMPv3 TRAP o pulsando la acción de los valores de SNMPv3 en la parte superior del segmento del usuario **SNMPv3**.
    - Seleccione para habilitar o deshabilitar las SNMPv3 TRAP. Si no está habilitada, la configuración seguirá establecida, pero no se enviarán SNMPv3 TRAP.
    - Se requiere la información de contacto y de ubicación del BMC y se configura en la página web de Propiedades del servidor. Para obtener más información, consulte “Configuración de ubicación y contacto” en la página 83.
    - Seleccione los tipos de sucesos que harán que se envíen TRAP al gestor de SNMPv3. Si pulsa el menú desplegable junto a las etiquetas de categoría Crítico, Atención o Sistema, puede seleccionar o cancelar la selección de las notificaciones para los componentes específicos en la categoría.

  Nota: La transferencia de datos entre el cliente de SNMP y el agente se puede proteger mediante cifrado. Los métodos compatibles para el **protocolo de privacidad** son CBC-DES y AES.
- Si se han creado destinatarios de SNMPv3 TRAP, serán listados en esta sección.
  - Para editar los valores de un destinatario SNMPv3, pulse el icono de lápiz debajo del encabezado de la acción en la fila junto al destinatario que desea configurar.
  - Para eliminar un destinatario de SNMPv3, pulse el icono de papelera de reciclaje.

Capturar los últimos datos de la pantalla de error del SO

Utilice la información de este tema para capturar y ver una pantalla de error del sistema operativo.

La pantalla del sistema operativo se captura automáticamente cuando se produce el tiempo de espera del proceso de vigilancia del SO. Si se produce un suceso que hace que el SO se detenga, se activa la función del proceso de vigilancia del SO y se captura el contenido de la pantalla. XClarity Controller almacena solo una captura de pantalla. Cuando se produce el tiempo de espera del proceso de vigilancia del SO, una nueva captura de pantalla sobrescribe la captura de pantalla anterior. Se debe habilitar el proceso de vigilancia del SO para que se capturen pantallas de error del SO. Para establecer el tiempo de espera del proceso de vigilancia del SO, consulte “Configuración de tiempos de espera de servidor” en la página 83 para obtener información. La característica de captura de pantalla de error del SO está disponible solo con el

nivel de funcionalidad avanzada o empresarial de XClarity Controller. Consulte la documentación de su servidor para obtener información acerca del nivel de funcionalidad del XClarity Controller instalada en el servidor.

Pulse la acción **Última pantalla de error** en la sección **Consola remota** de la página de inicio del XClarity Controller para ver una imagen de pantalla del sistema operativo que se capturó cuando se produjo el tiempo de espera del proceso de vigilancia del SO. La captura también se puede ver pulsando **Servicio** y luego **Última pantalla de error** en la sección **Acción rápida** de la página de inicio. Si el sistema no ha experimentado un tiempo de espera del proceso de vigilancia del SO y no ha capturado una pantalla del SO, se muestra un mensaje que indica que la pantalla de error no se ha creado.

Capítulo 5. Configuración del servidor

Utilice la información de este capítulo para comprender las opciones disponibles para las configuraciones del servidor.

Al configurar el servidor están disponibles las opciones siguientes:

- Adaptadores
- Opciones de arranque
- Política de alimentación
- Propiedades del servidor

Visualización de la información y de los valores de configuración del adaptador

Utilice la información de este tema para ver información sobre los adaptadores instalados en el servidor.

Pulse **Adaptadores** en **Configuración del servidor** para ver información sobre los adaptadores instalados en el servidor.

Notas:

- Si el adaptador no admite la supervisión de estado, no se podrá ver para supervisar o cambiar la configuración. Para revisar la información del inventario de todos los adaptadores PCI instalados, visite la página **Inventario**.

Configuración del modo y orden de arranque del sistema

Para configurar el modo y orden de arranque del sistema, utilice la información de este tema.

Cuando selecciona **Opciones de arranque** en **Configuración del servidor**, puede configurar el modo y el orden de arranque del sistema.

Nota: No se permite que ningún método en banda no autenticado cambie los valores del sistema relacionados con la seguridad. Por ejemplo, el arranque seguro NO debe poder configurar a través de API en banda autenticadas desde el sistema operativo o el shell de UEFI. Esto incluye OneCLI ejecutándose en banda y obtener las credenciales temporales utilizando IPMI, o con cualquier herramienta y API para configurar los valores relacionados con el Arranque seguro, la TPM y la contraseña de configuración de UEFI. Todos los valores relacionados con la seguridad deben requerir una autenticación adecuada con privilegios suficientes.

Para el modo de arranque del sistema, están disponibles las siguientes dos opciones:

Arranque UEFI
Seleccione esta opción para configurar un servidor compatible con Unified Extensible Firmware Interface (UEFI). Si arranca sistemas operativos habilitados para UEFI, esta opción podría reducir el tiempo de arranque, deshabilitando las ROM opcionales de valores heredados.

Arranque heredado
Seleccione esta opción si configura un servidor para que arranque un sistema operativo que requiera firmware heredado (BIOS). Seleccione esta opción solo si arranca sistemas operativos no habilitados para UEFI.

Para configurar el orden de arranque del sistema, seleccione un dispositivo de la lista **Dispositivos disponibles** y pulse la flecha derecha para agregar el dispositivo al orden de arranque. Para eliminar un dispositivo del orden de arranque, seleccione un dispositivo de la lista de orden de arranque y pulse la flecha izquierda para regresar el dispositivo a la lista de dispositivos disponibles. Para cambiar el orden de arranque, seleccione un dispositivo y pulse la flecha arriba o abajo para mover el dispositivo hacia arriba o hacia abajo en prioridad.

Cuando realiza un cambio en el orden de arranque, debe seleccionar una opción de reinicio antes de aplicar el cambio. Las siguientes opciones se encuentran disponibles:

- **Reiniciar el servidor inmediatamente**: Se guardan los cambios del orden de arranque y el servidor se reinicia inmediatamente sin apagar el sistema operativo.
- **Reiniciar el servidor normalmente**: Se guardan los cambios del orden de arranque y el sistema operativo se apaga antes de reiniciar el servidor.
- **Reiniciar manualmente después**: Los cambios del orden de arranque serán guardados, pero no surtirán efecto hasta la próxima vez que se reinicie el servidor.

Configuración de arranque único

Para ignorar temporalmente el arranque configurado y usar en vez el arranque de un dispositivo especificado una vez, use la información de este tema.

Pulse **Opciones de arranque** en **Configuración del servidor** y seleccione un dispositivo del menú desplegable para configurar el dispositivo del que el sistema se rearrancará una sola vez en el siguiente reinicio del servidor. Las siguientes opciones se encuentran disponibles:

Red PXE
Configura el servidor para intentar un arranque de red del entorno de ejecución de prearranque.

Soportes extraíbles principales
El servidor se arranca desde el dispositivo USB predeterminado.

CD/DVD predeterminado
El servidor se arranca desde la unidad de CD/DVD predeterminada.

Configuración del sistema F1
El servidor se arranca en el Lenovo XClarity Provisioning Manager.

Partición de diagnóstico
El servidor se arranca en la sección de diagnóstico del Lenovo XClarity Provisioning Manager.

Unidad de disco duro predeterminada
El servidor se arranca desde la unidad de disco predeterminada.

Soportes remotos principales
El servidor se arranca desde el medio virtual montado.

Sin arranque único
Se utiliza el orden de arranque configurado. No existe una omisión de arranque de una sola vez del orden de arranque configurado.

Cuando cambia el tipo de arranque que se realizará con el dispositivo de arranque de una sola vez, también puede especificar el arranque para sea un arranque heredado o un arranque UEFI. Pulse la casilla de verificación **Preferir arranque heredado** si desea que el arranque sea un arranque de BIOS heredado. Desmarque la casilla si desea un arranque UEFI. Cuando selecciona un cambio de una sola vez al orden de arranque, debe seleccionar una opción de reinicio antes de aplicar el cambio.

- **Reiniciar el servidor inmediatamente**: Se guardan los cambios del orden de arranque y el servidor se reinicia inmediatamente sin apagar el sistema operativo.
- **Reiniciar el servidor normalmente**: Se guardan los cambios del orden de arranque y el sistema operativo se apaga antes de reiniciar el servidor.
- **Reiniciar manualmente después**: Los cambios del orden de arranque serán guardados, pero no surtirán efecto hasta la próxima vez que se reinicie el servidor.

Gestión de alimentación del servidor

Para visualizar la información sobre la gestión de alimentación y realizar funciones de gestión de alimentación, utilice la información de este tema.

Seleccione **Política de alimentación** en **Configuración del servidor** para visualizar la información sobre la gestión de alimentación y realizar funciones de gestión de alimentación.

Nota: En un chasis que contiene un blade o nodos de servidores de alta densidad, la refrigeración y la alimentación del chasis está controlada por el controlador de gestión de chasis en lugar del XClarity Controller.

Configuración de la redundancia de alimentación

Para configurar la redundancia de alimentación, utilice la información de este tema.

Los campos disponibles en la sección de redundancia de alimentación incluyen:

- **Redundante (N+N)**: en este modo, el servidor continuará funcionando en el caso de una pérdida de una fuente de alimentación.
  - **Modo de salida cero**: una vez que se ha habilitado en la configuración redundante, algunas PSU entran automáticamente en el estado en espera bajo condiciones de carga liviana. De esta manera, la alimentación restante proporciona la carga de energía completa para aumentar la eficiencia.
- **Redundante (N+1)**: en este modo, el servidor continuará funcionando en el caso de una pérdida de una fuente de alimentación cuando hay cuatro fuentes de alimentación instaladas.
- **Modo no redundante**: en este modo, no se garantiza que el servidor continuará funcionando con la pérdida de una fuente de alimentación. El servidor se regulará si una fuente de alimentación falla, en un intento por mantenerse funcionando.

Pulse **Aplicar** después de realizar los cambios de la configuración.

Configuración de la política de limitación de alimentación

Para configurar el política de limitación de alimentación, utilice la información de este tema.

Puede elegir habilitar o deshabilitar la función de limitación de alimentación. Si se habilita la limitación de alimentación, se puede hacer una selección para limitar la cantidad de alimentación utilizada por el servidor. Si la limitación de alimentación está deshabilitada, el límite máximo de alimentación usado por el servidor será determinado por la política de redundancia de alimentación. Para cambiar el valor, primero pulse **Restablecer**. Elija el valor preferido; a continuación pulse **Aplicar**.

La limitación de alimentación se puede habilitar mediante medidas de consumo de alimentación de CA o medidas de consumo de alimentación de CC. En el menú desplegable, seleccione el tipo de medición que se utilizará para determinar la limitación de alimentación. Al cambiar entre CA y CC, el número en el control deslizante cambiará por consiguiente.

Hay dos modos de cambiar el valor de limitación de alimentación:

- **Método 1**: Mueva la marca del control deslizante al voltaje deseado para establecer el límite total de alimentación del servidor.
- **Método 2**: Ingrese el valor en el cuadro de entrada. La marca del control deslizante se moverá automáticamente a la posición correspondiente.

Pulse **Aplicar** después de realizar los cambios de la configuración.

Nota: La opción **Políticas de alimentación** no está disponible cuando XClarity Controller está en un chasis que contiene un blade o nodos de servidor de alta densidad. La política de alimentación es controlada por el controlador de gestión de chasis en lugar del XClarity Controller.

Configuración de la política de restauración de alimentación

Para configurar cómo el servidor reacciona cuando se restaura la alimentación después de una pérdida de alimentación, utilice la información de este tema.

Al configurar la política de restauración de alimentación, están disponibles las siguientes tres opciones:

Siempre desactivado
El servidor permanecerá apagado incluso cuando se restaure la alimentación.

Restaurar
El servidor se encenderá automáticamente cuando se restaure la alimentación si el servidor se ha encendido luego que ocurrió la falla de alimentación. De lo contrario, el servidor permanecerá apagado cuando se restaure la alimentación.

Siempre encendido
El servidor se encenderá automáticamente cuando se restablezca la alimentación.

Pulse **Aplicar** después de realizar los cambios de la configuración.

Nota: La opción **Políticas de restauración de alimentación** no está disponible en un chasis que contiene un blade o nodos de servidor de alta densidad. La política de restauración de alimentación es controlada por el controlador de gestión de chasis en lugar del XClarity Controller.

Acciones de alimentación

Consulte la información de este tema para comprender las acciones de alimentación que se pueden hacer que el servidor.

Pulse **Acción de alimentación** en la sección **Acción rápida** de la página de inicio del XClarity Controller.

La siguiente tabla contiene una descripción de las acciones de alimentación y reinicio que se pueden realizar en el servidor.

Tabla 6. Acciones de alimentación y descripciones

Tabla de dos columnas que contiene las descripciones de acciones de alimentación del servidor y reinicio.

Acción de alimentación	Descripción
Encender el servidor	Seleccione este elemento para encender el servidor y para arrancar el sistema operativo.
Apagar el servidor normalmente	Seleccione este elemento para apagar el sistema operativo y el servidor.

Tabla 6. Acciones de alimentación y descripciones (continuación)

Acción de alimentación	Descripción
Apagar el servidor inmediatamente	Seleccione este elemento para apagar el servidor sin apagar el sistema operativo primero.
Reiniciar el servidor normalmente	Seleccione este elemento para apagar el sistema operativo y apagar y volver a encender el servidor.
Reiniciar el servidor inmediatamente	Seleccione este elemento para apagar y volver a encender el servidor inmediatamente sin apagar el sistema operativo primero.
Arrancar el servidor a la configuración de sistema	Seleccione este elemento para encender o rearrancar el servidor y para arrancar automáticamente en la configuración del sistema sin la necesidad de tener que pulsar F1 durante el arranque.
Activar la interrupción no enmascarable (NMI)	Seleccione este elemento para forzar una interrupción no enmascarable (NMI) en un sistema “colgado”. La selección de esta acción permite que el sistema operativo de la plataforma realice un volcado de memoria para que pueda utilizarse con fines de depuración de la condición de bloqueo del sistema. El reinicio automático en el valor de NMI el menú de configuración del sistema F1 determina si el XClarity Controller reiniciará o no el servidor después de NMI.
Planificar acciones de alimentación	Seleccione esta acción para programar acciones de alimentación y reinicio diarias y semanales para el servidor.
Reiniciar el controlador de gestión	Seleccione esta acción para reiniciar el XClarity Controller
Apagar y volver a encender la alimentación de CA del servidor	Seleccione esta acción para encender y apagar el servidor.
Nota: Si el sistema operativo está en el modo de protector de pantalla o bloqueado cuando se intenta apagar el sistema operativo, el XClarity Controller no pueda iniciar un apagado normal. El XClarity Controller realizará un reinicio de hardware o se apagará después de que caduque el intervalo de retraso de apagado, mientras el sistema operativo puede seguir ejecutándose.	

Gestión y supervisión del consumo de alimentación con comandos IPMI

Utilice la información de este tema para gestionar y supervisar el consumo de alimentación mediante los comandos IPMI.

En este tema se explica cómo se puede usar el Intel Intelligent Power Node Manager y la Data Center Manageability Interface (DCMI) para proporcionar una supervisión de alimentación y térmico y una gestión de alimentación basada en políticas para un servidor mediante el uso de los comandos de gestión de alimentación de Intelligent Platform Management Interface (IPMI).

Para los servidores que usan Intel Node Manager SPS 3.0, los usuarios de XClarity Controller pueden usar los comandos de gestión de alimentación de IPMI proporcionados por el Management Engine (ME) de Intel para controlar las funciones del Node Manager y para supervisar el consumo de alimentación del servidor. La gestión de alimentación del servidor también se puede realizar mediante los comandos de gestión de alimentación de DCMI. En este tema se proporcionan ejemplos de comandos de gestión de alimentación de Node Manager y DCMI.

Gestión de alimentación del servidor mediante comandos de gestión de nodo

Utilice la información de este tema para gestionar la alimentación del servidor mediante el gestor del nodo.

El firmware Intel Node Manager no tiene una interfaz externa; por lo tanto, los comandos del Node Manager se deben primero recibir por el XClarity Controller y en seguida enviar al Intel Node Manager. XClarity Controller funciona como una transmisión y un dispositivo de transporte para los comandos IPMI mediante el enlace estándar de IPMI.

Nota: Cambiar las políticas de Node Manager mediante los comandos IPMI de Node Manager puede crear conflictos con la funcionalidad de gestión de alimentación del XClarity Controller. De forma predeterminada, crear un enlace con los comandos de Node Manager está deshabilitado para evitar cualquier conflicto.

Para los usuarios que desean gestionar la alimentación del servidor mediante Node Manager en vez de XClarity Controller, existe un comando IPMI de OEM (función de red: **0x3A**) y (comando: **0xC7**) disponible para su uso.

Para habilitar los comandos IPMI de Node Manager de forma remota, escriba:`ipmitool -H` **<$XClarity_ Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `raw` **0x3a 0xc7 0x01**

Para deshabilitar los comandos IPMI de Node Manager de forma remota, escriba:`ipmitool -H` **<$XClarity_ Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `raw` **0x3a 0xc7 0x00**

La siguiente información corresponde a ejemplos de los comandos de gestión de alimentación de Node Manager.

Notas:

- Al especificar IPMI **canal 0** y una dirección de destino **0x2c**, puede usar la IPMITOOL para enviar comandos al Intel Node Manager para su procesamiento. Un mensaje de solicitud se utiliza para iniciar una acción y un mensaje de respuesta se devuelve al solicitante.
- Los comandos se muestran en los formatos siguientes debido a las limitaciones de espacio.

Supervisión de alimentación mediante el uso de Get Global System Power Statistics, (código de comando 0xC8): Solicitud:`ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `-b` **0x00** `-t` **0x2c** `raw` **0x2E 0xC8 0x57 0x01 0x00 0x01 0x00 0x00** Respuesta:57 01 00 38 00 04 00 41 00 39 00 ec 56 f7 53 5a 86 00 00 50

Limitación de alimentación usando Set Intel Node Manager Policy, (código de comando 0xC1): Solicitud:`ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `-b` **0x00** `-t` **0x2c** `raw` **0x2e 0xC1 0x57 0x01 0x00 0x10 0x01 0xA0 0x00 0x00 0x00 0x60 0xea 0x00 0x00 0x00 0x00 0x1e 0x00**Respuesta:57 01 00

Limitación de alimentación usando Set Intel Node Manager Policy, (código de comando 0xC1): Solicitud:`ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `-b` **0x00** `-t` **0x2c** `raw` **0x2e 0xC1 0x57 0x01 0x00 0x10 0x01 0x00 0x00 0x00 0x00 0x60 0xea 0x00 0x00 0x00 0x00 0x1e 0x00**

Obtener la función de Id. de dispositivo usando Get Intel Management Engine Device ID: Solicitud: `ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `-b` **0x00** `-t` **0x2c** `raw` **0x06 0x01**Respuesta:50 01 03 05 02 21 57 01 00 05 0b 03 40 20 01

Para conocer comandos de Intel Node Manager adicionales, consulte la última publicación de **Especificación de interfaz externa de Intel Intelligent Power Node Manager usando IPMI** en https://businessportal.intel.com.

Gestión de alimentación del servidor mediante comandos DCMI

Utilice la información de este tema para gestionar la alimentación del servidor mediante los comandos DCMI.

El DCMI proporciona las funciones de supervisión y de control que se pueden exponer mediante interfaces estándar del software de gestión. Las funciones de gestión de alimentación del servidor también se pueden realizar mediante los comandos de DCMI.

La siguiente información corresponde a ejemplos de las funciones y de los comando de uso general de gestión de alimentación de DCMI. Un mensaje de solicitud se utiliza para iniciar una acción y un mensaje de respuesta se devuelve al solicitante.

Nota: Los comandos se muestran en los formatos siguientes debido a las limitaciones de espacio.

Get Power Reading: Solicitud:`ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `raw` **0x2c 0x02 0xdc 0x01 0x00 0x00** Respuesta:`dc 39 00 38 00 3b 00 39 00 e3 6f 0a 39 e8 03 00 00 40`

Set Power Limit: Solicitud:`ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **PASSW0RD** `raw` **0x2c 0x04 0xdc 0x00 0x00 0x00 0x00 0xA0 0x00 0xe8 0x03 0x00 0x00 0x00 0x00 0xe8 0x03** Respuesta:`dc`

Get Power Cap: Solicitud:`ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `raw` **0x2c 0x03 0xdc 0x00 0x00** Respuesta:`dc 00 00 00 a0 00 e8 03 00 00 00 00 01 00`

Activate the Power Limit: Solicitud:`ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `raw` **0x2c 0x05 0xdc 0x01 0x00 0x00** Respuesta:`dc`

Deactivate the Power Limit: Solicitud:`ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `raw` **0x2c 0x05 0xdc 0x00 0x00 0x00** Respuesta:`dc`

Nota: Es posible que en algunos servidores, las acciones de excepción del comando **Set Power Limit** no sean compatibles. Por ejemplo, es posible que el parámetro **Apagar el hardware del sistema y registrar sucesos en SEL** no sea compatible.

Para obtener la lista completa de comandos que admite la especificación de DCMI, consulte la versión más reciente de la **Especificación de la interfaz de la gestionabilidad de centros de datos** en https://www.intel.com/content/dam/www/public/us/en/documents/technical-specifications/dcmi-v1-5-rev-spec.pdf.

Funcionalidad de la consola remota

Utilice la información de este tema para entender cómo ver e interactuar remotamente con la consola del servidor.

Puede utilizar la funcionalidad de la consola remota en la interfaz web del XClarity Controller para ver y para interactuar con la consola del servidor. Puede asignar una imagen de disco (archivo ISO o IMG) como una unidad virtual en el servidor. La funcionalidad de la consola remota está disponible con las funciones de nivel avanzado o empresarial de XClarity Controller y solo están disponibles mediante la interfaz web. Debe iniciar sesión en el XClarity Controller con un Id. de usuario que tenga privilegios de acceso de supervisor o de acceso a la consola remota para utilizar las características de la consola remota. Para obtener más información sobre cómo actualizar desde la versión estándar de XClarity Controller a las versiones avanzadas o empresariales de XClarity Controller, consulte “Actualización de XClarity Controller” en la página 6.

Use las funciones de la consola remota para hacer lo siguiente:

- Visualización remota de video con resoluciones de gráficos de hasta 1280 x 1024 a 72 Hz o 75 Hz, independientemente del estado del servidor.

- Acceso remoto al servidor, utilizando el teclado y el ratón desde un cliente remoto.
- Monte los archivos ISO e IMG que se encuentran en el sistema local o en un sistema remoto como unidades virtuales disponibles para ser utilizadas por el servidor.
- Cargue una imagen IMG o ISO a la memoria del XClarity Controller y móntela al servidor como una unidad virtual. Se pueden cargar hasta un máximo de dos archivos con un tamaño máximo de 50 MB en la memoria del XClarity Controller.

Notas:

- Cuando la función de consola remota se inicia en modo multiusuario, (el XClarity Controller con las funciones empresariales configuradas para seis sesiones simultáneas), la función de disco remoto se puede ejecutar solo una sesión a la vez.
- La consola remota puede mostrar solo el video que se genera por el controlador de video en la placa del sistema. Si un adaptador del controlador de video separado está instalado y se usa en lugar del controlador de video del sistema, la consola remota del XClarity Controller no puede mostrar el contenido de video del adaptador añadido.
- Si tiene firewalls en la red, se debe abrir un puerto de red para admitir la función de consola remota. Para ver o cambiar el número de puerto de red utilizado por la función de consola remota, consulte "Habilitación del servicio y asignación de puertos" en la página 35.
- La función de consola remota utiliza HTML5 para mostrar el video del servidor en las páginas web. Para utilizar esta característica, su navegador debe admitir la visualización de contenido de video utilizando los elementos HTML5.
- Si utiliza certificados autofirmados y una dirección IPv6 para acceder al BMC con el navegador Internet Explorer, la sesión de consola remota puede no iniciarse debido a un error del certificado. Para evitar este problema, el certificado autofirmado se puede agregar a las entidades de certificación raíz de confianza de Internet Explorer:
  - Seleccione **Seguridad** en **Configuración de BMC** y descargue el certificado autofirmado.
  - Cambie la extensión del archivo del certificado a *.crt y pulse dos veces el archivo del certificado de la web.
  - Borre la caché del navegador IE11.
  - Pulse **Instalar certificado** para instalar el certificado en el almacén de certificados siguiendo los pasos del Asistente de importación de certificado.

Habilitar la funcionalidad de la consola remota

Este tema proporciona información acerca de la funcionalidad de la consola remota.

Como ya se mencionó, la funcionalidad de la consola remota de XClarity Controller solo está disponible con las funciones de nivel avanzado o empresarial de XClarity Controller. Si no tiene los privilegios para operar la consola remota, verá un icono de cerradura.

Después de comprar y obtener la clave de activación para la actualización de la versión avanzada de XClarity Controller, instálela utilizando las instrucciones que aparece en "Instalación de una clave de activación" en la página 93.

Para utilizar la funcionalidad de la consola remota, realice los pasos siguientes:

1. Pulse la imagen con una flecha blanca diagonal en la sección de la consola remota de la página de inicio del XClarity Controller o de la página web de la consola remota.
2. Seleccione uno de los siguientes modos:
   - Iniciar la consola remota en modo de usuario único
   - Iniciar la consola remota en modo multiusuario

Nota: XClarity Controller con las funciones empresariales admite hasta seis sesiones de video simultáneas en el modo multiusuario.

3. Seleccione si desea permitir o no que otros soliciten enviar una solicitud de desconexión a un usuario de consola remota cuando alguien desee usar la función de consola remota y la función ya esté en uso en el modo de usuario único o cuando el número máximo de usuarios estén usando la función de consola remota en el modo multiusuario. **Sin intervalo de tiempo de respuesta** especifica cuánto tiempo el XClarity Controller esperará antes de automáticamente desconectar el usuario si no se recibe ninguna respuesta a la solicitud de desconexión.
4. Seleccione si desea permitir o no que se registren videos de los últimos tres arranques del servidor.
5. Seleccione si desea permitir o no que se registren videos de los últimos tres bloqueos del servidor.
6. Seleccione si se debe permitir o no la captura de pantalla del error del SO con un error de hardware.
7. Pulse **Iniciar consola remota** para abrir la página de la consola remota en otra pestaña. Cuando todas las sesiones de consola remota posibles están en uso, aparecerá un cuadro de diálogo. En este cuadro de diálogo, el usuario puede enviar una solicitud de desconexión a un usuario de consola remota que ha habilitado el valor de **Permitir que otros pidan mi desconexión de sesión remota**. El usuario puede aceptar o rechazar la solicitud de desconexión. Si el usuario no responde dentro del intervalo especificado por el valor **Sin intervalo de tiempo de respuesta**, la sesión del usuario se finalizará automáticamente por el XClarity Controller.

Control de alimentación remoto

Este tema explica cómo enviar comandos de alimentación y reinicio del servidor desde la ventana de la consola remota.

Puede enviar comandos de encendido y reinicio del servidor desde la ventana de la consola remota sin tener que regresar a la página web principal. Para controlar la alimentación del servidor con la consola remota, pulse **Alimentación** y seleccione uno de los siguientes comandos:

Encender el servidor
Seleccione este elemento para encender el servidor y para arrancar el sistema operativo.

Apagar el servidor normalmente
Seleccione este elemento para apagar el sistema operativo y el servidor.

Apagar el servidor inmediatamente
Seleccione este elemento para apagar el servidor sin apagar el sistema operativo primero.

Reiniciar el servidor normalmente
Seleccione este elemento para apagar el sistema operativo y apagar y volver a encender el servidor.

Reiniciar el servidor inmediatamente
Seleccione este elemento para apagar y volver a encender el servidor inmediatamente sin apagar el sistema operativo primero.

Arrancar el servidor a la configuración de sistema
Seleccione este elemento para encender o rearrancar el servidor y para arrancar automáticamente en la configuración del sistema sin la necesidad de tener que pulsar F1 durante el arranque.

Captura de pantalla de consola remota

Utilice la información de este tema para entender cómo utilizar la función de captura de pantalla de consola remota.

La característica de captura de pantalla en la ventana de consola remota captura el contenido de visualización en video del servidor. Para capturar y guardar una imagen de pantalla, lleve a cabo los pasos siguientes:

Paso 1. En la ventana de la consola remota, pulse **Capturar pantalla**.

Paso 2. En la ventana emergente, pulse **Guardar archivo** y pulse **Aceptar**. El archivo tiene el nombre rpviewer.png y se guarda en su carpeta de descarga predeterminada.

Nota: La imagen de captura de pantalla se guarda como tipo de archivo PNG.

Soporte del teclado con consola remota

En la ventana de la consola remota en **Teclado**, se proporcionan los siguientes elementos de opción:

- Pulse **Teclado virtual** para iniciar el teclado virtual. Esta función es útil si está utilizando un dispositivo de tableta que no tiene un teclado físico. Las siguientes opciones se pueden utilizar para crear los macros y las combinaciones de teclas que se enviarán al servidor. El sistema operativo en el sistema del cliente que está usando puede atrapar ciertas combinaciones de teclas (por ejemplo Ctrl+Alt+Del), en vez de transmitirlas al servidor. Otras teclas, tales como F1 o Esc, se pueden interceptar por el programa o el navegador que esté utilizando. Los macros proporcionan un mecanismo para enviar combinaciones de teclas al servidor que el usuario no pueda enviar.
- Pulse **Macros del servidor** para utilizar los macros definidos por el servidor. Algunos macros del servidor quedan predefinidos por el firmware del XClarity Controller. Otros macros definidos por el servidor se pueden definir utilizando Lenovo XClarity Essentials y descargarlos del XClarity Controller. Estos macros se definen para todos los usuarios de la función de consola remota.
- Pulse **Configurar** para añadir o retirar macros definidos por el usuario. Los macros definidos por el usuario se definen solo para el usuario actual de la consola remota. Otros usuarios de la consola remota no verán macros definidos por el usuario de cada uno.
  - Pulse el icono Agregar macros y presione las secuencias de teclas que desee; a continuación, pulse **Añadir** para añadir un nuevo macro.
  - Para eliminar un macro definido por el usuario, seleccione el macro de la lista y pulse el icono de papelera de reciclaje.
  - Para enviar un macro definido por el usuario al servidor, seleccione la opción **Macros definidos por el usuario** y pulse el macro que desea enviar.

Soporte del mouse de la consola remota

Utilice esta información para entender las opciones del mouse con control remoto.

La ventana de la consola remota ofrece varias opciones para el control del mouse, incluido el control de mouse absoluto, el control de mouse relativo (sin aceleración) y el control de mouse (RHEL, Linux más antiguo).

Control absoluto y relativo del mouse

Utilice esta información para acceder a las opciones absolutas y relativas para controlar el mouse.

Para acceder a las opciones absolutas y relativas para controlar el mouse, realice los siguientes pasos:

Paso 1. En la ventana de la consola remota, pulse **Mouse**.

Paso 2. Pulse **Configuración del mouse** el menú desplegable.

Paso 3. Seleccione uno de los siguientes modos de **Aceleración del mouse**:

Posicionamiento absoluto (Windows, Linux más reciente y Mac OS X)
El cliente envía los mensajes de ubicación del mouse al servidor que en relación con el origen (área superior izquierda) del área de visualización.

Posicionamiento relativo, sin aceleración
El cliente envía la ubicación del mouse como desplazamiento desde la posición anterior del mouse.

Posicionamiento relativo (Linux antiguo)
Este modo aplica un factor de aceleración para alinear mejor el mouse en algunos destinos de Linux. Los valores de aceleración se han seleccionado para maximizar la compatibilidad con distribuciones de Linux más antiguas.

Grabación/reproducción de video en pantalla

Utilice la información de este tema para grabar o reproducir videos de la pantalla de presencia remota.

La interfaz web de XClarity Controller proporciona una función de tipo DVR que admite la grabación y la reproducción de los videos de la pantalla de presencia remota. Esta función solo admite la grabación de video en una carpeta de red. Actualmente, se admiten los protocolos NFS y CIFS. A continuación se describen los pasos para utilizar la función de grabación y reproducción.

1. En la página web de la consola remota, haga clic en **Grabación de pantalla** para abrir la ventana de configuración.
2. En la ventana de configuración, es posible que tenga que especificar la siguiente información.
   - Si se selecciona el tipo de montaje “CIFS”, especifique la **Carpeta remota**, el **Nombre de usuario** y los parámetros de **Contraseña**. El formato de la carpeta remota CIFS es “**//<dirección IP remota>/<nombre de la carpeta>**”. Por ejemplo: //xxx.xxx.xxx.xxx/carpeta.
   - Si se selecciona el tipo de montaje “NFS”, especifique los parámetros de **Carpeta remota**. El formato de la carpeta remota NFS es “**<dirección IP remota>:/<nombre de carpeta>**”. Por ejemplo: xxx.xxx.xxx.xxx:/carpeta.
   - Especifique el nombre del archivo de video, de ser necesario. Si ya se proporcionó un nombre de archivo, se mostrará un cuadro de mensaje de error. Para sobrescribir el nombre de archivo existente, elija “Sobrescribir nombre de archivo”. Si el cuadro “Auto” está marcado, el nombre del archivo de video se genera automáticamente.
   - “Tamaño máximo de archivo” denota el tamaño máximo del archivo de video antes de que la grabación de video se detenga automáticamente.
   - “Duración máxima de grabación” denota la duración máxima de la grabación de video antes de que la grabación se detenga automáticamente.
3. Haga clic en **Iniciar grabación** para iniciar la grabación de video.
4. Haga clic en **Detener grabación** para detener la grabación de video. Aparecerá una ventana emergente que indica “Grabación de video completada”, que muestra la información de grabación de video relevante.
5. Descargue los videos grabados de NFS o CIFS a su carpeta local. En la sección vista previa de la consola remota de la página de inicio de XClarity Controller, haga clic en **Videos grabados** y seleccione el archivo de video para reproducir.

Modos de pantalla de consola remota

Utilice la información de este tema para configurar los modos de la pantalla de consola remota.

Para configurar los modos de pantalla de la consola remota, pulse **Modo de pantalla**.

Las siguientes opciones de menú están disponibles:

Pantalla completa

Este modo llena el escritorio del cliente con la visualización en video. Si presiona la tecla Esc en este modo saldrá del modo de pantalla completa. Dado que el menú de la consola remota no se podrá ver en modo de pantalla completa, tendrá que salir del modo de pantalla completa para utilizar las características proporcionadas en el menú de la consola remota, como los macros del teclado.

Ajustar a pantalla
Este es el valor predeterminado cuando se inicia la consola remota. En esta configuración, el escritorio de destino se muestra por completo sin barras de desplazamiento. Se mantiene la relación de aspecto.

Pantalla de escalamiento
Con la escalabilidad habilitada, se ajusta la imagen de video para escalar la imagen completa para llenar la ventana de la consola.

Pantalla de origen
La imagen de video tiene las mismas dimensiones que el servidor final. Las barras de desplazamiento se visualizan si es necesario para permitir la visualización de las áreas de la imagen de video que no caben dentro de la ventana.

Modo de color
Ajusta la intensidad de color de la ventana de la consola remota. Hay dos opciones de modo de color:

- Color: 7, 9, 12, 15 y 23 bit
- Escala de grises: 16, 32, 64, 128 tonalidades

Nota: Generalmente, los ajustes del modo de color se realizan si su conexión con el servidor remoto posee un ancho de banda limitado y desea reducir la demanda de ancho de banda.

Métodos de montaje de medios

Utilice la información de este tema para comprender cómo realizar el montaje de medios.

Hay tres mecanismos proporcionados para montar los archivos ISO e IMG como unidades virtuales.

- Las unidades virtuales se pueden agregar al servidor desde una sesión de consola remota pulsando **Soportes**.
- Directamente desde la página web de la consola remota, sin establecer una sesión de consola remota.
- Herramienta independiente

Los usuarios necesitan contar con privilegios de **Acceso a Consola remota y Disco remoto** para usar las funciones del medio virtual.

Los archivos se pueden montar como medios virtuales desde el sistema local o desde un servidor remoto y se pueden acceder mediante la red o se pueden cargar en la memoria de XClarity Controller mediante la función de RDOC. Estos mecanismos se describen más abajo.

- Las medios locales son los archivos ISO e IMG que se encuentran en el sistema que está utilizando para acceder al XClarity Controller. Este mecanismo está disponible únicamente mediante la sesión de consola remota, no directamente desde la página web de la consola remota y está disponible con las características de XClarity Controller Enterprise. Para montar medios locales, pulse **Activar** en la sección **Montar medio local**. Se pueden montar hasta cuatro archivos concurrentemente en el servidor.

  Notas:

  – Al utilizar el explorador Google Chrome, estará disponible una opción de montaje adicional denominada **Montar archivos/carpetas**, la cual le permitirá arrastrar y soltar los archivos o carpeta.

  - Si hay varias sesiones simultáneas de consola remota en marcha con un XClarity Controller, esta función se puede activar únicamente por una de las sesiones.
- Los archivos que están ubicados en un sistema remoto también se pueden montar como medios virtuales. Se pueden montar hasta cuatro archivos simultáneos como unidades individuales. El XClarity Controller admite estos protocolos para compartir archivos:
  - **CIFS: Sistema de archivos de Internet común**:
    - Escriba la URL que ubica el archivo en el sistema remoto.
    - Si desea que el archivo se presente al servidor como medio virtual de solo lectura, marque la casilla de verificación.
    - Especifique las credenciales necesarias para que el XClarity Controller acceda al archivo en el sistema remoto.

      Nota: El XClarity Controller no admite espacios en el nombre de usuario, contraseña o URL. Asegúrese de que el servidor CIFS no tenga credenciales de inicio de sesión configuradas con un espacio en el nombre o la contraseña de usuario y que la URL no contiene un espacio.
    - Las opciones de montaje son opcionales y las define el protocolo CIFS.
    - Si el servidor remoto pertenece a un grupo de servidores, donde la seguridad se gestiona centralmente, especifique el nombre de dominio al que pertenece el servidor remoto.
  - **NFS: Network File System**:
    - Escriba la URL que ubica el archivo en el sistema remoto.
    - Si desea que el archivo se presente al servidor como medio virtual de solo lectura, marque la casilla de verificación.
    - Las opciones de montaje son opcionales y las define el protocolo NFS. Se admiten tanto NFSv3 y NFSv4. Por ejemplo, para usar NFSv3, se debe especificar la opción “nfsvers = 3”. Si el servidor NFS utiliza el tipo de seguridad AUTH_SYS para autenticar operaciones de NFS, debe especificar la opción “sec=sys”.
  - **HTTPFS: Sistema de archivos HTTP basado en FUSE**:
    - Escriba la URL que ubica el archivo en el sistema remoto
    - Si desea que el archivo se presente al servidor como medio virtual de solo lectura, marque la casilla de verificación.

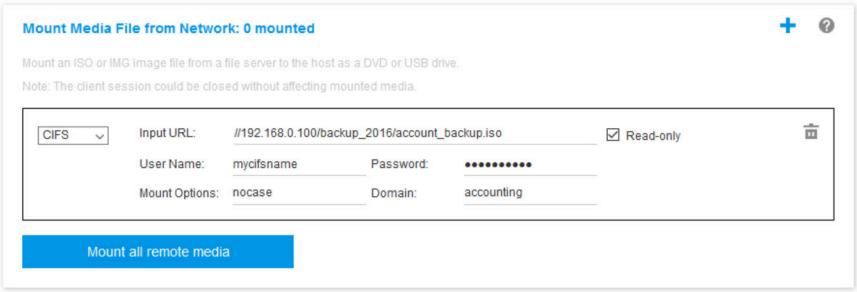
      Nota: Pueden producirse errores durante el proceso de montaje de los certificados de seguridad generados por Microsoft IIS. Si esto ocurre, consulte “Problemas de error de montaje de medios” en la página 81.

  Pulse **Montar todos los medios remotos** para montar el archivo como un medio virtual. Para quitar el medio virtual, pulse el icono de papelera de reciclaje a la derecha del medio montado.
- Se pueden cargar hasta dos archivos en la memoria del XClarity Controller y montar como medio virtual mediante la característica de RDOC del XClarity Controller. El tamaño total para ambos archivos no debe exceder 50 MB. Estos archivos se mantendrán en la memoria del XClarity Controller hasta que se eliminan, incluso si se termina la sesión de consola remota. La función RDOC admite estos mecanismos al cargar archivos:
  - **CIFS: Sistema de archivos de Internet común**: consulte la descripción arriba para obtener detalles.

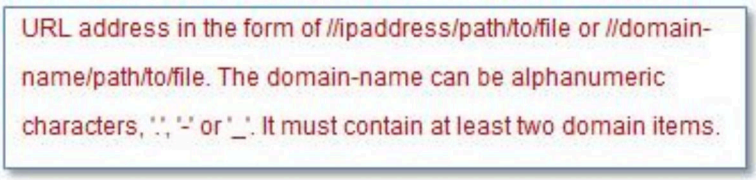
    Ejemplo:

    Para montar un archivo ISO denominado account_backup.iso que se encuentra en el directorio backup_2016 de un servidor CIFS en la dirección IP 192.168.0.100 como una unidad virtual de solo lectura en el servidor, debe rellenar los campos, como se muestra en la siguiente figura. En este ejemplo, el servidor que se encuentra en 192.168.0.100 es miembro de un grupo de servidores en el

dominio “accounting”. El nombre de dominio es opcional. Si su servidor CIFS no forma parte de un dominio, deje el campo **Dominio** en blanco. Se ha especificado la opción de montaje CIFS “nocase” en el campo **Opciones de montaje** en este ejemplo para indicarle al servidor CIFS que se debe omitir la comprobación de mayúsculas y minúsculas del nombre de archivo. El campo **Opciones de montaje** es opcional. El BMC no utiliza la información especificada por el usuario en este campo y simplemente se envía al servidor CIFS cuando se realiza la solicitud de montaje. Consulte la documentación de implementación del servidor CIFS para determinar qué opciones son compatibles con el servidor CIFS.



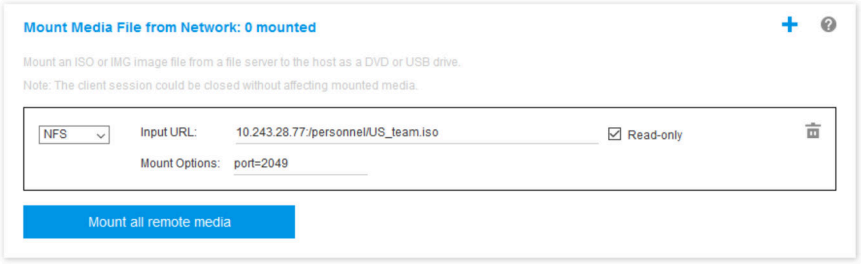
El BMC proporciona directrices cuando se especifica la URL. Si la URL que se introducen no es válida, el botón de montaje estará desactivado y se mostrará texto en rojo en el campo de la URL donde se muestra el formato esperado para la URL.



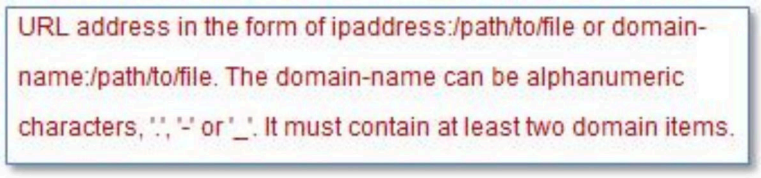
– **NFS: Sistema de archivos de red**: consulte la descripción arriba para obtener detalles.

Ejemplo:

Para montar un archivo ISO denominado US_team.iso que se encuentra en el directorio “personnel” de un servidor NFS en la dirección IP 10.243.28.77 como una unidad virtual de solo lectura en el servidor, debe rellenar los campos, como se muestra en la siguiente figura. La opción de montaje “puerto=2049” de NFS especifica que el puerto de red 2049 debe utilizarse para transferir los datos. El campo **Opciones de montaje** es opcional. La información especificada por el usuario en este campo se envía al servidor NFS cuando se realiza la solicitud de montaje. Consulte la documentación de implementación del servidor NFS para determinar qué opciones son compatibles con el servidor NFS.



El BMC proporciona directrices cuando se especifica la URL. Si la URL que se introducen no es válida, el botón de montaje estará desactivado y se mostrará texto en rojo en el campo de la URL donde se muestra el formato esperado para la URL.

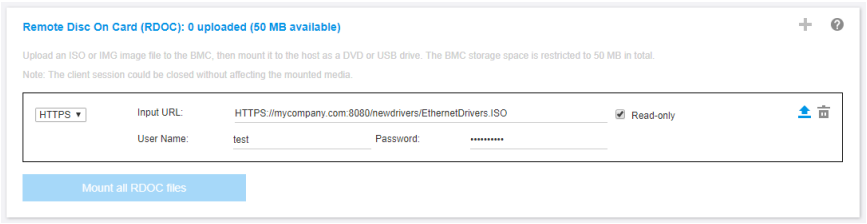


- **HTTPS – Protocolo seguro de transferencia de hipertexto**:
  - Escriba la URL que ubica el archivo en el sistema remoto.
  - Si desea que el archivo se presente al servidor como medio virtual de solo lectura, marque la casilla de verificación.
  - Especifique las credenciales necesarias para que el XClarity Controller acceda al archivo en el sistema remoto.

  Notas:

  - Pueden producirse errores durante el proceso de montaje de los certificados de seguridad generados por Microsoft IIS. Si esto ocurre, consulte “Problemas de error de montaje de medios” en la página 81.
  - El XClarity Controller no admite espacios en el nombre de usuario, contraseña o URL. Asegúrese de que el servidor CIFS no tenga credenciales de inicio de sesión configuradas con un espacio en el nombre o la contraseña de usuario y que la URL no contiene un espacio. **Ejemplo**:

    Para montar un archivo ISO denominado EthernetDrivers.ISO que se encuentra en el directorio “newdrivers” de un servidor HTTPS con el nombre de dominio “mycompany.com” mediante el puerto de red 8080 como una unidad virtual de solo lectura en el servidor, debe rellenar los campos, como se muestra en la siguiente figura.

    El BMC proporciona directrices cuando se especifica la URL. Si la URL que se introducen no es válida, el botón de montaje estará desactivado y se mostrará texto en rojo en el campo de la URL donde se muestra el formato esperado para la URL.

    URL address in the form of https://ipaddress[:port]/path/to/file or HTTPS://domain-name[:port]/path/to/file. The domain-name can be alphanumeric characters, '.', '-' or '_'. It must contain at least two domain items. The port number is optional

- **SFTP: Protocolo de transferencia de archivos SSH**
  - Escriba la URL que ubica el archivo en el sistema remoto.
  - Si desea que el archivo se presente al servidor como medio virtual de solo lectura, marque la casilla de verificación.
  - Especifique las credenciales necesarias para que el XClarity Controller acceda al archivo en el sistema remoto.

  Notas:

- El XClarity Controller no admite espacios en el nombre de usuario, contraseña o URL. Asegúrese de que el servidor CIFS no tenga credenciales de inicio de sesión configuradas con un espacio en el nombre o la contraseña de usuario y que la URL no contiene un espacio.
- Cuando el XClarity Controller se conecta a un servidor HTTPS, aparecerá una ventana emergente que muestra información del certificado de seguridad utilizado por el servidor HTTPS. El XClarity Controller no puede verificar la autenticidad del certificado de seguridad.

– **LOCAL: Sistema de archivos de Internet común**:
  - Examine su sistema en busca del archivo ISO o IMG que desea montar.
  - Si desea que el archivo se presente al servidor como medio virtual de solo lectura, marque la casilla de verificación.

Pulse **Montar todos los archivos RDOC** para montar el archivo como un medio virtual. Para quitar el medio virtual, pulse el icono de papelera de reciclaje a la derecha del medio montado.

Herramienta independiente

Para los usuarios que requieren el montaje de los dispositivos o imágenes (.iso / .img) utilizando XClarity Controller, los usuarios pueden utilizar la parte de código rdmount independiente del paquete OneCLI. En particular, rdmount abrirá una conexión con XClarity Controller y montará el dispositivo o imágenes en el host.

rdmount tiene la siguiente sintaxis:

```
rdmount -s ip_address -d <iso or device path> -l <userid> -p <password> -w port (443)
```

Ejemplo para montar un archivo iso:

```
$sudo ./rdmount -s 10.243.11.212 -d /home/user/temp/SLE-15-Installer-DVD-x86_64-RC2-DVD1.iso -l userid -p password -w 443
```

Disco remoto utilizando el cliente Java

En esta sección se describe cómo montar los soportes locales utilizando el cliente Java.

Puede utilizar el cliente Java para asignar al servidor una unidad de CD o DVD, una unidad de disquetes, una unidad flash USB que se encuentra en su equipo, o puede especificar una imagen de disco en su sistema para que el servidor la utilice. Puede utilizar la unidad para funciones como el reinicio (arranque) del servidor, la actualización de código, la instalación de nuevo software en el servidor y la instalación o actualización del sistema operativo en el servidor. Puede acceder al disco remoto. Las unidades y las imágenes de disco se muestran como unidades USB en el servidor.

Notas: La consola remota Java admite uno de los siguientes entornos Java y solo se puede abrir si el cliente HTML5 no se está ejecutando.

1. Oracle Java Runtime Environment 1.8/Java SE 8 o versiones más recientes
2. OpenJDK 8. Se admite la distribución de AdoptOpenJDK con HotSpot JVM.

Si utiliza AdoptOpenJDK, debe usar https://openwebstart.com/ en OSX, Windows y Linux.

Creación de un archivo de imágenes

Para crear un archivo de imagen nuevo desde una carpeta de origen especificada, lleve a cabo los pasos siguientes:

1. Haga clic en la opción **Crear imagen** en la pestaña **Medio virtual** en la ventana de Cliente de Java de medio virtual. Se muestra la ventana Crear imagen desde carpeta.

2. Haga clic en el botón **Examinar** asociado con el campo **Carpeta de origen** para seleccionar la carpeta de origen específica.
3. Haga clic en el botón **Examinar** asociado con el campo **Nuevo archivo de imagen** para seleccionar el archivo de imagen que se va a utilizar.
4. Haga clic en el botón **Crear imagen**.

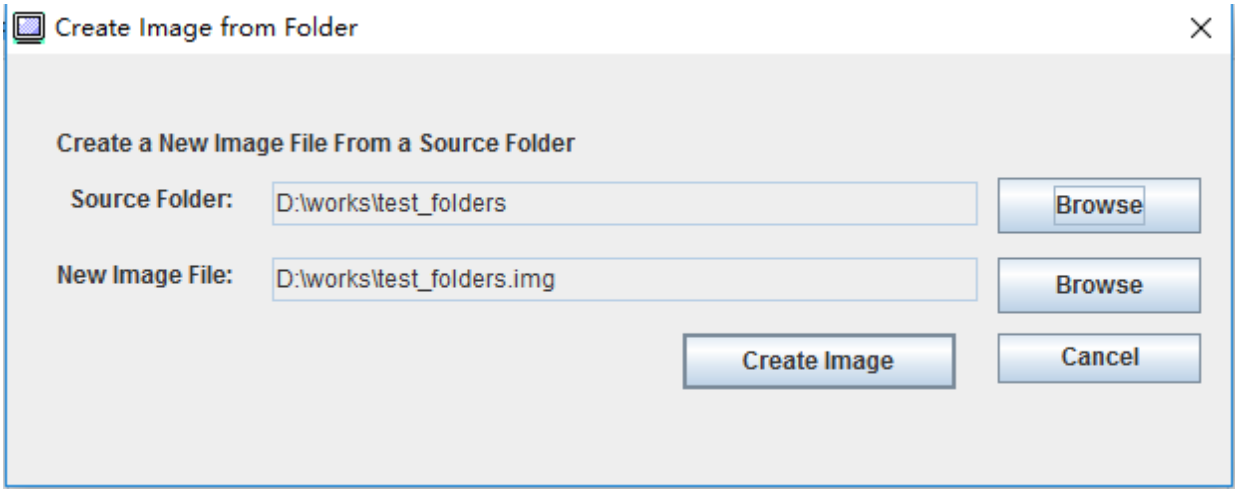


Figura 1. Creación de un archivo de imágenes

Selección de los dispositivos que se van a montar

Para montar la imagen local, la carpeta y la unidad de CD/DVD/USB, lleve a cabo los pasos siguientes:

Haga clic en la opción **Seleccionar dispositivos para montar** en la pestaña **Medio virtual** en la ventana de Cliente de Java de medio virtual. Se muestra la ventana Seleccionar dispositivos para montar.

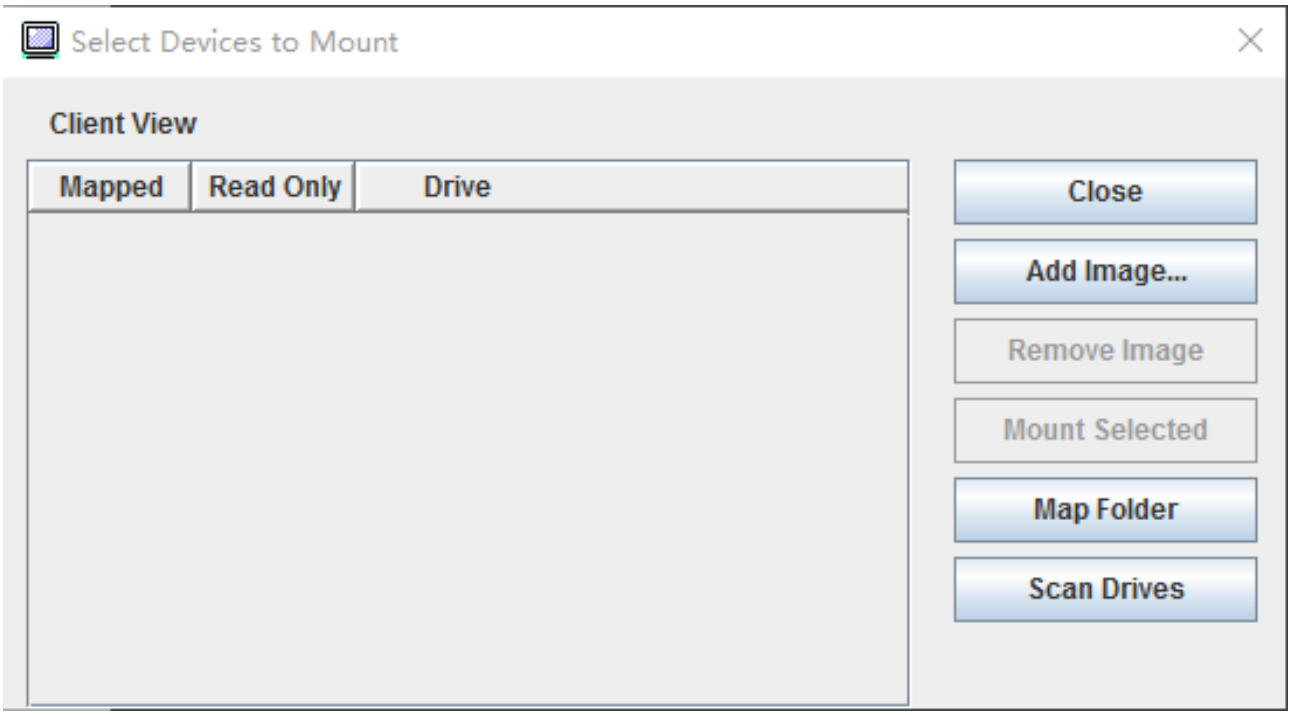


Figura 2. Ventana Seleccionar dispositivos para montar

Puede montar la imagen local, la carpeta y la unidad de CD/DVD/USB llevando a cabo los pasos siguientes:

- **Montar imagen local**:
  1. Haga clic en el botón **Añadir imagen** para seleccionar la imagen que desea montar.
  2. Compruebe la opción **Asignada**.
  3. Compruebe la opción **Solo lectura** para habilitar la función si es necesario.
  4. Haga clic en el botón **Montar selección** y podrá montar la imagen local satisfactoriamente.

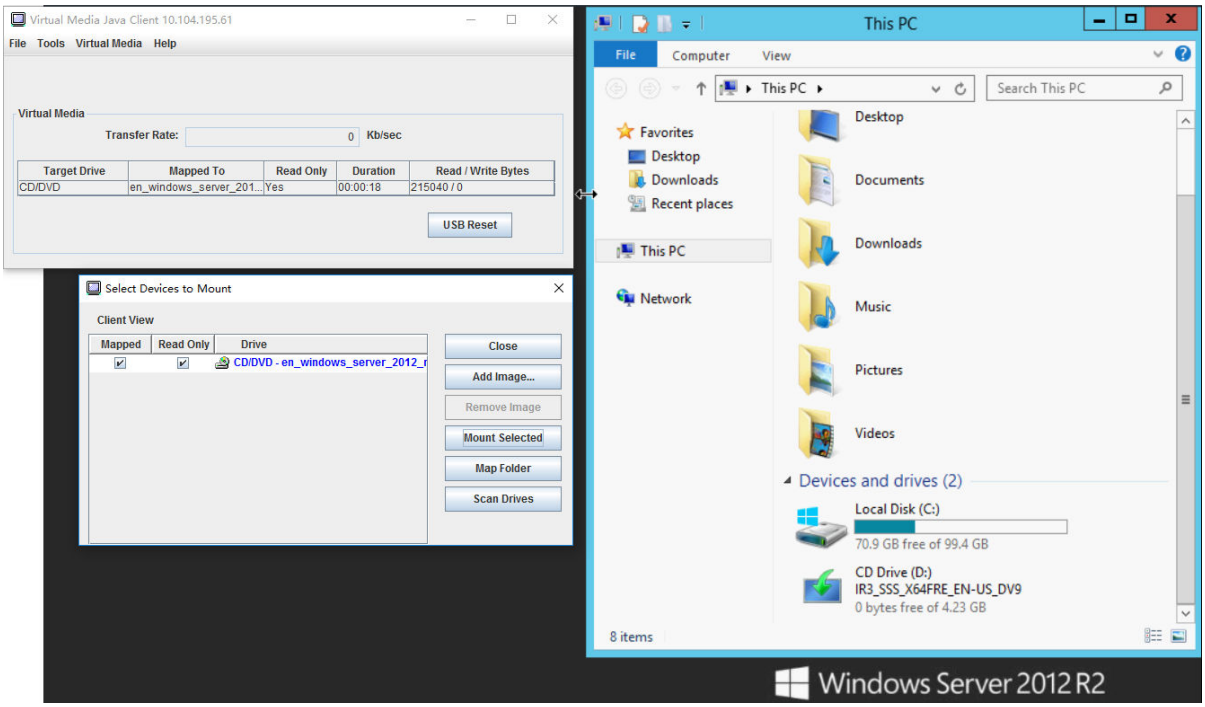
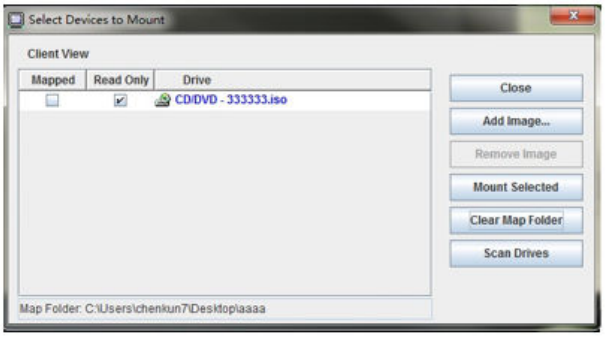


Figura 3. Montar imagen local

- **Montar carpeta local**:
  1. Haga clic en el botón **Asignar carpeta** para seleccionar la carpeta local que desea montar.
  2. Haga clic en el botón **Montar selección** y podrá montar la carpeta local satisfactoriamente.



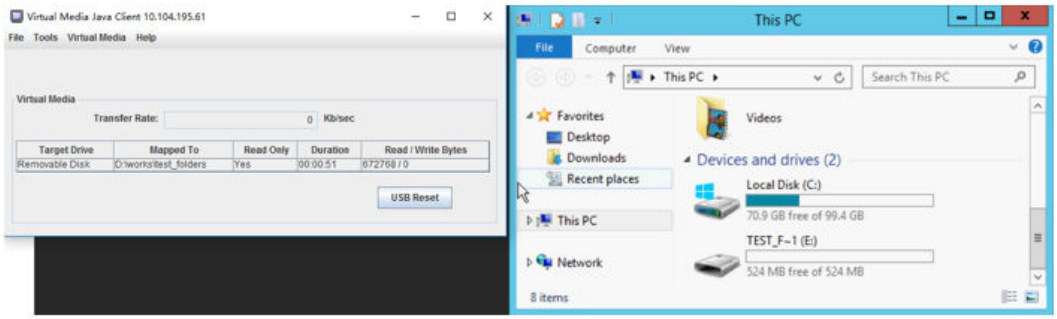


Figura 4. Montar carpeta local

- **Montar unidad de CD/DVD o USB**:
  1. Haga clic en el botón **Detección de unidades** para detectar una unidad de CD/DVD o USB conectados.
  2. Compruebe la opción **Asignada**.
  3. Compruebe la opción **Solo lectura** para habilitar la función si es necesario.
  4. Haga clic en el botón **Montar selección** y podrá montar la imagen local satisfactoriamente.

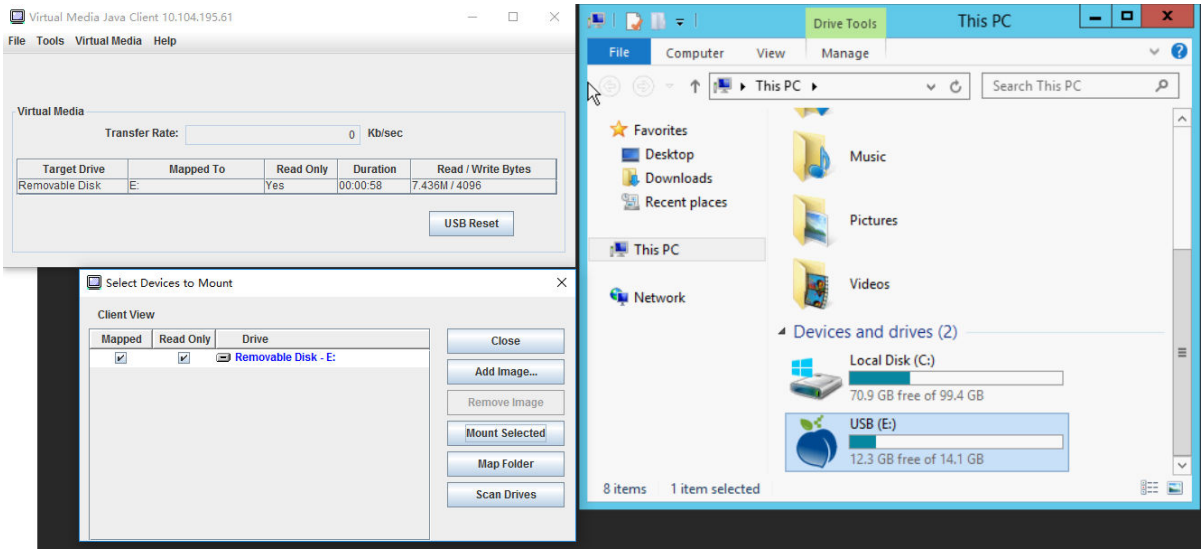


Figura 5. Montar unidad de CD/DVD o USB

La ventana Seleccionar dispositivos para montar contiene una lista de los dispositivos locales actuales que están disponibles para el montaje. Esta ventana contiene los siguientes campos y botones:

- El campo **Asignado** contiene la casilla de verificación que le permite seleccionar los dispositivos que va a montar o asignar.
- El campo **Solo lectura** contiene la casilla de verificación que le permite seleccionar los dispositivos asignados o montados que serán de **solo lectura** en el servidor host.
- El campo **Unidad** contiene la ruta del dispositivo en el equipo local.
- Haga clic en el botón **Cerrar** para cerrar la ventana Seleccionar dispositivos para montar.
- Haga clic en el botón **Añadir imagen** para buscar la imagen de disquete y el archivo de imagen ISO en el sistema de archivos local que desee añadir a la lista de dispositivos.
- Haga clic en el botón **Quitar imagen** para quitar una imagen que se ha añadido a la lista de dispositivos.
- Haga clic en el botón **Montar selección** para montar o asignar todos los dispositivos que están marcados para su montaje o asignación en el campo **Asignado**.

  Nota: La carpeta se montará como de solo lectura.
- Haga clic en el botón **Detección de unidades** para actualizar la lista de dispositivos locales.

Selección de los dispositivos que se van a desmontar

Para desmontar los dispositivos de servidor de host, realice los pasos siguientes:

1. Haga clic en la opción **Desmontar todo** en la pestaña **Medio virtual** en la ventana de Cliente de Java de medio virtual.

2. Después de seleccionar la opción **Desmontar todo** , se muestra una ventana de confirmación de Desmontar todo. Si acepta, **todos los** dispositivos de servidor host del servidor se desmontarán.

   Nota: No pueden desmontar unidades de forma individual.

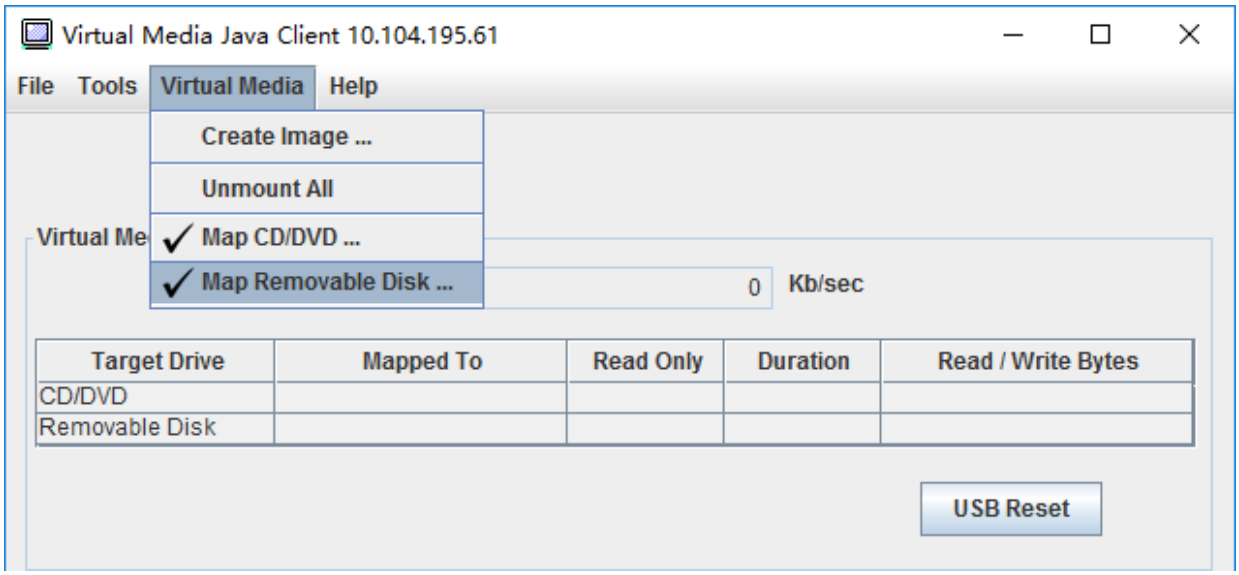


Figura 6. Desmontar todo

Problemas de error de montaje de medios

Utilice la información de este tema para resolver los problemas de error de montaje de medios.

Al utilizar certificados de seguridad generados por Microsoft IIS, pueden producirse errores durante el proceso de montaje. Si esto ocurre, sustituya el certificado de seguridad con uno nuevo generado por openssl. El archivo pfx recién generado se carga en el servidor de Microsoft IIS.

El siguiente es un ejemplo que muestra cómo se genera el nuevo certificado de seguridad mediante openssl en el sistema operativo Linux.

```
$ openssl
OpenSSL>

$ openssl genrsa 1024 > server.key
Generating RSA private key, 1024 bit long modulus
.....++++++
.....++++++
e is 65537 (0x10001)

$ openssl req -new -key server.key > server.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CN
State or Province Name (full name) [Some-State]:BJ
Locality Name (eg, city) []:HD
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Lenovo
Organizational Unit Name (eg, section) []:Lenovo
```

```
Common Name (e.g. server FQDN or YOUR name) []:10.245.18.66
Email Address []:test@test.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:LNV

$ ls
server.csr  server.key

$ openssl req -x509 -days 3650 -key server.key -in server.csr > server.crt
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CN
State or Province Name (full name) [Some-State]:BJ
Locality Name (eg, city) []:BJ
Organization Name (eg, company) [Internet Widgits Pty Ltd]:LNV
Organizational Unit Name (eg, section) []:LNV
Common Name (e.g. server FQDN or YOUR name) []:10.245.18.66
Email Address []:test@test.com

$ ls
server.crt  server.csr  server.key

$ openssl pkcs12 -export -out server.pfx -inkey server.key -in server.crt
Enter Export Password:
Verifying - Enter Export Password:

$ ls
server.crt  server.csr  server.key  server.pfx
```

Salir de la sesión de consola remota

Este tema explica cómo finalizar la sesión de consola remoto.

Para salir de la sesión de consola remoto, cierre las ventanas de consola remota y de sesión de medio virtual.

Descarga de datos de servicio

Utilice la información de este tema para recopilar información del servicio sobre su servidor. Este proceso normalmente se realiza solo a petición del personal de servicio para ayudarle a resolver un problema de servidor.

En la página de inicio del XClarity Controller, pulse la opción **Servicio** en la sección **Acción rápida** y seleccione **Descargar datos del servicio**. Pulse **Aceptar** para descargar los datos del servicio.

El proceso de recopilar datos del servicio y soporte tarda unos minutos para generar los datos de servicio. El archivo se guardará a su carpeta de descarga predeterminada. La convención de denominación para el archivo de datos de servicio sigue este patrón:<machine type and model>_<serial number>_xcc_<date>-<time>.tgz

Por ejemplo: 7X2106Z01A_2345678_xcc_170511-175656.tgz.

Además del formato tgz, los datos de servicio también pueden puede descargarse con el formato tzz. Tzz utiliza un algoritmo de compresión diferente y puede extraerse con una herramienta como “lzop”.

Propiedades del servidor

Utilice la información en este tema para cambiar o ver propiedades del servidor importantes.

Configuración de ubicación y contacto

Utilice la información de este tema para establecer diferentes parámetros para identificar el sistema para el personal de operaciones y soporte.

Seleccione **Propiedades del servidor** en **Configuración del servidor**, para configurar la información de **Ubicación y contacto**.

Contacto
Le permite especificar el nombre y número de teléfono de la persona a la que se debe contactar si hay un problema con el sistema.

Nota: Este campo es igual que el campo de contacto en la configuración de SNMPv3 y es obligatorio para habilitar SNMPv3.

Nombre del bastidor
Le permite ubicar el servidor más fácilmente al especificar en qué bastidor se encuentra.

Nota: El campo es opcional y no puede configurarse en un nodo Flex.

Número de sala
Le permite ubicar el servidor más fácilmente al especificar en qué sala se encuentra.

Creación
Le permite ubicar el servidor más fácilmente al especificar en qué edificio se encuentra.

U más bajo
Le permite ubicar el servidor más fácilmente al especificar la posición en el bastidor.

Nota: El campo es opcional y no puede configurarse en un nodo Flex.

Dirección
Le permite especificar la dirección postal completa donde se encuentra el servidor.

Nota: Una vez ingresada la información relevante, aparecerá como una sola línea en el campo **Ubicación** en la sección SNMPv3 y en la página de inicio del XClarity Controller.

Configuración de tiempos de espera de servidor

Utilice la información de este tema para establecer los tiempos de espera del servidor.

Estos tiempos de espera se usan para restaurar el funcionamiento de un servidor que se ha colgado.

Seleccione **Propiedades del servidor** en **Configuración del servidor** para configurar los tiempos de espera del servidor. Se proporcionan las siguientes selecciones de tiempo de espera del servidor:

Proceso de vigilancia del SO
El proceso de vigilancia del SO se utiliza para supervisar el sistema operativo para asegurarse de que no está colgado. La interfaz Ethernet sobre USB debe estar habilitada para esta característica. Consulte

"Configuración de Ethernet sobre USB" en la página 33 para obtener más detalles. XClarity Controller se pone en contacto con el sistema operativo en un intervalo configurado en la selección **Tiempo del proceso de vigilancia del SO**. Si el sistema operativo no responde antes del siguiente control, el XClarity Controller supone que el sistema operativo se ha colgado. XClarity Controller capturará el contenido de la pantalla del servidor y después reiniciará el servidor en un intento por restaurar el funcionamiento. XClarity Controller reiniciará el servidor solo una vez. Si el sistema operativo continúa colgado después del reinicio, en lugar de reiniciar de forma continua el servidor, el servidor se mantendrá en el estado colgado para que se pueda investigar y corregir el problema. Para rearmar el proceso de vigilancia del SO, apague y vuelva a encender el servidor. Para habilitar el proceso de vigilancia del SO, seleccione un intervalo en el menú desplegable del tiempo del proceso de vigilancia del SO y pulse **Aplicar**. Para deshabilitar el proceso de vigilancia del SO, seleccione **Ninguno** en el menú desplegable del tiempo del proceso de vigilancia del SO.

Vigilancia de cargador

El proceso de vigilancia del cargador supervisa el intervalo de tiempo entre la finalización de POST y cuando el sistema operativo comienza a funcionar. La interfaz Ethernet sobre USB debe estar habilitada para esta característica. Consulte "Configuración de Ethernet sobre USB" en la página 33 para obtener más detalles. Cuando se completa la POST, XClarity Controller inicia un contador de tiempo y comienza a contactar al sistema operativo. Si el sistema operativo no responde en el tiempo configurado en la selección del proceso de vigilancia del cargados, XClarity Controller supone que el arranque del sistema operativo se ha colgado. XClarity Controller luego reiniciará el servidor en un intento por restaurar el funcionamiento. XClarity Controller reiniciará el servidor solo una vez. Si el arranque del sistema operativo continúa colgado después del reinicio, en lugar de reiniciar de forma continua el servidor, el servidor se mantendrá en el estado colgado para que se pueda investigar y corregir el problema. Se rearma el proceso de vigilancia del cargador cuando el servidor se apaga y se vuelve a encender o cuando del servidor arranca correctamente el sistema operativo. Para habilitar el proceso de vigilancia del cargador, seleccione un intervalo en el menú desplegable del tiempo del proceso de vigilancia del cargador y pulse **Aplicar**. Para deshabilitar el proceso de vigilancia del cargador, seleccione **Ninguno** en el menú desplegable del tiempo del proceso de vigilancia del cargador.

Habilitar el retardo de apagado

Use el campo de retardo de apagado para especificar el número de minutos que el subsistema del XClarity Controller esperará para que se apague el sistema operativo antes de apagar el sistema. Para configurar el tiempo de espera del retardo de apagado, seleccione el intervalo desde el menú desplegable y pulse **Aplicar**. Para deshabilitar que el XClarity Controller fuerce el apagado, seleccione **Ninguno** en el menú desplegable.

Mensaje de advertencia de intrusión

Para crear un mensaje que se muestra cuando un usuario inicia sesión en el XClarity Controller, utilice la información de este tema.

Seleccione **Propiedades del servidor** en **Configuración del servidor**. Utilice la opción **Mensaje de advertencia de intrusión** para configurar un mensaje que quiere mostrar al usuario. Cuando termine, pulse **Aplicar**.

El texto del mensaje se mostrará en el área de mensajes de la página de inicio de sesión del XClarity Controller cuando un usuario inicia sesión.

Establecimiento de fecha y hora de XClarity Controller

Utilice la información en este tema para comprender la configuración de fecha y hora de XClarity Controller. Se proporcionan las instrucciones para configurar la fecha y hora del XClarity Controller. La fecha y hora del XClarity Controller se utiliza para marcar la hora de todos los sucesos que se registran en el registro de sucesos y las alertas enviadas.

En la página de inicio del XClarity Controller, pulse el icono del reloj en la esquina superior derecha para ver o cambiar la fecha y hora del XClarity Controller. El XClarity Controller no tiene su propio reloj en tiempo real. Puede configurar el XClarity Controller para sincronizar su fecha y hora con un servidor de protocolo de tiempo de red con el hardware del reloj en tiempo real del servidor.

Sincronización con el NTP

Siga estos pasos para sincronizar el reloj del XClarity Controller con el servidor NTP:

- Seleccione **Sincronizar la hora con el NTP** y especifique la dirección del servidor NTP.
- Los servidores NTP adicionales se pueden especificar pulsando el icono "+".
- Especifique con qué frecuencia desea que el XClarity Controller se sincronice con el servidor NTP.
- La hora que se obtiene del servidor NTP está en formato de hora universal coordinada (UTC).
  - Si desea que el XClarity Controller ajuste la fecha y la hora para su región local, seleccione la zona horaria disponible para compensar su zona en el menú desplegable.
  - Si su ubicación posee horario de verano, marque la casilla de verificación **Ajustar automáticamente el horario de verano (DST)**.
- Cuando los cambios de configuración estén completos, pulse **Aplicar**.

Sincronizar con el host

La hora del hardware del reloj en tiempo real del servidor puede estar en formato de hora universal coordinada (UTC) o puede haberse ajustado y haber almacenado en formato de hora local. Algunos sistemas operativos almacenan el reloj en tiempo real en formato UTC, mientras que otros la almacenan como hora local. El reloj en tiempo real del servidor no indica en qué formato se encuentra la hora. Por lo tanto, cuando el XClarity Controller se configura para sincronizar con el reloj en tiempo real del host, el usuario puede elegir cómo el XClarity Controller utiliza la hora y fecha que se obtiene del reloj en tiempo real.

- Local (ejemplo: Windows): En este modo, el XClarity Controller trata la hora y fecha que se obtiene del reloj en tiempo real como la hora local con cualquier zona horaria y con los ajustes de DST ya aplicados.
- UTC (ejemplo: Linux): En este modo, el XClarity Controller trata la hora y fecha que se obtiene del reloj en tiempo real como hora universal coordinada, sin zona horaria y ni con los ajustes de DST ya aplicados. En este modo puede ajustar la fecha y la hora para su región local, al seleccionar la zona horaria disponible para compensar su zona en el menú desplegable. Si su ubicación posee horario de verano, también puede marcar la casilla de verificación **Ajustar automáticamente el horario de verano (DST)**..
- Cuando los cambios de configuración estén completos, pulse **Aplicar**.

Notas:

- Cuando se produce el cambio a horario de verano, no se realizarán las acciones que se hayan programado para que el XClarity Controller las realice durante el intervalo cuando el reloj se adelanta. Por ejemplo, si el horario de verano en EE. UU. empieza a las 2:00 am el 12 de marzo y una acción de alimentación se programa para las 2:10 am el 12 de marzo, esta acción no ocurrirá. Una vez que la hora alcanza las 2:00 am, el XClarity Controller leerá la hora como las 3:00 am.
- Los valores de fecha y hora del XClarity Controller no se pueden modificar en un Flex System.

Capítulo 6. Configuración de almacenamiento

Utilice la información de este capítulo para comprender las opciones disponibles para las configuraciones de almacenamiento.

Al configurar el almacenamiento, están disponibles las opciones siguientes:

- Detalle
- Configuración de RAID

Detalle RAID

Para usar la función de detalle RAID, utilice la información de este tema.

Esta función muestra la estructura física de los dispositivos de almacenamiento y la configuración de almacenamiento junto con detalles como su ubicación, fabricante, nombre de producto, estado, capacidad, interfaz, soportes, factor de forma y otra información.

Configuración de RAID

Para llevar a cabo las funciones de la configuración de RAID, utilice la información de este tema.

Utilice la información en este tema para ver y configurar los grupos de almacenamiento, los discos virtuales asociados y las unidades para el adaptador RAID. Si el sistema se apaga, enciéndalo para ver la información de RAID.

Visualización y configuración de las unidades virtuales

Utilice la información de este tema para ver y configurar las unidades virtuales.

Cuando selecciona **Configuración de RAID** en **Configuración del servidor**, se selecciona la pestaña **Configuración de matriz** y se muestran los discos virtuales existentes de forma predeterminada. Las unidades lógicas se clasifican por matrices de discos y controladores. Se muestra información detallada sobre el disco virtual, como el tamaño de banda y la información arrancable del disco virtual.

Para configurar los valores de RAID, pulse **Habilitar modo de edición**.

En el modo de edición, puede pulsar el menú de la acción del controlador, ver los discos virtuales actuales de RAID y crear nuevos discos virtuales de RAID.

En el menú Acciones del controlador, puede llevar a cabo las siguientes acciones:

Borrar la configuración RAID
Borra toda la configuración y los datos del controlador seleccionado.

Gestionar configuración externa
Importa las unidades externas que se hayan detectado. Una unidad externa es una unidad que se ha movido desde otra configuración RAID al controlador RAID actual

Nota: Se le notificará si no se detecta ninguna unidad externa.

La información de los discos virtuales RAID actuales para un controlador particular se muestran como “tarjetas de discos virtuales” respectivos. Cada tarjeta muestra información sobre el nombre, el estado, la

capacidad y las acciones del disco virtual. El icono de lápiz permite editar la información y el icono de papelera de reciclaje le permite eliminar la “tarjeta de disco virtual”.

Nota: La capacidad y el nivel de RAID no se pueden cambiar.

Si hace clic en el nombre del disco virtual, aparece una ventana de propiedades del disco virtual.

Para crear un nuevo disco virtual de RAID, siga los pasos mostrados a continuación:

Nota: Si no hay memoria restante, no puede crear un nuevo disco virtual.

1. **Seleccione unidades o una matriz de discos que tenga memoria libre**
   a. Al crear un disco virtual en una nueva matriz de discos, deberá especificar el nivel de RAID. Si no hay suficientes unidades a seleccionar y pulsa **Siguiente**, un mensaje de error aparecerá bajo el campo de nivel de RAID.

      Para algunos niveles de RAID, se requiere espacio. También existe una cantidad mínima de unidades que deben existir en el espacio.
      1) Para este tipo de circunstancias, la interfaz web mostrará **Espacio 1** de forma predeterminada.
      2) Seleccione las unidades y pulse **Añadir miembro** para añadir las unidades al **Espacio 1**. Cuando **Espacio 1** no tiene suficientes unidades, deshabilite el enlace **Agregar espacio**.
      3) Pulse **Agregar espacio** para añadir el **Espacio 2**. Seleccione las unidades y pulse **Añadir miembro** para añadir el **Espacio 2**.
      4) Pulse **Añadir miembro** para añadir las unidades al espacio más reciente. Si desea añadir unidades al **Espacio 1** de nuevo, necesita hacer clic en el espacio 1 y seleccionar las unidades para agregar al **Espacio 1**.
      5) Si el número de espacio alcanza la cantidad máxima, deshabilite **Agregar espacio**.
   b. Para crear discos virtuales en una matriz de discos existente, necesita seleccionar una matriz de discos que tenga capacidad libre.
2. **Creación de un disco virtual**
   a. De forma predeterminada, cree un disco virtual que utiliza toda la memoria de almacenamiento. El icono **Añadir** está deshabilitado cuando se utiliza todo el almacenamiento. Puede pulsar el icono de lápiz para cambiar la capacidad u otras propiedades.
   b. Cuando edita el primer disco virtual para usar solo parte de la capacidad de almacenamiento, se habilita el icono **Añadir**. Pulse el icono para mostrar la ventana **Agregar disco virtual**.
   c. Si hay más de un disco virtual, el icono **Eliminar** se habilitará. Este icono no se mostrará si hay un disco virtual. Cuando pulsa el icono **Eliminar**, la fila seleccionada se eliminará de inmediato. No habrá ninguna ventana de confirmación ya que el disco virtual no se ha creado todavía.
   d. Pulse **Iniciar la creación del disco virtual** para iniciar el proceso.

Nota: Cuando el controlador no es compatible, aparecerá un mensaje.

Visualización y configuración del inventario de almacenamiento

Utilice la información de este tema para ver y configurar el inventario de almacenamiento.

En la pestaña **Inventario de almacenamiento** puede ver y configurar las matrices de discos, las unidades virtuales asociadas y las unidades para el controlador RAID.

- **Para dispositivos de almacenamiento que admiten la configuración RAID**:
  1. Si el controlador incluye las matrices de discos configuradas, mostrará las unidades instaladas basadas en la matriz de discos. La siguiente información describe los elementos que aparecen en la ventana.

- **Título de la tabla**: Muestra la identificación de la matriz de discos, el nivel de RAID y el número de unidades globales.
- **Contenido de la tabla**: Enumera las propiedades básicas; nombre de la unidad, estado de RAID, el tipo, el número de serie, el número de pieza, el número de las FRU y las acciones. Puede ir a la página **Inventario** para visualizar todas las propiedades que el XClarity Controller puede detectar.
- **Acciones**: A continuación se muestran las acciones que se pueden realizar. Algunas acciones no estarán disponibles cuando la unidad está en un estado diferente.
  - **Asignar repuesto dinámico**: Especifica la unidad de como repuesto dinámico global o repuesto dinámico dedicado.
  - **Extraer repuesto dinámico**: Quita la unidad del repuesto dinámico.
  - **Colocar unidad de disco fuera de línea**: Establece la unidad fuera de línea.
  - **Colocar unidad de disco en línea**: Establece la unidad en línea.
  - **Configurar unidad de disco como reutilizable**: Establece la unidad como reutilizable.
  - **Establecer unidad de disco como faltante**: Establece la unidad como faltante.
  - **Hace que la unidad sea buena para JBOD**: Añade la unidad al conjunto de discos JBOD.
  - **Hace que la unidad no configurada sea buena**: Hace que la unidad esté disponible para configurar en una matriz, o para utilizar como repuesto dinámico de emergencia.
  - **Hace que la unidad no configurada sea mala**: Marca la unidad como una en mal estado, evitando que se utilice en una matriz o como repuesto dinámico de emergencia.
  - **Establecer la unidad de disco como lista para quitarla**: Establece la unidad para la extracción.

2. Si el controlador incluye unidades que aún no se han configurado, serán visualizarán en la tabla **Unidades distintas de RAID**. Al pulsar la opción **Convertir JBOD a listo para configurar**, aparece una ventana que muestra todas las unidades que admiten esta acción. Puede seleccionar una o más unidades para la conversión.

Para dispositivos de almacenamiento que no admiten la configuración RAID: XClarity Controller puede no detectar las propiedades de algunas unidades.

Capítulo 7. Actualización del firmware del servidor

Para actualizar el firmware del servidor, utilice la información en este tema.

Visión general

Información general sobre la actualización de firmware del servidor.

La opción **Actualización de firmware** en el panel de navegación tiene 4 características:

- **Firmware del sistema:** descripción general del estado y la versión del firmware del sistema. Y para realizar la actualización de firmware del sistema.
- **Promoción automática de XCC principal a copia de seguridad:** una vez habilitada, el firmware del banco de copia de seguridad pendiente se sincronizará desde el banco principal después de que el banco primario haya pasado la medición de la Métrica de estabilidad de la imagen (ISM).
- **Firmware del adaptador:** visión general del firmware del adaptador instalado, su estado y versión. Y para realizar la actualización de firmware del adaptador.

El estado y las versiones de firmware actuales para el BMC, UEFI, LXPM, LXPM, controladores y adaptadores se muestran incluyendo las versiones principales y de copia de seguridad del BMC. Existen cuatro categorías para el estado del firmware:

- **Activo:** el firmware está activo.
- **Inactivo:** el firmware no está activo.
- **Pendiente:** el firmware está en espera de quedar activo.
- **N/A:** Ningún firmware se ha instalado para este componente.

Atención:

- XCC e IMM deben actualizarse a la versión más reciente antes de actualizar la UEFI. La actualización en orden distinto puede dar como resultado una conducta extraña o incorrecta.
- La instalación de la actualización de firmware equivocada puede hacer que el servidor no funcione correctamente. Antes de instalar una actualización de firmware o controlador de dispositivo, consulte el archivo readme y cambie los archivos de historial provistos con la actualización que se descargó. Estos archivos tienen información importante acerca de la actualización y del procedimiento de instalación; suelen incluir un procedimiento especial para actualizar desde las versiones de firmware o controlador de dispositivo más antiguas hasta las más recientes. Dado que el navegador web puede contener datos de caché XCC, se recomienda volver a cargar la página web después de actualizar el firmware del XCC.
- Algunas actualizaciones de firmware requieren el reinicio del sistema, que realiza la activación del firmware o la actualización interna. Este proceso en el arranque del sistema se denomina “modo de mantenimiento del sistema”, que no permite a los usuarios acciones de alimentación temporalmente. El modo también está habilitado durante la actualización del firmware. El usuario no debe desconectar la alimentación de CA cuando el sistema entre en modo de mantenimiento.

Actualización de firmware del sistema, adaptador y PSU

Pasos para actualizar el firmware del sistema, el firmware del adaptador y el firmware de la actualización.

Para aplicar manualmente la actualización del **Firmware del sistema**, el **firmware del adaptador** y el **Firmware de PSU**, lleve a cabo los siguientes pasos:

1. Haga clic en **Actualizar firmware** dentro de cada característica. Se abre la ventana Actualización del firmware del servidor.
2. Pulse **Examinar** para seleccionar el archivo de actualización de firmware que desea usar.
3. Vaya al archivo que desea seleccionar y pulse **Abrir**. A continuación regresa a la ventana Actualización del firmware del servidor con el archivo seleccionado en pantalla.
4. Pulse **Siguiente >** para iniciar la carga y verificar el proceso en el archivo seleccionado. Aparecerá una barra de progreso a medida que el archivo se carga y se verifica. Puede ver esta ventana de estado para verificar que el archivo que seleccionó para actualizar es el archivo correcto. Para el **Firmware del sistema**, la ventana de estado tendrá información relacionada con el tipo de archivo de firmware que debe actualizarse; por ejemplo BMC, UEFI o LXPM. Después de que el archivo de firmware se cargue y se verifique satisfactoriamente, pulse **Siguiente** para seleccionar el dispositivo que desea actualizar.
5. Pulse **Actualizar** para comenzar la actualización del firmware. Un medidor de progreso muestra el progreso de la actualización. Cuando la actualización de firmware se complete correctamente, pulse **Finalizar**. Si la actualización necesita reiniciar el XClarity Controller para surtir efecto, se mostrará un mensaje de aviso. Para conocer más detalles sobre cómo reiniciar el XClarity Controller, consulte “Acciones de alimentación” en la página 64.

Capítulo 8. Gestión de licencia

La gestión de licencia de Lenovo XClarity Controller permite instalar y gestionar las características opcionales de gestión del servidor y del sistema.

Existen múltiples niveles de funciones y características del firmware del XClarity Controller disponibles para el servidor. El nivel del firmware instalado en el servidor varía según el tipo de hardware.

Puede actualizar la funcionalidad del XClarity Controller comprando e instalando una clave de activación.

Para pedir una clave de activación, póngase en contacto con el representante de ventas o socio comercial.

Utilice la interfaz web de XClarity Controller o CLI de XClarity Controller para instalar manualmente una clave de activación que le permita utilizar una característica opcional que haya comprado. Antes de activar una clave:

- La clave de activación debe estar en el sistema que utiliza para iniciar sesión en el XClarity Controller.
- Debe haber solicitado la clave de licencia y haber recibido el código de autorización a través del correo o el correo electrónico.

Consulte “Instalación de una clave de activación” en la página 93, “Eliminación de una clave de activación” en la página 94 o “Exportación de una clave de activación” en la página 94 para obtener información acerca del manejo de una clave de activación mediante la interfaz web del XClarity Controller. Consulte “Comando keycfg” en la página 132 para obtener información acerca del manejo de una clave de activación mediante CLI del XClarity Controller.

Para registrar un ID que administre su licencia de XClarity Controller, pulse el siguiente enlace: https://fod.lenovo.com/lkms/angular/app/pages/index.htm#/welcome

Además, existe información acerca de la gestión de licencias de servidores Lenovo disponible en el sitio web siguiente de **Lenovo Press**:

https://lenovopress.com/redp4895-using-lenovo-features-on-demand

Atención: No puede actualizar directamente el XClarity Controller estándar a la funcionalidad de nivel empresarial. Necesitará primero actualizar a nivel avanzado antes de que la funcionalidad de nivel empresarial puede activarse.

Instalación de una clave de activación

Utilice la información en este tema para añadir una función opcional al servidor.

Para instalar una clave de activación, lleve a cabo los siguientes pasos:

Paso 1. Pulse **Licencia** en **Configuración de BMC**.

Paso 2. Pulse **Licencia de actualización**.

Paso 3. En la ventana **Añadir nueva licencia**, pulse **Examinar**; a continuación, seleccione el archivo de clave de activación para añadir en la ventana de carga del archivo y **Abrir** para añadir el archivo o **Cancelar** para detener la instalación. Para terminar de añadir la clave, pulse **Aceptar** en la ventana Añadir clave de activación o **Cancelar** para detener la instalación.

La ventana de acción satisfactoria indica que la clave de activación está instalada.

Notas:

- Si la clave de activación no es válida, aparecerá una ventana de error.

Paso 4. Pulse **Aceptar** para cerrar la ventana de acción satisfactoria.

Eliminación de una clave de activación

Utilice la información en este tema para eliminar una función opcional del servidor.

Para eliminar una clave de activación, lleve a cabo los siguientes pasos:

Paso 1. Pulse **Licencia** en **Configuración de BMC**.

Paso 2. Seleccione la clave de activación a eliminar y, a continuación, **Eliminar**.

Paso 3. En la ventana Confirmar eliminación de la clave de activación, pulse **Aceptar** para confirmar o **Cancelar** para conservar el archivo de clave.
La clave de activación seleccionada se elimina del servidor y ya no aparece en la página de gestión de licencias.

Exportación de una clave de activación

Utilice la información en este tema para exportar una función opcional del servidor.

Para exportar una clave de activación, lleve a cabo los siguientes pasos:

Paso 1. Pulse **Licencia** en **Configuración de BMC**.

Paso 2. En la página Gestión de licencias, seleccione la clave de activación a exportar y, a continuación, **Exportar**.

Paso 3. En la ventana **Exportar la licencia seleccionada** pulse **Exportar** para confirmar la exportación de la clave de activación o **Cancelar** para cancelar la solicitud de exportación de la clave.

Paso 4. Seleccione el directorio para guardar el archivo.
La clave de activación seleccionada se exporta del servidor.

Capítulo 9. API REST Redfish de Lenovo XClarity Controller

Lenovo XClarity Controller proporciona un conjunto de API REST que cumplen con Redfish fáciles de utilizar que permiten acceder a los datos y servicios de Lenovo XClarity Controller desde aplicaciones que se ejecutan fuera del marco de Lenovo XClarity Controller.

Esto permite una integración sencilla de las capacidades de Lenovo XClarity Controller en otro software, ya sea que se ejecute el software en el mismo sistema que el servidor de Lenovo XClarity Controller o en un sistema remoto dentro de la misma red. Estas API se basan en la API REST Redfish estándar de la industria y se acceden a través del protocolo HTTPS.

Puede encontrar la Guía del usuario de API REST Redfish de XClarity Controller aquí: https://pubs.lenovo.com/xcc-restapi/xcc_restapi_book.pdf.

Lenovo proporciona secuencias de comandos de código abierto de ejemplo Redfish que pueden utilizarse como referencia para desarrollar software que se comunica con la API REST Redfish de Lenovo. Estos scripts de muestra se pueden encontrar aquí:

- Python: https://github.com/lenovo/python-redfish-lenovo
- PowerShell: https://github.com/lenovo/powershell-redfish-lenovo

Las especificaciones de DMTF relacionadas con la API de theRedfish están disponibles en: https://redfish.dmtf.org/. Este sitio web proporciona especificaciones generales y otros materiales de referencia en la API REST Redfish.

Capítulo 10. Interfaz de la línea de comandos

Utilice la información en este tema para ingresar comandos que gestionan y supervisan el XClarity Controller sin tener que utilizar la interfaz web del XClarity Controller.

Utilice la interfaz de línea de comandos (CLI) del XClarity Controller para acceder al XClarity Controller sin tener que utilizar la interfaz web. Proporciona un subconjunto de funciones de gestión proporcionadas por la interfaz web.

Puede acceder a la CLI mediante una sesión SSH. Debe autenticarse en el XClarity Controller antes de emitir comandos CLI.

Acceso a la interfaz de la línea de comandos

Utilice la información de este tema para acceder al CLI.

Para acceder al CLI, inicie una sesión SSH en la dirección IP del XClarity Controller (consulte “Configuración de redirección serie a SSH” en la página 97 para obtener más información).

Inicio de sesión en la sesión de línea de comandos

Utilice la información en este tema para iniciar sesión en la línea de comandos.

Lleve a cabo los pasos siguientes para iniciar sesión en la línea de comandos:

Paso 1. Establezca una conexión con el XClarity Controller.

Paso 2. En el indicador de nombre del usuario, escriba el Id. de usuario.

Paso 3. En la solicitud de contraseña, escriba la contraseña que utiliza para iniciar sesión en XClarity Controller.

Con eso inicia sesión en el comando de línea. El indicador de línea de comando es `system>`. La sesión de línea de comandos continúa hasta que se escribe `exit` en la línea de comandos. Cierra la sesión y se finaliza la sesión.

Configuración de redirección serie a SSH

Este tema proporciona información sobre cómo utilizar el XClarity Controller como servidor terminal en serie.

La redirección serie a SSH le permite a un administrador del sistema utilizar el XClarity Controller como servidor terminal en serie. Un puerto serie del servidor se puede acceder desde una conexión SSH cuando se habilita la redirección serie.

Nota: Se utiliza el comando CLI **console 1** para iniciar una sesión de redirección en serie con el puerto COM.

Sesión la ejemplo

```
$ ssh USERID@10.240.1.12
Password:

system>
```

Todo el tráfico de la sesión SSH se direcciona a COM2.

```
ESC (
```

Escriba la secuencia de teclas de salida para volver la CLI. En este ejemplo, pulse Esc y después escriba un paréntesis izquierdo. Se visualiza un mensaje de CLI para indicar la vuelta a CLI de IMM.

```
system>
```

Sintaxis del comando

Revise las instrucciones de este tema para comprender cómo especificar los comando en la CLI.

Lea las instrucciones siguientes antes de utilizar los comandos:

- Cada comando tiene el formato siguiente:
  `command [`**arguments**`] [-`**options**`]`
- La sintaxis del comando distingue entre mayúsculas y minúsculas.
- El nombre del comando se escribe en minúsculas.
- Todos los argumentos deben seguir inmediatamente al comando. Las opciones siguen inmediatamente a los argumentos.
- Cada opción es precedida siempre por de un (-). Una opción puede ser una opción corta (una letra) o una opción larga (varias letras).
- Si una opción tiene un argumento, el argumento es obligatorio, por ejemplo:
  `ifconfig eth0 -i 192.168.70.34 -g 192.168.70.29 -s 255.255.255.0`
  donde **ifconfig** es el comando, eth0 es un argumento y -i, -g y -s son opciones. En este ejemplo, las tres opciones tienen argumentos.
- Los corchetes indican que un argumento o una opción es opcional. Los corchetes no forman parte de comando que se escribe.

Características y limitaciones

Este tema contiene información sobre las características y las limitaciones de CLI.

CLI tiene las siguientes características y limitaciones:

- Se permiten varias sesiones de CLI simultáneas a través de SSH.
- Se permite un comando por línea (límite de 1024 caracteres, incluyendo espacios).
- No hay carácter de continuación para los comandos largos. La única función de edición es la clave de tecla de retroceso para borrar el carácter que acaba de escribir.
- Las teclas de flecha arriba y abajo se pueden utilizar para examinar los ocho últimos comandos. El comando **history** muestra una lista de los ocho últimos comandos, que luego se pueden utilizar como acceso directo para implementar un comando, como en el ejemplo siguiente:

```
system > history
 0 ifconfig eth0
 1 readlog
 2 readlog
 3 readlog
 4 history
system > !0
-state enabled
-c dthens
-i 192.168.70.125
-g 0.0.0.0
```

```
-s 255.255.255.0
-n XClarity ControllerA00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
system >
```

- En CLI, el límite de almacenamiento de salida es de 2 KB. No hay almacenamiento intermedio. La salida de un comando individual no puede exceder los 2048 caracteres. Este límite no aplica en el modo de redirección de serie (los datos se protegen durante la redirección de serie).
- Los mensajes de texto simple se utilizan para denotar el estado de la realización del comando, como en el ejemplo siguiente:
```
system> power on
ok
system> power state
Power: On
State: System power off/State unknown
system>
```
- La sintaxis del comando distingue entre mayúsculas y minúsculas.
- Debe haber al menos un espacio entre una opción y su argumento. Por ejemplo, `ifconfig eth0 -i192.168.70.133` es una sintaxis equivocada. La sintaxis correcta es `ifconfig eth0 -i 192.168.70.133`.
- Todos los comandos tienen las opciones `-h`, `-help` y `?` , que indican el soporte de sintaxis. Todos los ejemplos siguientes darán el mismo resultado:
```
system> power -h
system> power -help
system> power ?
```
- Algunos de los comandos que se describen en las secciones siguientes no están disponibles para la configuración del sistema. Para ver una lista de los comandos admitidos por la configuración, utilice la opción `help` o `?`, tal como se muestra en las ilustraciones siguientes:
```
system> help
system> ?
```
- En un Flex System, el CMM gestiona algunos valores y no se pueden modificar desde el XClarity Controller.

Lista alfabética de comandos

Este tema contiene una lista de comandos CLI en orden alfabético. Se proporcionan enlaces a los temas para cada comando. Cada tema de comandos proporciona información sobre el comando, su función, sintaxis y uso.

La lista completa de todos los comandos CLI de XClarity Controller, en orden alfabético, es como sigue:

- “Comando accseccfg” en la página 115
- “Comando adapter” en la página 180
- “Comando alertcfg” en la página 117
- “Comando alertentries” en la página 165
- “Comando asu” en la página 118
- “Comando backup” en la página 121
- “Comando batch” en la página 168
- “Comando clearcfg” en la página 168
- “Comando clearlog” en la página 102

Comandos de utilidad

Este tema proporciona una lista alfabética de los comandos CLI de utilidad.

Actualmente, hay 3 comando de la utilidad:

Comando exit

Utilice este comando para cerrar la sesión en el servidor CLI.

Utilice el comando **exit** para cerrar la sesión y salir de la sesión CLI.

Comando help

Este comando muestra una lista de todos los comandos.

Use el comando **help** para mostrar una lista de todos los comandos con una breve descripción de cada uno. También puede escribir ? en el indicador de comandos.

Comando history

Este comando proporciona una lista de comandos emitidos anteriormente.

Utilice el comando **history** para visualizar una lista indexada de los últimos ocho comandos emitidos. Los índices se pueden utilizar a continuación como atajos (precedidos de !) para volver a emitir los comandos desde esta lista de historial.

Ejemplo:

```
system> history
 0 ifconfig eth0
 1 readlog
 2 readlog
 3 readlog
 4 history
system> ifconfig eth0
-state enabled
-c dthens
-i 192.168.70.125
HISTORY-g 0.0.0.0
-s 255.255.255.0
-n XCCA00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
system>
```

Comandos del monitor

Este tema proporciona una lista alfabética de los comandos CLI del monitor.

Actualmente, hay 11 comandos de monitor:

Comando clearlog

Este comando se usa para borrar el registro de sucesos de IMM.

Utilice el comando **clearlog** para borrar el registro de sucesos del IMM. Debe tener autorización para borrar los registros de sucesos para utilizar este comando.

Nota: Este comando está diseñado solo para el uso del personal de soporte.

En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 7. Comando clearlog

La tabla siguiente es una tabla de dos columna y una fila que consta de las opciones y las descripciones asociadas.

Opción	Descripción
-t <all | platform | audit>	Tipo de suceso, elija el tipo de suceso a borrar. Si no se especifica, se seleccionarán todos los tipos de sucesos.

Descripciones de tipos de suceso

- all: todos los tipos de sucesos, lo que incluye los sucesos de plataforma y sucesos de auditoría.
- platform: tipo de suceso de plataforma.
- audit: tipo de suceso de auditoría.

Ejemplo:

```
system> clearlog
All event log cleared successfully
```

```
system> clearlog -t all
All event log cleared successfully
system> clearlog -t platform
Platform event log cleared successfully
system> clearlog -t audit
Audit event log cleared successfully
```

Comando fans

Se utiliza este comando para visualizar la velocidad de los ventiladores del servidor.

Utilice el comando **fans** para visualizar la velocidad de cada uno de los ventiladores del servidor.

Ejemplo:

```
system> fans
fan1 75%
fan2 80%
fan3 90%
system>
```

Comando ffdc

Se utiliza este comando para generar un nuevo archivo de datos de servicio.

Utilice el comando de recopilación de datos de primer error (**ffdc**) para generar y descargar datos de servicio al soporte.

La lista siguiente consta de comandos para utilizarse con el **ffdc**:

- **generate**, crea un nuevo archivo de datos de servicio
- **status**, estado de control del archivo de datos de servicio
- **copy**, copia datos de servicio existentes
- **delete**, elimina datos de servicio existentes

En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 8. Comando ffdc

La tabla siguiente es una tabla de tres columnas y varias filas que consta de las opciones, las descripciones de las opciones y los valores asociados para las opciones.

Opción	Descripción	Valores
-t	Número de tipo	1 (descarga de procesador) y 4 (datos de servicio). La descarga del procesador contiene todos los registros y archivos disponibles. Los datos de servicio contienen solo un subconjunto de los registros y los archivos. El valor predeterminado es 1.
-f [1]	Nombre de archivo remoto o directorio de destino sftp.	Para sftp, utilice la ruta completa o arrastre/en el nombre del directorio (~/o/tmp/). El valor predeterminado es el nombre generado por el sistema.
-ip [1]	Dirección del servidor tftp/ sftp	
-pn [1]	Número de puerto del servidor tftp/sftp	El valor predeterminado es 69/22.

Tabla 8. Comando ffdc (continuación)

Opción	Descripción	Valores
-u [1]	Nombre de usuario para el servidor sftp	
-pw [1]	Contraseña para el servidor sftp	

1. Argumento adicional para los comandos **generate** y **copy**

Sintaxis:
```
ffdc [options]
option:
  -t 1 or 4
  -f
  -ip ip_address
  -pn port_number
  -u username
  -pw password
```

Ejemplo:
```
system> ffdc generate
Generating ffdc...
system> ffdc status
Type 1 ffdc: in progress
system> ffdc copy -t 1 -ip 192.168.70.230 -u User2 -pw Passw0rd -f /tmp/
Waiting for ffdc.....
Copying ffdc...
ok
system> ffdc status
Type 1 ffdc: completed
8737AC1_DSY0123_xcc_120317-153327.tgz


system> ffdc generate
Generating ffdc...
system> ffdc status
Type 1 ffdc: in progress
system> ffdc status
Type 1 ffdc: in progress
system> ffdc copy -ip 192.168.70.230
Copying ffdc...
ok
system> ffdc status
Type 1 ffdc: completed
8737AC1_DSY0123_xcc_120926-105320.tgz
system>
```

Comando hreport

Utilice este comando para mostrar un informe integrado de estado.

La siguiente tabla muestra los comandos hreport.

Tabla 9. Comandos hreport

La tabla siguiente es una tabla de dos columnas y varias filas que consta de las descripciones de diferentes comandos hreport.

Tabla 9. Comandos hreport (continuación)

Opción	Descripción
generar	Crear nuevo informe de estado
estado	Comprobar el estado
copy	Copiar el informe existente de estado
suprimir	Eliminar el informe existente de estado

En la tabla siguiente se muestran los argumentos para las opciones de generate y copy.

Tabla 10. Comando generate y copy

La tabla siguiente es una tabla de dos columnas y varias filas que consta de las opciones de los comandos generate y copy y las descripciones asociadas.

Opción	Descripción
-f	Nombre de archivo remoto o directorio de destino sftp (la opción predeterminada es un nombre generado por el sistema ((para sftp, use la ruta completa o / al final en el nombre del directorio (~/ o /tmp/))
-ip	Dirección del servidor tftp/sftp
-pn	Número de puerto del servidor tftp/sftp (predeterminado 69/22)
-u	Nombre de usuario para el servidor sftp
-pw	Contraseña para el servidor sftp

Comando mhlog

Utilice este comando para visualizar las entradas de registro de actividad del historial de mantenimiento

En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 11. Comando mhlog

La tabla siguiente es una tabla de dos columnas y varias filas que consta de las opciones y las descripciones asociadas.

Opción	Descripción
-c <count>	Mostrar entradas de “recuento” (1 a 250)
-i <index>	Mostrar entradas empezando en el índice (1 a 250)
-f	Nombre de archivo remoto del archivo de registro
-ip	Dirección del servidor tftp/sftp
-pn	Número de puerto del servidor tftp/sftp (predeterminado 69/22)
-u	Nombre de usuario para el servidor sftp
-pw	Contraseña para el servidor sftp

Ejemplo

La pantalla tendrá una apariencia similar a la siguiente:

```
Type            Message                                                                  Time
-------------   ------------                                                             ----
Hardware        SAS Backplane1(SN: XXXX9CE009L) is added.                               05/08/2020,04:23:18
Hardware        CPU 1(SKU NO: 50844440) is added.                                       05/08/2020,04:23:22
Hardware        CPU 2(SKU NO: 50844440) is added.                                       05/08/2020,04:23:22
Hardware        M2 Card(SN: R1SH9AJ0037) is added.                                      05/08/2020,04:23:22
Firmware        Primary XCC firmware is updated to TGBT99T by XCC Web.                  05/08/2020,06:40:37
Firmware        Primary XCC firmware is activated to TGBT99T .                          05/08/2020,06:41:26
Hardware        PSU1(SN: D1DG94C00075) is added.                                        05/08/2020,06:43:28
```

Comando led

Use este comando para mostrar y configurar los estados de LED.

El comando **led** muestra y establece los estados de LED del servidor.

- Ejecutar el comando **led** sin opciones muestra el estado de los LED del panel frontal.
- La opción de comando **led -d** debe utilizarse con la opción de comando **led -identify on**.

En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 12. Comando led

La tabla siguiente es una tabla de tres columnas y varias filas que consta de las opciones, las descripciones de las opciones y los valores asociados para las opciones.

Opción	Descripción	Valores
-l	Obtener el estado de todos los LED del sistema y los subcomponente del sistema	
-chklog	Apagar el LED de comprobación de registro	desactivado
-identify	Cambiar el estado del LED de identificación del alojamiento	apagado, encendido, parpadeo
-d	Activar el LED de identificación por un periodo especificado	Periodo de tiempo (segundos)

Sintaxis:

```
led [options]
option:
  -l
  -chklog off
  -identify state
  -d time
```

Ejemplo:

```
system> led
Fault                Off
Identify             On            Blue
Chklog               Off
Power                Off

system> led -l
Label                Location                State          Color
Battery              Planar                  Off
BMC Heartbeat        Planar                  Blink          Green
BRD                  Lightpath Card          Off
Channel A            Planar                  Off
```

```
Channel B             Planar                Off
Channel C             Planar                Off
Channel D             Planar                Off
Channel E             Planar                Off
Chklog                Front Panel           Off
CNFG                  Lightpath Card        Off
CPU                   Lightpath Card        Off
CPU 1                 Planar                Off
CPU 2                 Planar                Off
DASD                  Lightpath Card        Off
DIMM                  Lightpath Card        Off
DIMM 1                Planar                Off
DIMM 10               Planar                Off
DIMM 11               Planar                Off
DIMM 12               Planar                Off
DIMM 13               Planar                Off
DIMM 14               Planar                Off
DIMM 15               Planar                Off
DIMM 16               Planar                Off
DIMM 2                Planar                Off
DIMM 3                Planar                Off
DIMM 4                Planar                Off
DIMM 5                Planar                Off
DIMM 6                Planar                Off
DIMM 7                Planar                Off
DIMM 8                Planar                Off
DIMM 9                Planar                Off
FAN                   Lightpath Card        Off
FAN 1                 Planar                Off
FAN 2                 Planar                Off
FAN 3                 Planar                Off
Fault                 Front Panel (+)       Off
Identify              Front Panel (+)       On            Blue
LINK                  Lightpath Card        Off
LOG                   Lightpath Card        Off
NMI                   Lightpath Card        Off
OVER SPEC             Lightpath Card        Off
PCI 1                 FRU                   Off
PCI 2                 FRU                   Off
PCI 3                 FRU                   Off
PCI 4                 FRU                   Off
Planar                Planar                Off
Power                 Front Panel (+)       Off
PS                    Lightpath Card        Off
RAID                  Lightpath Card        Off
Riser 1               Planar                Off
Riser 2               Planar                Off
SAS ERR               FRU                   Off
SAS MISSING           Planar                Off
SP                    Lightpath Card        Off
TEMP                  Lightpath Card        Off
VRM                   Lightpath Card        Off
system>
```

Comando readlog

Este comando muestra los registros de sucesos del IMM.

Utilice el comando **readlog** para visualizar las entradas de registro de sucesos IMM. Se muestran cinco registros de sucesos al mismo tiempo. Las entradas se visualizan de más reciente a más antigua.

readlog muestra las primeras cinco entradas del registro de sucesos, que la más reciente, en la primera ejecución y luego las cinco siguientes para cada llamada siguiente.

readlog -a muestra todas las entradas del registro de sucesos, empezando por la más reciente.

readlog -f restablece el contador y muestra las primeras 5 entradas en el registro de sucesos, empezando por la más reciente.

readlog -date date muestra las entradas de registro de sucesos para la fecha especificada, en el formato mm/dd/aa. Puede ser una lista de fechas separadas por barras verticales (|).

readlog -sev severity muestra las entradas de registro de sucesos para el nivel de gravedad especificado (E, W, I). Puede ser una lista de niveles de gravedad separados por barras verticales (|).

readlog -i ip_address establece la dirección IP IPv4 o IPv6 del servidor TFTP o SFTP donde se guarda el registro de sucesos. Las opciones de comando **-i** y **-l** se utilizan juntas para especificar la ubicación.

readlog -l filename establece el nombre del archivo del registro de sucesos. Las opciones de comando **-i** y **-l** se utilizan juntas para especificar la ubicación.

readlog -pn port_number muestra o establece el número de puerto del servidor TFTP o SFTP (valor predeterminado 69/22).

readlog -u username especifica el nombre de usuario para el servidor SFTP.

readlog -pw password especifica la contraseña para el servidor SFTP.

Sintaxis:

```
readlog [options]
option:
  -a
  -f
  -date date
  -sev severity
  -i ip_address
  -l filename
  -pn port_number
  -u username
  -pw password
```

Ejemplo:

```
system> readlog -f
1 I 2017-06-17T09:31:59.217  Remote Login Successful. Login ID: USERID
from SSH at IP address 10.134.78.180
2 I 2017-06-17T07:23:04.685  Remote Login Successful. Login ID: USERID
from webguis at IP address 10.134.78.180.
3 I 2017-06-16T11:00:35.581  Login ID: USERID from webguis at IP address 10.134.78.180 has logged off.
4 I 2017-06-16T11:00:15.174  Login ID: USERID from webguis at IP address 10.104.209.144 has logged off.
5  I 2017-06-16T10:40:14.352  Login ID: USERID from webguis at IP address 10.104.209.144 has logged off.
system> readlog
6 E SERVPROC 12/18/03 10:09:31 Fan 2 Fault. Multiple fan failures
7 E SERVPROC 12/18/03 10:09:31 Fan 1 Fault. Single fan failure
8 I SERVPROC 12/18/03 10:09:25 Ethernet[0] Link Established at 100Mb, Full Duplex.
9 I SERVPROC 12/18/03 10:09:24 Ethernet[0] configured to do Auto Speed/Auto Duplex.
10 I SERVPROC 12/18/03 10:09:24 Ethernet[0] MAC Address currently
being used: 0x00-09-6B-CA-0C-80
system>
```

Comando syshealth

Este comando proporciona un resumen del estado o los sucesos activos.

Utilice el comando **syshealth** para visualizar un resumen de estado o de sucesos activos del servidor. Se muestra el estado de alimentación, el estado del sistema, el estado de hardware (incluye ventilador, fuente de alimentación, almacenamiento, procesador, memoria), conteo de reinicio y estado de software de IMM.

Sintaxis:

```
syshealth [argument]
argument:
  summary      -display the system health summary
  activeevents -display active events
  cooling - display cooling devices health status
  power - display power modules health status
  storage - display local storage health status
  processors - display processors health status
  memory - display memory health status
```

Ejemplo:

```
system> syshealth summary
Power    On
State    OS booted
Restarts 29

system> syshealth activeevents
No Active Event Available!
```

Comando temps

Este comando muestra toda la información de temperatura y de límites de temperatura.

Utilice el comando **temps** para visualizar todas las temperaturas y límites de temperatura. El mismo conjunto de temperaturas se muestra como en la interfaz de la web.

```
Example
system> temps
Temperatures are displayed in degrees Fahrenheit/Celsius

         WR      W       T      SS      HS
-----------------------------------------------
CPU1     N/A     N/A    80/27   N/A     N/A
CPU2     N/A     N/A    80/27   N/A     N/A
DASD1   66/19   73/23   82/28   88/31   92/33
Amb     59/15   70/21   83/28   90/32   95/35
system>
```

Notas:

1. La salida tiene los siguientes encabezados de columna:

   WR: restablecimiento de advertencia (valor de histéresis de límite positivo)

   W: advertencia (límite superior no crítico)

   T: temperatura (valor actual)

   SS: apagado de software (límite crítico superior)

   HS: apagado brusco (límite superior no recuperable)
2. Todos los valores de temperatura están los grados Fahrenheit/centígrados.
3. N/A representa no aplicable.

Comando volts

Utilice este comando para ver la información de voltaje del servidor.

Utilice el comando **volts** para visualizar todos los voltajes y límites de voltaje. El mismo conjunto de voltajes se muestra como en la interfaz de la web.

```
Example:
system> volts

     i HSL    SSL    WL     WRL    V      WRH    WH    SSH    HSH
-------------------------------------------------------------------
5v     5.02  4.00  4.15  4.50  4.60  5.25  5.50  5.75   6.00
3.3v   3.35  2.80  2.95  3.05  3.10  3.50  3.65  3.70   3.85
12v    12.25 11.10 11.30 11.50 11.85 12.15 12.25 12.40  12.65
-5v    -5.10 -5.85 -5.65 -5.40 -5.20 -4.85 -4.65 -4.40  -4.20
-3.3v -3.35 -4.10 -3.95 -3.65 -3.50 -3.10 -2.95 -2.80  -2.70
VRM1                          3.45
VRM2                          5.45
system>
```

Nota: La salida tiene los siguientes encabezados de columna:

- HSL: apagado brusco bajo (límite inferior no recuperable)
- SSL: apagado de software bajo (límite crítico inferior)
- WL: advertencia baja (límite inferior no crítico)
- WRL: restablecimiento de advertencia bajo (valor de histéresis de límite negativo)
- V: voltaje (valor actual)
- WRH: restablecimiento de advertencia alto (valor de histéresis de límite positivo)
- WH: advertencia alta (límite superior no crítico)
- SSH: apagado de software alto (límite crítico superior)
- HSH: apagado brusco alto (límite superior no recuperable)

Comando vpd

Este comando muestra la configuración y los datos informativos (datos de producto fundamentales) asociados con el hardware y el software del servidor.

Utilice el comando **vpd** para visualizar los datos de producto fundamentales para el sistema (sys), IMM (bmc), servidor BIOS (uefi), Lenovo XClarity Provisioning Manager (lxpm), firmware de servidor (fw), componentes del servidor (comp) y dispositivos PCIe (pcie). La misma información se muestra como en la interfaz web.

Sintaxis:

```
vpd sys  - displays Vital Product Data for the system
vpd bmc  - displays Vital Product Data for the management controller
vpd uefi - displays Vital Product Data for system BIOS
vpd lxpm  - displays Vital Product Data for system LXPM
vpd fw   - displays Vital Product Data for the system firmware
vpd comp - displays Vital Product Data for the system components
vpd pmem - displays Vital Product Data for Intel Optane PMem
vpd pcie - displays Vital Product Data for PCIe devices
```

Ejemplo:

```
system> vpd bmc
```

```
Type            Status      Version     Build     ReleaseDate
----            -------       -----       ------
BMC (Primary)   Active      0.00        DVI399T    2017/06/06
BMC (Backup)    Inactive    1.00        TEI305J    2017/04/13

system>
```

Comandos de control de alimentación y reinicio del servidor

Este tema proporciona una lista alfabética de los comandos CLI de alimentación y reinicio.

Actualmente hay 4 comandos de alimentación y de reinicio del servidor:

Comando power

Este comando describe cómo controlar la alimentación del servidor.

Utilice el comando **power** para controlar la alimentación del servidor. Para emitir comandos **power**, debe tener el nivel de autoridad de Acceso a Alimentación de servidor remoto/reinicio.

La siguiente tabla contiene un subconjunto de comandos que se pueden utilizar con **power**.

Tabla 13. Comando power

La tabla siguiente es una tabla de tres columnas y varias filas que consta de los comandos de alimentación, las descripciones de comandos y los valores asociados para los comandos.

Comando	Descripción	Valor
encender	Utilice este comando para encender la alimentación del servidor.	encendido, apagado
apagar	Utilice este comando para apagar la alimentación del servidor. **Nota:** La opción **-s** apaga el sistema operativo antes de que se apague el servidor.	encendido, apagado
apagar y encender la alimentación	Use este comando para apagar la alimentación del servidor y luego encenderla. **Nota:** La opción **-s** apaga el sistema operativo antes de que se apague el servidor.	
power enterS3	Utilice este comando para colocar el sistema operativo en el modo S3 (suspensión). **Nota:** Se utiliza este comando solo cuando el sistema operativo está encendido. El modo S3 no se admite en todos los servidores.	
power rp	Utilice esta opción para especificar la política de restauración de alimentación de host.	alwayson|alwaysoff|restore
power S3resume	Utilice este comando para activar el sistema operativo del modo S3 (suspensión). **Nota:** Se utiliza este comando solo cuando el sistema operativo está encendido. El modo S3 no se admite en todos los servidores.	
estado de energía	Utilice este comando para visualizar el estado de alimentación del servidor y el estado actual del servidor.	encendido, apagado

La siguiente tabla contiene las opciones para los comandos **power on**, **power off** y **power cycle**.

Tabla 14. Comando power

La tabla siguiente es una tabla de tres columnas y varias filas que consta de las opciones, las descripciones de las opciones y los valores asociados para las opciones.

Opción	Descripción	Valores
-s	Use esta opción para apagar el sistema operativo antes de que se apague el servidor. **Nota:** La opción **-s** es implícita al usar la opción **-every** para los comandos **power off** y **power cycle**.	
-every	Utilice esta opción con los comandos **power on**, **power off** y **power cycle** para controlar la alimentación del servidor. Puede configurar la fecha, la hora y la frecuencia (diaria o semanal) de encendido, apagado o el ciclo de alimentación del servidor.	**Nota:** Los valores para esta opción se presentan en líneas separadas debido a las limitaciones de espacio. Sun|Mon|Tue|Wed|Thu| Fri|Sat|Day|clear
-t	Utilice esta opción para especificar las horas y minutos para encender el servidor, apagar el sistema operativo y apagar o reiniciar el servidor.	Utilice el formato siguiente: hh:mm
-d	Utilice esta opción para especificar la fecha para encender el servidor. Esta es una opción adicional para el comando **power on**. **Nota:** Las opciones **-d** y **-every** no se pueden usar juntas en el mismo comando.	Utilice el formato siguiente: mm/dd/aaaa
-clear	Utilice esta opción para borrar la fecha programada de encendido. Esta es una opción adicional para el comando **power on**.	

Sintaxis:

```
power on
power off [-s]
power state
power cycle [-s]
```

La siguiente información corresponde a ejemplos del comando **power**.

Para apagar el sistema operativo y el servidor cada domingo a la 1:30, escriba el siguiente comando:

```
system> power off
-every Sun -t 01:30
```

Para apagar el sistema operativo y reiniciar el servidor cada día a la 1:30, escriba el siguiente comando:

```
system> power cycle
-every Day -t 01:30
```

Para encender el servidor cada lunes a la 1:30, especifique el comando siguiente:

```
system> power on
-every Mon -t 13:00
```

Para encender el servidor el 31 de diciembre de 2013 a las 11:30 pm, especifique el comando siguiente:

```
system> power on
-d 12/31/2013 -t 23:30
```

Para borrar un ciclo semanal de alimentación, especifique el comando siguiente:

```
system> power cycle
-every clear
```

Comando reset

Este comando describe cómo restablecer el servidor.

Utilice el comando **reset** para reiniciar el servidor. Para utilizar este comando, debe contar con autoridad de acceso a la alimentación y reinicio.

En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 15. Comando reset

La tabla siguiente es una tabla de tres columnas y varias filas que consta de las opciones, las descripciones de las opciones y los valores asociados para las opciones.

Opción	Descripción	Valores
-s	Apaga el sistema operativo antes de restablecer el servidor.	
-d	Retrasa realizar de restablecimiento por el número de segundos dados.	0 - 120
-nmi	Genera una interrupción no enmascarable (NMI) en el servidor.	

Sintaxis:

```
reset [option]
option:
-s
-d
-nmi
```

Comando fuelg

Este comando muestra información acerca de la alimentación del servidor.

Utilice el comando **fuelg** para visualizar información sobre el uso de alimentación del servidor y para configurar la gestión de alimentación del servidor. Este comando también configura las políticas para la pérdida de redundancia de alimentación. En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 16. Comando fuelg

La tabla siguiente es una tabla de tres columnas y varias filas que consta de las opciones, las descripciones de las opciones y los valores asociados para las opciones.

Opción	Descripción	Valores
-pme	Habilita o deshabilita la gestión de alimentación y limitación de alimentación en el servidor.	encendido, apagado
-pcapmode	Establece el modo de limitación de alimentación del servidor.	entrada, salida

Tabla 16. Comando fuelg (continuación)

Opción	Descripción	Valores
-pcap	Un valor de voltaje numérico que entra dentro del rango de valores de limitación de alimentación que aparece cuando se ejecuta el comando fuelg, sin opciones, en el destino.	valor numérico del voltaje
-history	Mostrar el consumo de alimentación o el historial de rendimiento	pc, rendimiento
-period	Un valor numérico para mostrar el historial (1, 6, 12, 24 horas)	valor numérico en horas
-pm	Establece el modo de política de pérdida de alimentación redundante.	• **bt**: básico con regulación • **rt**: redundante con regulación (predeterminada) • **ort**: N_1 redundante con regulación
-zm	Habilitar o deshabilitar el modo de salida cero. Esta configuración solo se puede establecer cuando el modo de la política está establecido en redundante con regulación.	encendido, apagado
-perf	Visualiza el uso actual de cálculo, incluyendo el sistema, el microprocesador y E/S.	porcentaje
-pc	Mostrar consumo de alimentación actual	• **salida**: muestra el consumo de alimentación CC actual. Para los servidores de bastidor y de torre, incluirá el consumo de energía del sistema, la CPU, la memoria y otros componentes, para los servidores blade ITE, solo incluye el consumo de alimentación del sistema. • **entrada**: muestra el consumo de alimentación de entrada actual, incluido el consumo de alimentación del sistema.

Sintaxis:

```
fuelg [options]
option:
  -pme on|off
  -pcapmode input|output
  -pcap
  -history
  -period
  -pm bt|r|rt
  -zm on|off
  -perf
  -pc input|output
```

Ejemplo:

```
system> fuelg
-pme: on
system>
```

Comando pxeboot

Este comando muestra y establece la condición del entorno de ejecución de prearranque.

Ejecutar **pxeboot** sin opciones regresa la configuración actual del entorno de ejecución de prearranque. En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 17. Comando pxeboot

La tabla siguiente es una tabla de tres columnas y una fila que consta de la opción, la descripción de la opción y los valores asociados para la opción.

Opción	Descripción	Valores
-en	Establece la condición del entorno de ejecución de prearranque para el siguiente reinicio del sistema.	habilitado, deshabilitado

Sintaxis:
```
pxeboot [options]
option:
  -en state
```

Ejemplo:
```
system> pxeboot
-en disabled
system>
```

Comando serial redirect

Este tema contiene el comando serial redirect.

Existe solo un comando serial redirect: “Comando console” en la página 115.

Comando console

Se utiliza este comando para iniciar una sesión de consola de redirección en serie.

Utilice el comando **console** para iniciar una sesión de consola de redirección en serie al puerto de serie designado del IMM.

Sintaxis:
```
console 1
```

Comandos de configuración

Este tema proporciona una lista alfabética de los comandos CLI de configuración.

Actualmente, hay 41 comandos de configuración:

Comando accseccfg

Use este comando para mostrar y configurar los valores de seguridad de la cuenta.

Ejecutar el comando **accseccfg** sin opciones muestra toda la información de seguridad de la cuenta. En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 18. Comando accseccfg

La tabla siguiente es una tabla de tres columnas y varias filas que consta de las opciones, las descripciones de las opciones y los valores asociados para las opciones.

Opción	Descripción	Valores
-am	Establece el método de autenticación del usuario.	local, ldap, localldap, ldaplocal
-lp	Periodo de bloqueo tras superar el número máximo de errores de inicio de sesión (minutos).	Entre 0 y 2880, 0 = el período de bloqueo no caduca
-pe	Periodo de caducidad de la contraseña (en días).	Entre 0 y 365, 0 = no caduca nunca
-pew	Periodo de tiempo de advertencia de caducidad de la contraseña **Nota:** El periodo de advertencia de caducidad de la contraseña debe ser menor al periodo de caducidad de la contraseña.	Entre 0 y 30, 0 = nunca advertir
-pc	Reglas de complejidad de contraseña habilitadas.	encendido, apagado
-pl	Longitud dela contraseña.	Si se habilitan las reglas de complejidad de la contraseña, la longitud de la contraseña se encuentra entre 8 y 32. De lo contrario, se encuentra entre 0 y 32.
-ci	Intervalo mínimo de cambio de contraseña (horas).	Entre 0 y 240, 0 = cambiar inmediatamente.
-lf	Número máximo de errores de inicio de sesión.	Entre 0 y 10, 0 = no bloquear nunca
-chgdft	Cambie la contraseña predeterminada en el primer inicio de sesión.	encendido, apagado
-chgnew	Cambie la contraseña de usuario nuevo en el primer inicio de sesión.	encendido, apagado
-rc	Ciclo de reutilización de la contraseña.	Entre 0 y 10, 0 = reutilizar inmediatamente.
-wt	Tiempo de espera de la sesión de inactividad de la web y del shell seguro (minutos).	Entre 0 y 1440

Syntax:

```
accseccfg [options]
option:
   -legacy
   -high
   -custom
   -am authentication method
   -lp lockout_period
   -pe time_period
   -pr state
   -pc state
   -pd number_characters
   -pl number_characters
   -ci minimum_interval
   -lf number_failures
   -chgdft state
   -chgnew state
   -rc reuse_cycle
   -wt timeout
```

Ejemplo:

```
system> accseccfg
-legacy
-am local
-lp 2
-pe 0
-pr off
-pd 1
-pl 4
-ci 0
-lf 0
-chgdft off
-chgnew off
-rc 0
-wt user
system>
```

Comando alertcfg

Use este comando para mostrar y configurar los parámetros de alerta remota global de IMM.

Ejecutar el comando **alertcfg** sin opciones muestra todos los parámetros globales de alerta remota. En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 19. Comando alertcfg

La tabla siguiente es una tabla de tres columnas y varias filas que consta de las opciones, las descripciones de las opciones y los valores asociados para las opciones.

Tabla 19. Comando alertcfg (continuación)

Opción	Descripción	Valores
-dr	Establece el tiempo de espera entre reintentos antes de que el IMM vuelva a realizar una alerta.	0 a 4,0 minutos, en incrementos de 0,5 minutos
-da	Establece el tiempo de espera antes de que el IMM envíe una alerta al destinatario siguiente en la lista.	0 a 4,0 minutos, en incrementos de 0,5 minutos
-rl	Establece el número de veces adicionales que el IMM intentará enviar una alerta, si los intentos anteriores no se completaron correctamente.	0 a 8

Sintaxis:
```
alertcfg [options]
  options:
    -rl retry_limit
    -dr retry_delay
    -da agent_delay
```

Ejemplo:
```
system>alertcfg
-dr 1.0
-da 2.5
-rl 5
system>
```

Comando asu

Este comando se utiliza para la configuración de UEFI.

Se usan los comandos de Advanced Settings Utility (ASU) para configurar UEFI. El sistema principal se debe reiniciar para que los cambios de disco de UEFI entren en vigencia.

La siguiente tabla contiene un subconjunto de comandos que se pueden utilizar con **asu**.

Tabla 20. Comando asu

La tabla siguiente es una tabla de tres columnas y varias filas que consta de un subconjunto de comandos que se pueden utilizar conjuntamente mediante el comando **asu**. Se proporciona la información descriptiva y los valores asociados para los comandos.

Comando	Descripción	Valor
suprimir	Utilice este comando para eliminar una instancia o un registro de una configuración. La configuración debe ser una instancia que permite la eliminación, por ejemplo, iSCSI.AttemptName.1.	**setting_instance**
ayuda	Utilice este comando para visualizar la información de ayuda para una o varias configuraciones.	**configuración**

Tabla 20. Comando asu (continuación)

Comando	Descripción	Valor
set	Utilice este comando para cambiar el valor de una configuración. Establece la configuración de UEFI para ingresar un valor. **Notas:** • Establece uno o varios pares de configuraciones o valores. • La configuración puede contener comodines si se amplía a una única configuración. • El valor debe delimitarse en comillas dobles, si contiene espacios. • Los valores de la lista ordenada están separados por el símbolo igual (=). Por ejemplo, establecer B*.Bootorder “CD/DVD Rom=Hard Disk 0=PXE Network.”	**setting value**
showgroups	Utilice este comando para visualizar los grupos de configuración disponibles. Este comando muestra los nombres de los grupos conocidos. Los nombres de grupo pueden variar en función de los dispositivos instalados.	**configuración**
show	Utilice este comando para visualizar el valor actual para una o varias configuraciones.	**configuración**
showvalues	Utilice este comando para visualizar todos los valores posibles para una o varias configuraciones. **Notas:** • Este comando mostrará la información sobre los valores permisibles para la configuración. • Se muestra el número mínimo y máximo de instancias permitidas para la configuración. • El valor predeterminado aparecerá, si está disponible. • El valor predeterminado aparece entre paréntesis angulares (< y >). • Los valores de texto muestran la longitud mínima y máxima y la expresión regular.	**configuración**
Notas: • En la sintaxis de comandos, **setting** es el nombre de la configuración que desea ver o cambiar y **value** es el valor que está colocando en la configuración. • **Setting** puede ser más que un nombre, excepto cuando usa el comando **set**. • **Setting** puede contener comodines, como por ejemplo un asterisco (*) o un símbolo de interrogación (?). • **Setting** puede ser un grupo, el nombre de una configuración o **all**.		

Los ejemplos de sintaxis del comando **asu** se presentan en la lista siguiente:

- Para visualizar todas las opciones del comando asu escriba `asu --help`.
- Para visualizar la ayuda detallada de todos los comandos escriba `asu -v --help`.
- Para visualizar la ayuda detallada de un comando escriba `asu -v set --help`.
- Para cambiar un valor escriba `asu set` **setting value**.
- Para visualizar el valor actual escriba `asu show` **setting**.
- Para visualizar las configuraciones en formato de lote largo escriba `asu show -l -b all`

- Para ver todos los posibles valores de una configuración escriba `asu showvalues` **setting**. Ejemplo del comando **show values**:
```
system> asu showvalues S*.POST*
SystemRecovery.POSTWatchdogTimer==<Disable>=Enable
SystemRecovery.POSTWatchdogTimerValue=numeric min=5 max=20 step=1 default=5
system>
```

En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 21. Opciones de asu

La tabla siguiente es una tabla de tres columnas y varias filas que consta de las opciones, las descripciones de las opciones y los valores asociados para las opciones.

Opción	Descripción	Valores
-b	Visualizar en formato de lote.	
--help[1]	Visualizar uso y opciones del comando. La opción --help se coloca antes del comando, por ejemplo **asu --help show**.	
--help[1]	Visualiza la ayuda del comando. La opción --help se coloca después del comando, por ejemplo **asu show --help**.	
-l	Nombre de configuración con formato largo (incluye la configuración definida).	
-m	Nombre de configuración con formato mixto (usa el Id. de configuración).	
-v[2]	Salida detallada.	

1. La opción --help se puede utilizar con cualquier comando.
2. La opción -v se utiliza solo entre **asu** y el comando.

Sintaxis:
```
asu [options] command [cmdopts]
options:
   -v verbose output
   --help display main help
cmdopts:
   --help help for the command
```

Nota: Vea comandos individuales para obtener más opciones de comando.

Utilice los comandos de transacción de asu para establecer múltiples configuraciones de UEFI y para crear y ejecutar comandos de modo por lotes. Utilice los comandos **tropen** y **trset** para crear un archivo de transacción que contiene múltiples configuraciones a aplicar. Con el comando **tropen** se abre una transacción con un Id. determinado. Los valores se añaden a la configuración mediante el comando **trset**. Con el comando **trcommit** se confirma la transacción completada. Cuando haya finalizado con la transacción, se puede eliminar con el comando **trrm**.

Nota: La operación de restauración de la configuración de UEFI creará una transacción con un Id. utilizando un número de tres dígitos aleatorio.

La siguiente tabla contiene los comandos de transacción que se pueden utilizar con **asu**.

Tabla 22. Comandos de transacción de asu

La tabla siguiente es una tabla de tres columnas y varias filas que consta de los comandos de transacciones, las descripciones de comandos y los valores asociados para los comandos.

Comando	Descripción	Valor
tropen **id**	Este comando crea un nuevo archivo de transacción que contiene varias configuraciones que se fijarán.	**Id** es la cadena de identificación, caracteres alfanuméricos de 1 a 3.
trset **id**	Este comando añade una o más configuraciones o pares de valores a una transacción.	**Id** es la cadena de identificación, caracteres alfanuméricos de 1 a 3.
trlist **id**	Este comando muestra el contenido del archivo de transacción primero. Puede ser útil cuando el archivo de transacción se crea en la carcasa de CLI.	**Id** es la cadena de identificación, caracteres alfanuméricos de 1 a 3.
trcommit **id**	Este comando confirma y ejecuta el contenido del archivo de transacción. Se muestran los resultados de la ejecución y los errores.	**Id** es la cadena de identificación, caracteres alfanuméricos de 1 a 3.
trrm **id**	Este comando elimina el archivo de transacción después de que haya confirmado.	**Id** es la cadena de identificación, caracteres alfanuméricos de 1 a 3.

Ejemplo de establecer múltiples configuraciones de UEFI:

```
asu tropen TR1
asu trset TR1 UEFI.BootModes.SystemBootMode "UEFI and Legacy"
asu trset TR1 BootOrder.BootOrder "CD/DVD Rom=Hard Disk 0=PXE Network"
asu trset TR1 BootOrder.WolBootOrder "CD/DVD Rom=Hard Disk 0=PXE Network"
asu trset TR1 UEFI.DevicesandIOPorts.Com1BaudRate 115200
asu trset TR1 UEFI.DevicesandIOPorts.Com1DataBits 8
asu trset TR1 UEFI.DevicesandIOPorts.Com1FlowControl Disable
asu trset TR1 UEFI.DevicesandIOPorts.Com1Parity None
asu trset TR1 UEFI.DevicesandIOPorts.Com1StopBits 1
asu trset TR1 UEFI.DevicesandIOPorts.COMPort1 Enable
asu trcommit TR1
```

Comando backup

Utilice este comando para crear un archivo de copia de seguridad que contiene los valores de seguridad actuales del sistema.

En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 23. Comando backup

La tabla siguiente es una tabla de tres columnas y varias filas que consta de las opciones, las descripciones de las opciones y los valores asociados para las opciones.

Opción	Descripción	Valores
-f	Nombre del archivo de copia de seguridad	Nombre de archivo válido
-pp	Contraseña o frase de paso utilizada para cifrar contraseñas en el archivo de copia de seguridad	Contraseña válida o frase de paso entre comillas
-ip	Dirección IP del servidor TFTP/SFTP	Dirección IP válida
-pn	Número de puerto del servidor TFTP/SFTP	Número de puerto válido (predeterminado 69/22)

Tabla 23. Comando backup (continuación)

Opción	Descripción	Valores
-u	Nombre de usuario para el servidor SFTP	Nombre de usuario válido
-pw	Contraseña para el servidor SFTP	Contraseña válida
-fd	Nombre del archivo para la descripción de XML de los comandos CLI de copia de seguridad	Nombre de archivo válido

Sintaxis:

```
backup [options]
  option:
   -f    filename
   -pp   password
   -ip   ip address
   -pn   port number
   -u    username
   -pw   password
   -fd   filename
```

Ejemplo:

```
system> backup f xcc-back.cli pp xxxxxx ip 192.168.70.200
ok
system>
```

Comando dhcpinfo

Utilice este comando para ver la configuración IP asignada al servidor DHCP para eth0.

Utilice el comando **dhcpinfo** para ver la configuración IP asignada al servidor DHCP para eth0, si la interfaz está configurada automáticamente por un servidor DHCP. Puede utilizar el comando **ifconfig** para habilitar o deshabilitar DHCP.

Sintaxis:

```
dhcpinfo eth0
```

Example:

```
system> dhcpinfo eth0
   -server :  10.240.0.10
   -n      :  XCC-7X19-123456789A
   -i      :  10.243.4.66
   -i6     :  ::
   -g      :  10.243.0.1
   -s      :  255.255.240.0
   -d      :  labs.lenovo.com
   -d6     :
   -dns1   :  10.240.0.10
   -dns2   :  10.240.0.11
   -dns3   :  0.0.0.0
   -dns61  :  ::
   -dns62  :  ::
   -dns63  :  ::
```

La tabla siguiente describe la salida del ejemplo.

Tabla 24. Comando dhcpinfo

La tabla siguiente es una tabla de dos columna y varias filas donde se describen las opciones utilizadas en el ejemplo anterior.

Opción	Descripción
-server	Servidor DHCP que asignó la configuración
-n	Nombre de host asignado
-i	Dirección IPv4 asignada
-g	Puerta de enlace asignada
-s	Máscara de subred asignada
-d	Nombre de dominio asignado
-dns1	Dirección IP principal del servidor DNS IPv4
-dns2	Dirección IP IPv4 de DNS secundaria
-dns3	Dirección IP terciaria del servidor DNS IPv4
-i6	Dirección IPv6
-d6	Nombre de dominio IPv6
-dns61	Dirección IP principal del servidor DNS IPv6
-dns62	Dirección IP IPv6 de DNS secundaria
-dns63	Dirección IP terciaria del servidor DNS IPv6

Comando dns

Utilice este comando para ver y establecer la configuración DNS del IMM.

Nota: En Flex System, los valores de DNS no se pueden modificar en el IMM. Las configuraciones DNS son manejadas por el CMM.

Ejecutar el comando **dns** sin opciones muestra toda la información de configuración de DNS. En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 25. Comando dns

La tabla siguiente es una tabla de tres columnas y varias filas que consta de las opciones, las descripciones de las opciones y los valores asociados para las opciones.

Opción	Descripción	Valores
-state	Estado de DNS	encendido, apagado
-ddns	Estado de DDNS	habilitado, deshabilitado
-i1	Dirección IP principal del servidor DNS IPv4	Dirección IP en formato de dirección IP con decimal separado por puntos.
-i2	Dirección IP IPv4 de DNS secundaria	Dirección IP en formato de dirección IP con decimal separado por puntos.
-i3	Dirección IP terciaria del servidor DNS IPv4	Dirección IP en formato de dirección IP con decimal separado por puntos.

Tabla 25. Comando dns (continuación)

Opción	Descripción	Valores
-i61	Dirección IP principal del servidor DNS IPv6	Dirección IP en formato IPv6.
-i62	Dirección IP IPv6 de DNS secundaria	Dirección IP en formato IPv6.
-i63	Dirección IP terciaria del servidor DNS IPv6	Dirección IP en formato IPv6.
-p	Prioridad IPv4/IPv6	ipv4, ipv6

Sintaxis:
```
dns [options]
option:
  -state state
  -ddns state
  -i1 first_ipv4_ip_address
  -i2 second_ipv4_ip_address
  -i3 third_ipv4_ip_address
  -i61 first_ipv6_ip_address
  -i62 second_ipv6_ip_address
  -i63 third_ipv6_ip_address
  -p priority
```

Nota: La ilustración siguiente muestra la configuración IMM donde está deshabilitado DNS.

Ejemplo:
```
system> dns
   -state   :  disabled
   -i1      :  0.0.0.0
   -i2      :  0.0.0.0
   -i3      :  0.0.0.0
   -i61     :  ::
   -i62     :  ::
   -i63     :  ::
   -ddns    :  enabled
   -dnsrc   :  DHCP
   -ddn     :
   -ddncur  :  labs.lenovo.com
   -p       :  ipv6
   -dscvry  :  enabled

system>
```
La tabla siguiente se describen las opciones utilizadas en el ejemplo anterior.

Tabla 26. salida del comando dns

La tabla siguiente es una tabla de dos columna y varias filas donde se describen las opciones utilizadas en el ejemplo anterior.

Opción	Descripción
-state	Estado de DNS (`on` o `off`)
-i1	Dirección IP principal del servidor DNS IPv4
-i2	Dirección IP IPv4 de DNS secundaria
-i3	Dirección IP terciaria del servidor DNS IPv4
-i61	Dirección IP principal del servidor DNS IPv6

Tabla 26. salida del comando dns (continuación)

Opción	Descripción
-i62	Dirección IP IPv6 de DNS secundaria
-i63	Dirección IP terciaria del servidor DNS IPv6
-ddns	Estado de DDNS (`enabled` o `disabled`)
-dnsrc	Nombre de dominio DDNS de preferencia (`dhcp` o `manual`)
-ddn	DDN manualmente especificado
-ddncur	DDN actual (solo lectura)
-p	Servidores DNS preferidos (`ipv4` o `ipv6`)

Comando encaps

Utilice este comando para permitir que el BMC salga del modo de encapsulación.

En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 27. Comando encaps

La tabla siguiente es una tabla de dos columna y una fila que consta de las opciones y las descripciones asociadas.

Opción	Descripción
lite off	Permite que BMC salga del modo de encapsulación y abra el acceso global a todos los usuarios

Comando ethtousb

Utilice el comando **ethtousb** para visualizar y configurar Ethernet para la asignación de puerto Ethernet sobre USB.

El comando le permite asignar un número de puerto Ethernet externo a un número de puerto diferente para Ethernet sobre USB.

Ejecutar el comando **ethtousb** sin opciones muestra toda la información de Ethernet sobre USB. En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 28. Comando ethtousb

La tabla siguiente es una tabla de tres columnas y varias filas que consta de las opciones, las descripciones de las opciones y los valores asociados para las opciones.

Tabla 28. Comando ethtousb (continuación)

Opción	Descripción	Valores
-en	Estado de Ethernet sobre USB	habilitado, deshabilitado
-m**x**	Configura la asignación de puertos para el índice **x**	Par de puertos, separados por dos puntos (:), de la forma **port1:port2** Donde: • El número de índice de puerto, **x**, se especifica como entero entre 1 y 10 en la opción de comando. • **port1** del par de puertos es el número externo del puerto Ethernet. • **port2** del par de puertos es el número del puerto Ethernet sobre USB.
-rm	Extrae la asignación de puertos para el índice especificado	1 a 10 Los índices de mapa de puerto se visualizan mediante el comando **ethtousb** sin opciones.

Sintaxis:
```
ethtousb [options]
option:
  -en state
  -mxport_pair
  -rm map_index
```

Ejemplo:
```
system> ethtousb  -en enabled -m1 100:200 -m2 101:201
system> ethtousb
 -en enabled
 -m1 100:200
 -m2 101:201
system> ethtousb -rm 1
system>
```

Comando firewall

Utilice este comando para configurar el firewall para restringir el acceso desde ciertas direcciones y, opcionalmente, limitar el marco temporal de acceso. Si no se especifica ninguna opción, se muestran los valores actuales.

En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 29. Comando firewall

La tabla siguiente es una tabla de tres columnas y varias filas que consta de las opciones y las descripciones asociadas.

Opción	Descripción	Valores
-bips	Bloquea 1 a 3 direcciones IP (separado por coma, CIDR o rango)	Direcciones IP válidas **Nota:** Las direcciones IPv4 e IPv6 pueden utilizar el formato CIDR para bloquear un rango de direcciones.
-bmacs	Bloquea 1 a 3 direcciones MAC (separado por coma)	Direcciones MAC válidas **Nota:** El filtrado de direcciones MAC solo funciona con direcciones específicas.
-bbd	Bloquea la fecha de inicio	Fecha con formato <AAAA-MM-DD>

Tabla 29. Comando firewall (continuación)

Opción	Descripción	Valores
-bed	Bloquea la fecha de finalización	Fecha con formato <AAAA-MM-DD>
-bbt	Bloquea la hora de inicio	Hora con formato <HH:MM>
-bet	Bloquea la hora de finalización	Hora con formato <HH:MM>
-bti	Intervalos de tiempo de bloques 1 a 3 (separados por comas) Por ejemplo, **firewall - bti 01:00–02:00,05:05–10:30** bloqueará el acceso durante 01:00 a 02:00 y 05:05 a 10:30 todos los días	Rango de tiempo con formato <HH:MM-HH:MM>
-clr	Borrar la regla de firewall para un tipo dado	ip, mac, datetime, interval, all
Las siguientes opciones son para el bloqueo de direcciones IP		
-iplp	Periodo de bloqueo de la dirección IP en minutos.	Valor numérico entre 0 y 2880, 0 = no caduca nunca
-iplf	Número máximo de errores de inicio de sesión antes de que la dirección IP se bloquee. **Nota:** Si este valor no es 0, debe ser mayor o igual que el <Número máximo de errores de inicio de sesión> establecido por **<accseccfg-lf>**	Valor numérico entre 0 y 32, 0 = no se bloquea nunca
-ipbl	Mostrar/configurar la lista de direcciones IP que se están bloqueando.	del, clrall, show • **-del**: eliminar una dirección IPv4 o IPv6 de la lista de bloqueo • **-clrall**: borrar todas las IP de bloqueo • **-show**: mostrar todas las IP de bloqueo

Ejemplo:

```
· “firewall”: Show all options’ value and IP addresses blocking list.
· “firewall -bips  192.168.1.1,192.168.1.0/24,192.168.1.1-192.168.1.5”: Block the access from multi IPs
· “firewall -bti 01:00-02:00,05:05-10:30,14:15-20:00”: Block all access during 01:00-02:00,05:05-10:30,14:15-20:00 every day.
· “firewall –clr all”: Clear all rules of “Block List and Time Restriction”.
· “firewall -iplp 60”:Set IP address lockout period to 60 minutes.
· “firewall -iplf 5”:Set maximum number of login failures to 5 timesi.
· “firewall -ipbl -del 192.168.100.1”:Delete 192.168.100.1 from IP address blocking list.
· “firewall –ipbl -del 3fcc:1234::2”:Delete 3fcc:1234::2 from IP address blocking list.
· “firewall –ipbl –clrall”:  Delete all blocking IP addresses.
· “firewall –ipbl –show”:    Show all blocking IP addresses.
```

Comando gprofile

Use este comando para mostrar y configurar perfiles de grupos para el IMM.

En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 30. Comando gprofile

La tabla siguiente es una tabla de tres columnas y varias filas que consta de las opciones, las descripciones de las opciones y los valores asociados para las opciones.

Tabla 30. Comando gprofile (continuación)

Opción	Descripción	Valores
-clear	Eliminar un grupo	habilitado, deshabilitado
-n	El nombre del grupo	Cadena de hasta 63 caracteres para **group_name**. El **group_name** debe ser único.
-a	Nivel de autoridad basado en roles	supervisor, operator, rbs <role list>: nsc|am|rca|rcvma|pr|bc|cel|ac Los valores de la lista de roles se especifica utilizando una lista de valores separados por una barra vertical.
-h	Visualizar uso y opciones del comando	

Sintaxis:

```
gprofile [1 - 16 group_profile_slot_number] [options]
options:
-clear state
-n  group_name
-a  authority level:
    -nsc network and security
    -am user account management
    -rca remote console access
    -rcvma remote console and remote disk access
    -pr remote server power/restart access
    -bc basic adapter configuration
    -cel ability to clear event logs
    -ac advanced adapter configuration
-h help
```

Comando hashpw

Utilice este comando con la opción-sw para habilitar/deshabilitar la función de contraseña de terceros o con la opción -re para habilitar/deshabilitar la autorización de la recuperación de la contraseña de terceros.

En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 31. Comando hashpw

La tabla siguiente es una tabla de tres columnas y varias filas que consta de las opciones, las descripciones de las opciones y los valores asociados para las opciones.

Opción	Descripción	Valores
-sw	Estado del conmutador de contraseña de terceros	habilitado, deshabilitado
-re	Estado de lectura de contraseña de terceros **Nota:** La lectura puede configurarse si el conmutador está habilitado.	habilitado, deshabilitado

Ejemplo:

```
system> hashpw -sw enabled -re enabled
system> users -5 -n guest5 -shp ef92b778bafe771e89245b89ecbc08a44a4e166c06659911881f383d4473e94f -a super
system> users -5 ghp
ef92b778bafe771e89245b89ecbc08a44a4e166c06659911881f383d4473e94f
system> users
Account      Login ID      Advanced Attribute              Role            Password Expires
```

```
-------      --------      ------------------              ------             ----------------
   1           USERID                   Native                  Administrator      Password doesn't expire
5           guest5    Third-party Password              Administrator                   90 day(s)
```

Comando ifconfig

Utilice este comando para configurar la interfaz Ethernet.

Escriba `ifconfig eth0` para visualizar la configuración actual de la interfaz Ethernet. Para cambiar la configuración de la interfaz Ethernet, escriba las opciones, seguidas por los valores. Para cambiar la configuración de la interfaz, debe tener al menos la autoridad de Red del adaptador y Configuración de seguridad.

Nota: En un Flex System, un CMM de Flex System gestiona los valores de VLAN y no se pueden modificar desde el IMM.

En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 32. Comando ifconfig

La tabla siguiente es una tabla de tres columnas y varias filas que consta de las opciones, las descripciones de las opciones y los valores asociados para las opciones.

Opción	Descripción	Valores
-b	Dirección MAC grabada (solo lectura y no configurable)	
-state	Estado de interfaz	disabled, enabled
-c	Método de configuración	dhcp, static, dthens (dthens corresponde a la opción **intentar servidor dhcp, si falla, usar configuración estática** en la interfaz web)
-i	Dirección IP estática	Dirección en formato válido.
-g	Dirección de puerta de enlace	Dirección en formato válido.
-s	Máscara de subred	Dirección en formato válido.
-n	Nombre de host	Cadena de hasta 63 caracteres. La cadena puede incluir letras, dígitos, puntos, guiones bajos y guiones.
-r	Velocidad de datos	10, 100, auto
-d	Modo dúplex	full, half, auto
-m	MTU	Números entre 60 y 1500.
-l	LAA	Formato de dirección MAC. No se permiten direcciones multidifusión (el primer byte debe ser par).
-dn	Nombre de dominio	Nombre de dominio en formato válido.
-auto	Configuración de autonegociación, que determina si la velocidad de datos y la configuración de red dúplex son configurables	verdad, falso
-ghn	Obtener nombre de host de DHCP	disabled, enabled
-nic	switch NIC mode[1]	shared, dedicated, shared:nixX[2]

Tabla 32. Comando ifconfig (continuación)

Opción	Descripción	Valores
-failover[2]	Modo de conmutación por error	none, shared, shared:nicX
-nssync[3]	Sincronización de configuración de red	habilitado, deshabilitado
-address_table	Tabla de direcciones IPv6 generadas automáticamente y sus longitudes de prefijo **Nota:** La opción es visible solo si están habilitado IPv6 y autoconfiguración sin estado.	Este valor es de solo lectura y no se puede configurar.
-ipv6	Estado de IPv6	deshabilitado, habilitado
-lla	Dirección local de enlace **Nota:** La dirección local de enlace aparece solo si IPv6 está habilitado.	El IMM determina la dirección local de enlace. Este valor es de solo lectura y no se puede configurar.
-ipv6static	Estado IPv6 estático	deshabilitado, habilitado
-i6	Dirección IP estática	Dirección IP estática para canal de Ethernet 0 en formato IPv6.
-p6	Longitud del prefijo de dirección	Números entre 1 y 128.
-g6	Puerta de enlace o ruta predeterminada	Dirección IP para la puerta de enlace o ruta predeterminada para el canal de Ethernet 0 en IPv6.
-dhcp6	Estado DHCPv6	habilitado, deshabilitado
-sa6	Estado de autoconfiguración sin estado de IPv6	habilitado, deshabilitado
-vlan	Habilitar o deshabilitar etiquetado VLAN	habilitado, deshabilitado
-vlanid	Etiqueta de identificación de paquete de red para el IMM	Números entre 1 y 4094.

Notas:

1. -nic también mostrará el estado de nic. [activo] indica cuál nic XCC está utilizando actualmente

   Por ejemplo:
   ```
   -nic: shared:nic3
   nic1: dedicate
   nic2: ext card slot #3
   nic3: ext card slot 5 [active]
   ```
   Indica que nic3 está en modo compartido, en la ranura 5, nic2 está en slot3, nic1 es un puerto dedicado de XCC y XCC está utilizando nic3.
2. El valor shared:nicX está disponible en los servidores que tienen una tarjeta de red de entretapa opcional instalada. El IMM puede usar esta tarjeta de red de entretapa.
3. Si el IMM está configurado para utilizar el puerto de red de gestión dedicado, la opción -failover ordenará el IMM para cambiar al puerto de red compartida si el puerto dedicado se desconecta.
4. Si se habilita el modo de conmutación por error, la opción -nssync ordena al IMM utilizar los mismos valores de red que se utilizan en el puerto de red de gestión dedicado del puerto de red compartida.

Sintaxis:

```
ifconfig eth0 [options]
options:

  -state interface_state
```

-c **config_method**
-i **static_ipv4_ip_address**
-g **ipv4_gateway_address**
-s **subnet_mask**
-n **hostname**
-r **data_rate**
-d **duplex_mode**
-m **max_transmission_unit**
-l **locally_administered_MAC**
-b **burned_in_MAC_address**
-dn **domain_name**
-auto **state**
-nic **state**
-failover mode
-nssync **state**
-address_table
-lla ipv6_link_local_addr
-dhcp6 **state**
-ipv6 **state**
-ipv6static **state**
-sa6 **state**
-i6 **static_ipv6_ip_address**
-g6 **ipv6_gateway_address**
-p6 **length**
-vlan **state**
-vlanid **VLAN ID**

Ejemplo:

```
system> ifconfig eth0
-state    :   enabled
-c        :   dthens
-ghn      :   disabled
-i        :   192.168.70.125
-g        :   0.0.0.0
-s        :   255.255.255.0
-n        :   IMM00096B9E003A
-auto     :   true
-r        :   auto
-d        :   auto
-vlan     :   disabled
-vlanid  :   1
-m        :   1500
-b        :   00:09:6B:9E:00:3A
-l        :   00:00:00:00:00:00
-dn       :
-ipv6     :  enabled
-ipv6static :  disabled
-i6       :  ::
-p6       :  64
-g6       :  ::
-dhcp6   :  enabled
-sa6      :  enabled
-lla      :  fe80::6eae:8bff:fe23:91ae
-nic :  shared:nic3
      nic1: dedicate
      nic2: ext card slot #3
      nic3: ext card slot #5  [active]
-address_table    :

system> ifconfig eth0 -c static -i 192.168.70.133
These configuration changes will become active after the next reset of the IMM.
```

Comando keycfg

Utilice este comando para visualizar, añadir o eliminar claves de activación.

Las claves de activación controlan el acceso a funcionalidades opcionales de IMM.

Notas:

- Cuando se ejecuta el comando **keycfg** sin opciones, se muestra la lista de claves de activación instaladas. Información clave desplegada incluye un número de índice para cada clave de activación, el tipo de clave de activación, la fecha de validez de la clave, el número de usos restantes, el estado de la clave y una descripción de la clave.
- Añada nuevas claves de activación a través de la transferencia de archivos.
- Elimine las claves antiguas especificando el número de clave o del tipo de clave. Al eliminar las claves por tipo, solo se elimina la primera clave de un tipo dado.

En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 33. Comando keycfg

La tabla siguiente es una tabla de tres columnas y varias filas que consta de las opciones, las descripciones de las opciones y los valores asociados para las opciones.

Opción	Descripción	Valores
-add	Añadir clave de activación	Valores para las opciones de comando -ip, -pn, -u, -pw y -f
-ip	Dirección IP del servidor TFTP con la clave de activación a añadir	Dirección IP válida para el servidor TFTP
-pn	Número de puerto del servidor de TFTP/SFTP con la clave de activación a añadir	Número de puerto válido para el servidor de TFTP/SFTP (valor predeterminado 69/22)
-u	Nombre de usuario del servidor de SFTP con la clave de activación a añadir	Nombre de usuario válido para el servidor SFTP
-pw	Contraseña del servidor de SFTP con la clave de activación a añadir	Contraseña válida para el servidor FTP
-f	Nombre de archivo para la clave de activación a añadir	Nombre de archivo válido para el archivo de clave de activación
-del	Eliminar clave de activación por número de índice	Número de índice válido de clave de activación de **keycfg**
-deltype	Eliminar clave de activación por tipo de clave	Valor válido del tipo de clave

Sintaxis:

```
keycfg [options]
option:
  -add
     -ip tftp/sftp server ip address
     -pn pn port number of tftp/sftp server (default 69/22)
     -u  username for sftp server
     -pw password for sftp server
     -f  filename
```

```
-del   n ( where n is a valid ID number from listing)
-deltype x ( where x is a Type value)
```

Ejemplo:

```
system> keycfg
ID  Type  Valid           Uses           Status    Description
1   4     10/10/2010      5               "valid"   "IMM remote presence"
2   3     10/20/2010      2               "valid"   "IMM feature
3   32796 NO CONSTRAINTS  NO CONSTRAINTS "valid"   "IBM Security Key Lifecycle Manager for SEDs FoD"
system>
```

Nota: El campo **Descripción** para el Id. número 3 se muestra en líneas separadas debido a las limitaciones de espacio.

Comando ldap

Use este comando para mostrar y configurar los parámetros de configuración del protocolo LDAP.

En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 34. Comando ldap

La tabla siguiente es una tabla de tres columnas y varias filas que consta de las opciones, las descripciones de las opciones y los valores asociados para las opciones.

Opción	Descripción	Valores
-a	Método de autenticación del usuario	solo local, solo LDAP, local primer y luego LDAP, LDAP primero y luego local
-aom	Modo de solo autenticación	habilitado, deshabilitado
-b	Método de vinculación	anónimo, vinculación con ClientDN y contraseña, vinculación con credencial de inicio de sesión
-c	Nombre distinguido del cliente	Cadena de hasta 127 caracteres para **client_dn**.
-d	Dominio de búsqueda	Cadena de hasta 63 caracteres para **search_domain**
-f	Filtro del grupo	Cadena de hasta 127 caracteres para **group_filter**
-fn	Nombre del bosque	Para los entornos de Active Directory. Cadena hasta de 127 caracteres.
-g	Atributo de búsqueda de grupos	Cadena de hasta 63 caracteres para **group_search_attr**
-l	Atributo de permiso de inicio de sesión	Cadena de hasta 63 caracteres para **string**
-p	Contraseña del cliente	Cadena de hasta 15 caracteres para **client_pw**
-pc	Confirmar contraseña del cliente	Cadena de hasta 15 caracteres para **confirm_pw** Uso del comando es: ldap -p **client_pw** -pc **confirm_pw** Se necesita esta opción cuando se modifica la contraseña del cliente. Compara el argumento **confirm_pw** con el argumento **client_pw**. El comando fallará si los argumentos no coinciden.
-ep	Contraseña cifrada	Contraseña de copia de seguridad/restauración (solo para uso interno)
-r	Nombre distinguido (DN) de entrada raíz	Cadena de hasta 127 caracteres para **root_dn**.

Tabla 34. Comando ldap (continuación)

Opción	Descripción	Valores
-rbs	Seguridad basada en roles mejorada para usuarios de Active Directory	habilitado, deshabilitado
-s1ip	Nombre de host/dirección IP del servidor 1	Cadena hasta de 127 caracteres o una dirección IP para **host name/ip_addr**
-s2ip	Nombre de host/dirección IP del servidor 2	Cadena hasta de 127 caracteres o una dirección IP para **host name/ip_addr**
-s3ip	Nombre de host/dirección IP del servidor 3	Cadena hasta de 127 caracteres o una dirección IP para **host name/ip_addr**
-s4ip	Nombre de host/dirección IP del servidor 4	Cadena hasta de 127 caracteres o una dirección IP para **host name/ip_addr**
-s1pn	Número de puerto del servidor 1	Un número de puerto de hasta 5 dígitos para **port_number**
-s2pn	Número de puerto del servidor 2	Un número de puerto de hasta 5 dígitos para **port_number**
-s3pn	Número de puerto del servidor 3	Un número de puerto de hasta 5 dígitos para **port_number**
-s4pn	Número de puerto del servidor 4	Un número de puerto de hasta 5 dígitos para **port_number**
-t	Nombre de servidor de destino	Cuando se habilita la opción de rbs, este campo especifica un nombre de destino que puede asociar con uno o más roles en el servidor Active Directory con la herramienta Snap-In de seguridad basada en roles (RBS).
-u	Atributo de búsqueda UID	Cadena de hasta 63 caracteres para **search_attrib**
-v	Obtiene la dirección del servidor LDAP mediante DNS	apagado, encendido
-h	Visualiza uso y opciones del comando	

Sintaxis:

```
ldap [options]
options:
   -a loc|ldap|locld|ldloc
   -aom enable/disabled
   -b anon|client|login
   -c client_dn
   -d search_domain
   -f group_filter
   -fn forest_name
   -g group_search_attr
   -l string
   -p client_pw
   -pc confirm_pw
   -ep encrypted_pw
   -r root_dn
   -rbs enable|disabled
   -s1ip host name/ip_addr
   -s2ip host name/ip_addr
   -s3ip host name/ip_addr
```

-s4ip **host name/ip_addr**
-s1pn **port_number**
-s2pn **port_number**
-s3pn **port_number**
-s4pn **port_number**
-t **name**
-u **search_attrib**
-v **off|on**
-h

Comando ntp

Use este comando para ver y configurar el protocolo de tiempo de red (NTP).

En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 35. Comando ntp

La tabla siguiente es una tabla de tres columnas y varias filas que consta de las opciones, las descripciones de las opciones y los valores asociados para las opciones.

Opción	Descripción	Valores
-en	Habilita o deshabilita el protocolo de tiempo de red.	habilitado, deshabilitado
-i[1]	Nombre o dirección IP del servidor del protocolo de tiempo de red. Este es el número de índice del servidor del protocolo de tiempo de red.	El nombre del servidor NTP a utilizar para la sincronización del reloj. El intervalo del número de índice del servidor NTP es -i1 a -i4.
-f	La frecuencia (en minutos) que el reloj de IMM se sincroniza con el servidor del protocolo de tiempo de red.	3 a 1440 minutes
-synch	Solicita una sincronización inmediata con el servidor del protocolo de tiempo de red.	Con este parámetro no se utilizan valores.

1. -i es lo mismo que i1.

Sintaxis:
```
ntp [options]
options:
-en state
-i  hostname/ip_addr
-f  frequency
-synch
```

Ejemplo:
```
system> ntp
-en: disabled
-f: 3 minutes
-i: not set
```

Comando portcfg

Utilice este comando para configurar el IMM para la característica serie de redirección.

El IMM se debe configurar para coincidir con los valores internos del puerto serie del servidor. Para cambiar la configuración de puerto de serie, escriba las opciones, seguidas por los valores. Para cambiar la configuración de puerto de serie, debe tener al menos la autoridad de Configuración del adaptador de redes y seguridad.

Nota: El puerto de serie externo del servidor solo lo puede utilizar el IMM para la funcionalidad de IPMI. La CLI no es compatible a través del puerto serie. Las opciones **serred** y **cliauth** presentes en el Remote Supervisor Adapter II CLI no están soportadas.

Ejecutar el comando **portcfg** sin opciones muestra la configuración de puerto de serie. En la tabla siguiente se muestran los argumentos para las opciones.

Nota: El número de bits de datos (8) se establece en el hardware y no se puede cambiar.

Tabla 36. Comando portcfg

La tabla siguiente es una tabla de tres columnas y varias filas que consta de las opciones, las descripciones de las opciones y los valores asociados para las opciones.

Opción	Descripción	Valores
-b	Velocidad en baudios	9600, 19200, 38400, 57600, 115200
-p	Paridad	ninguno, impar, par
-s	Bits de parada	1, 2
-climode	Modo CLI	0, 1, 2 Donde: • 0 = none: CLI deshabilitado • 1 = cliems: CLI habilitado con secuencias de teclas compatibles con EMS • 2 = cliuser: CLI habilitado con secuencias de teclas definida por el usuario

Sintaxis:
```
portcfg [options]
 options:
   -b baud_rate
   -p parity
   -s stopbits
   -climode mode
```

Ejemplo:
```
system> portcfg
-b: 57600
-climode: 2 (CLI with user defined keystroke sequence)
-p: even
-s: 1
system> portcfg -b 38400
ok
system>
```

Comando portcontrol

Utilice este comando para encender o apagar el puerto de servicio de red.

Actualmente este comando solo admite el control del puerto para el protocolo IPMI. Escriba **portcontrol** para visualizar el estado del puerto IPMI. Para habilitar o deshabilitar el puerto de red de IPMI, escriba la opción **-ipmi** seguido de los valores **on** u **off**.

Tabla 37. Comando portcontrol

La tabla siguiente es una tabla de tres columnas y varias filas que consta de las opciones, las descripciones de las opciones y los valores asociados para las opciones.

Opción	Descripción	Valores
-all	Habilitar o deshabilitar todas las interfaces y protocolos de detección	encendido, apagado
-cim	Habilita o deshabilita la detección CIM	encendido, apagado
-ipmi	Habilita o deshabilita el acceso IPMI mediante LAN	encendido, apagado
-ipmi-kcs	Habilita o deshabilita el acceso IPMI desde el servidor	encendido, apagado
-rest	Habilita o deshabilita la detección REST	encendido, apagado
-slp	Habilita o deshabilita la detección SLP	encendido, apagado
-snmp	Habilita o deshabilita la detección SNMP	encendido, apagado
-ssdp	Habilita o deshabilita la detección SSDP	encendido, apagado
-cli	Habilita o deshabilita la detección CLI	encendido, apagado
-web	Habilita o deshabilita la detección WEB	encendido, apagado

Sintaxis:

```
portcontrol [options]
 options:
   -ipmi on/off
```

Ejemplo:

```
system> portcontrol
cim : on
ipmi : on
ipmi-kcs : on
rest : on
slp : on
snmp : off
ssdp : on
cli : on
web : on
```

Comando ports

Use este comando para mostrar y configurar los puertos de IMM.

Ejecutar el comando **ports** sin opciones muestra la información de los puertos de IMM. En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 38. Comando ports

La tabla siguiente es una tabla de tres columnas y varias filas que consta de las opciones, las descripciones de las opciones y los valores asociados para las opciones.

Opción	Descripción	Valores
-open	Mostrar los puertos abiertos	
-reset	Restablecer los puertos a los valores predeterminados	
-httpp	Número de puerto HTTP	Número de puerto predeterminado: 80
-httpsp	Número de puerto HTTPS	Número de puerto predeterminado: 443
-sshp	Número de puerto CLI heredado de SSH	Número de puerto predeterminado: 22
-snmpap	Número de puerto de agente SNMP	Número de puerto predeterminado: 161
-snmptp	Número de puerto de SNMP traps	Número de puerto predeterminado: 162
-rpp	Número de puerto de presencia remota	Número de puerto predeterminado: 3900
-cimhp	Número de puerto de CIM sobre HTTP	Número de puerto predeterminado: 5988
-cimhsp	Número de puerto de CIM sobre HTTPS	Número de puerto predeterminado: 5989

Sintaxis:
```
ports [options]
option:
  -open
  -reset
  -httpp port_number
  -httpsp port_number
  -sshp port_number
  -snmpap port_number
  -snmptp port_number
  -rpp port_number
  -cimhp port_number
  -cimhsp port_number
```

Ejemplo:
```
system> ports
-httpp 80
-httpsp 443
-rpp 3900
-snmpap 161
-snmptp 162
-sshp 22
-cimhp 5988
-cimhsp 5989
system>
```

Comando rdmount

Utilice este comando para montar imágenes de disco remoto o recursos compartidos de red

En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 39. Comando rdmount

La tabla siguiente es una tabla de dos columnas y varias filas que consta de las opciones y las descripciones asociadas.

Notas:

- Se pueden cargar hasta dos archivos en la memoria del XClarity Controller y montar como medio virtual mediante la característica de RDOC del XClarity Controller. El tamaño total para ambos archivos no debe exceder 50 MB. Las imágenes cargadas son de solo lectura, a menos que se utilice la opción -rw.
- Cuando utiliza los protocolos HTTP, FTP o SFTP para montar o asignar las imágenes, el tamaño total de todas las imágenes no debe superar los 50 MB. Si se utilizan los protocolos NFS o SAMBA, no hay límites de tamaño.

Opción	Descripción
-r	Operación rdoc (si se usa, debe ser la primera opción) -r -map: monta las imágenes RDOC -r -unmap<filename>: desmonta las imágenes RDOC montadas -r-maplist: muestra las imágenes RDOC montadas mediante el navegador web de XClarity Controller y la interfaz CLI
-map	-t tipo de sistema de archivos <samba|nfs|http|sftp|ftp> -ro solo lectura -rw read-write -u usuario -p contraseña -l ubicación del archivo (formato de URL) -o opción (cadena de opción adicional para montaje de samba y nfs) -d dominio (dominio para montaje samba)
-maplist	muestra las imágenes asignadas
-unmap <id|fname>	usa el Id. con las imágenes de red, el nombre de archivo con rdoc
-mount	monta las imágenes asignadas
-unmount	desmonta las imágenes montadas

Comando restore

Utilice este comando de restaurar valores del sistema desde un archivo de copia de seguridad.

En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 40. Comando restore

La tabla siguiente es una tabla de tres columnas y varias filas que consta de las opciones, las descripciones de las opciones y los valores asociados para las opciones.

Tabla 40. Comando restore (continuación)

Opción	Descripción	Valores
-f	Nombre del archivo de copia de seguridad	Nombre de archivo válido
-pp	Contraseña o frase de paso utilizada para cifrar contraseñas en el archivo de copia de seguridad	Contraseña válida o frase de paso entre comillas
-ip	Dirección IP del servidor TFTP/SFTP	Dirección IP válida
-pn	Número de puerto del servidor TFTP/SFTP	Número de puerto válido (predeterminado 69/22)
-u	Nombre de usuario para el servidor SFTP	Nombre de usuario válido
-pw	Contraseña para el servidor SFTP	Contraseña válida

Sintaxis:
```
restore [options]
option:
  -f filename
  -pp password
  -ip ip_address
  -pn port_number
username
  -pw password
```

Ejemplo:
```
system> restore f xcc-back.cli pp xxxxxx ip 192.168.70.200
ok
system>
```

Comando restoredefaults

Utilice este comando para restaurar todas las configuraciones de IMM al valor predeterminado de fábrica.

- No existen opciones para el comando **restoredefaults**.
- Se le solicitará confirmar el comando antes de continuar.

Sintaxis:
```
restoredefaults
```

Ejemplo:
```
system> restoredefaults

This action will cause all IMM settings to be set to factory defaults.

If this is the local system, you will lose your TCP/IP connection as a result.
You will need to reconfigure the IMM network interface to restore connectivity.
After the IMM configuration is cleared, the IMM will be restarted.

Proceed? (y/n)
Y
Restoring defaults
```

Comando roles

Use este comando para mostrar o configurar los roles.

En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 41. Comando roles

La tabla siguiente es una tabla de tres columnas y varias filas que consta de las opciones, las descripciones de las opciones y los valores asociados para las opciones.

Opción	Descripción	Valores
-n	Roles a configurar	Limitado a 32 caracteres
-p	Establecer privilegios	custom:am|rca|rcvma|pr|cel|bc|nsc|ac|us • **am**: acceso de gestión de cuenta de usuario • **rca**: acceso a consola remota • **rcvma**: acceso a consola remota y disco remoto (medio virtual) • **pr**: acceso a alimentación/reinicio remoto del servidor • **cel**: capacidad de borrar registros de sucesos • **bc**: configuración del adaptador (básica) • **nsc**: configuración del adaptador (red y seguridad) • **ac**: configuración del adaptador (avanzada) • **us**: seguridad UEFI **Nota:** los indicadores de permisos personalizados anteriores se pueden utilizar en cualquier combinación
d	Eliminar una fila	

Sintaxis

```
   roles [-options] - display/configure roles
   - role_account -role number[3-31]
options:
   -n        - role name (limited to 32 characters)
   -p        - privilege (custom:am|rca|rcvma|pr|cel|bc|nsc|ac|us)
      am     - User account management access
      rca    - Remote console access
      rcvma  - Remote console and remote disk (virtual media) access
      pr     - Remote server power/restart access
      cel    - Ability to clear event logs
      bc     - Adapter Configuration (basic)
      nsc    - Adapter Configuration (network and security)
      ac     - Adapter Configuration (advanced)
      us     - UEFI Security
      Note: the above custom permission flags can be used in any combination
   -d        - delete a row
```

Ejemplo

```
system> roles -3 -n test1 -p custom:am|rca|rcvma
```

```
ok


system> roles
Account              Role                              Privilege                    Assigned To
------- ----------------------------------   -------------------------     -------------------------------
    0                    Administrator                    all                          USERID
    1                         ReadOnly                      none
    2                         Operator              custom:pr|cel|bc|nsc
    3                             test1              custom:am|rca|rcvma
```

Comando seccfg

Utilice este comando para realizar la reversión de firmware.

En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 42. Comando seccfg

La tabla siguiente es una tabla de dos columnas y varias filas que consta de las opciones y las descripciones asociadas.

Opción	Descripción	Valor
-fwrb	Permite la reversión del firmware a versiones previas	sí, no
-rppen	Habilitar la presencia física remota (solo lectura)	/
-rppto	Tiempo de espera de la presencia física remota (solo lectura)	/
-rpp	Presencia física (si está habilitado en la BIOS)	sí, no
-aubp	habilitar o deshabilitar la función de promoción automática de copia de seguridad a principal	habilitado, deshabilitado

Comando set

Utilice este comando para cambiar algunos valores de IMM.

- Algunas configuraciones de IMM se pueden cambiar con un sencillo comando **set**.
- Algunas de estas configuraciones, tales como variables de entorno, son utilizadas por la CLI.

En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 43. Comando set

La tabla siguiente es una tabla de tres columnas y una fila que consta de la descripción del comando y la información asociada.

Opción	Descripción	Valores
value	Establece el valor para la ruta o configuración especificada	Valor apropiado para la ruta o configuración especificada.

Sintaxis:
`set` [**options**]

```
option:
  value
```

Comando smtp

Use este comando para mostrar y configurar los valores de la interfaz SMTP.

Ejecutar el comando **smtp** sin opciones muestra toda la información de interfaz de SMTP. En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 44. Comando smtp

La tabla siguiente es una tabla de tres columnas y varias filas que consta de las opciones, las descripciones de las opciones y los valores asociados para las opciones.

Opción	Descripción	Valores
-auth	Soporte de autenticación SMTP	habilitado, deshabilitado
-authepw	Contraseña cifrada de autenticación SMTP	Cadena de contraseña válida
-authmd	Método de autenticación SMTP	CRAM-MD5, LOGIN
-authn	Nombre del usuario de autenticación SMTP	Cadena (límite de 256 caracteres)
-authpw	Contraseña de autenticación de SMTP	Cadena (límite de 256 caracteres)
-pn	Número de puerto SMTP	Número de puerto válido
-s	Nombre de host o dirección IP del servidor SMTP	Dirección IP o nombre de host válido (límite de 63 caracteres)

Sintaxis:

```
smtp [options]
option:
  -auth enabled|disabled
  -authepw password
  -authmd CRAM-MD5|LOGIN
  -authn username
  -authpw password
  -s ip_address_or_hostname
  -pn port_number
```

Ejemplo:

```
system> smtp
-s test.com
-pn 25
system>
```

Comando snmp

Use este comando para mostrar y configurar la información de interfaz de SNMP.

Ejecutar el comando **snmp** sin opciones muestra toda la información de interfaz de SNMP. En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 45. Comando snmp

La tabla siguiente es una tabla de tres columnas y varias filas que consta de las opciones, las descripciones de las opciones y los valores asociados para las opciones.

Tabla 45. Comando snmp (continuación)

Opción	Descripción	Valores
-a3	Agente de SNMPv3	encendido, apagado **Notas:** Para habilitar el agente SNMPv3, se debe cumplir con el siguiente criterio: • El contacto de IMM se especifica con la opción de comando -cn. • La ubicación de IMM se especifica con la opción de comando -l.
-t1	Trampas SNMPv1	encendido, apagado
-t2	Capturas SNMPv2	encendido, apagado
-t	Trampas SNMPv3	encendido, apagado
-l	Ubicación de IMM	Cadena (límite de 47 caracteres). **Notas:** • Los argumentos que contienen espacios deben estar entre comillas. No se permiten espacios antes ni después de los argumentos. • Borre la ubicación del IMM al no especificar ningún argumento o especificando una cadena vacía como argumento, como “”.
-cn	Nombre de contacto de IMM	Cadena (límite de 47 caracteres). **Notas:** • Los argumentos que contienen espacios deben estar entre comillas. No se permiten espacios antes ni después de los argumentos. • Borre el nombre de contacto del IMM al no especificar ningún argumento o especificando una cadena vacía como argumento, como “”.
-c	Nombre de comunidad SNMP	Cadena (límite de 15 caracteres). **Notas:** • Los argumentos que contienen espacios deben estar entre comillas. No se permiten espacios antes ni después de los argumentos. • Borre un nombre de comunidad de SNMP al no especificar ningún argumento o especificando una cadena vacía como argumento, como “”.
-ct	Nombre de comunidad de capturas SNMPv2	Cadena (límite de 15 caracteres). **Notas:** • Los argumentos que contienen espacios deben estar entre comillas. No se permiten espacios antes ni después de los argumentos. • Borre el nombre de contacto del IMM al no especificar ningún argumento o especificando una cadena vacía como argumento, como “”.
-ci	Nombre de host o dirección IP del comunidad SNMP	Dirección IP o nombre de host válido (límite de 63 caracteres). **Notas:** • Una dirección IP o nombre de host solo puede contener puntos, guiones bajos, signos de menos, letras y dígitos. No se permiten espacios insertados ni puntos consecutivos. • Borre una dirección IP o nombre de host de comunidad SNMP al no especificar ningún argumento.

Tabla 45. Comando snmp (continuación)

Opción	Descripción	Valores
-cti	Dirección IP de la comunidad de capturas/ nombre de host de la comunidad de capturas SNMPv2	Dirección IP o nombre de host válido (límite de 63 caracteres). **Notas:** • Una dirección IP o nombre de host solo puede contener puntos, guiones bajos, signos de menos, letras y dígitos. No se permiten espacios insertados ni puntos consecutivos. • Borre una dirección IP o nombre de host de comunidad SNMP al no especificar ningún argumento.
-eid	ID de motor SNMP	Cadena (límite de 1 de 27 caracteres)

Sintaxis:
```
snmp [options]
option:
 -a3 state
  -t state
  -l location
  -cn contact_name
  -t1 state
  -c community name
  -ci community IP address/hostname
  -t2 state
  -ct community name
  -cti community IP address/hostname
  -eid engine id
```

Ejemplo:
```
system> snmp
-t enabled
-a3 enabled
-l ZhangjiangMansion
-cn Kelvin
-t1 enabled
-c community1
-ci host1
-t2 enabled
-ct community2
-cti host2
-eid XCC-7Z70-DSYM09X
system>
```

Comando snmpalerts

Utilice este comando para gestionar las alertas enviadas mediante SNMP.

Ejecutar **snmpalerts** sin opciones muestra todos los valores de alertas de SNMP. En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 46. Comando snmpalerts

La tabla siguiente es una tabla de tres columnas y varias filas que consta de las opciones, las descripciones de las opciones y los valores asociados para las opciones.

Tabla 46. Comando snmpalerts (continuación)

Opción	Descripción	Valores
-status	Estado de alerta SNMP	encendido, apagado
-crt	Establece sucesos críticos que envían alertas	all, none, custom:te|vo|po|di|fa|cp|me|in|re|ot Las configuraciones de alertas críticas personalizadas se especifican utilizando una lista de valores separados por una barra vertical de la forma **snmpalerts -crt custom:te|vo**, donde los valores personalizados son: • te: umbral superado de temperatura crítica • vo: umbral superado de voltaje crítico • po: error crítico de alimentación • di: error de la unidad de disco duro • fa: error del ventilador • cp: error del microprocesador • me: error de memoria • in: incompatibilidad de hardware • re: error de redundancia de alimentación • ot: todos los otros sucesos críticos
-crten	Envía alertas de sucesos críticos	habilitado, deshabilitado
-wrn	Establece sucesos de advertencia que envían alertas	all, none, custom:rp|te|vo|po|fa|cp|me|ot Las configuraciones de alertas de advertencia personalizadas se especifican utilizando una lista de valores separados por una barra vertical de la forma **snmpalerts -wrn custom:rp|te**, donde los valores personalizados son: • rp: advertencia de redundancia de alimentación • te: umbral superado de temperatura de advertencia • vo: umbral superado de voltaje de advertencia • po: umbral superado de alimentación de advertencia • fa: suceso no crítico del ventilador • cp: microprocesador en estado degradado • me: advertencia de memoria • ot: todos los otros sucesos de advertencia
-wrnen	Envía alertas de sucesos de advertencia	habilitado, deshabilitado

Tabla 46. Comando snmpalerts (continuación)

Opción	Descripción	Valores
-sys	Establece sucesos de rutina que envían alertas	all, none, custom:lo|tio|ot|po|bf|til|pf|el|ne Las configuraciones de alertas de rutina personalizadas se especifican utilizando una lista de valores separados por una barra vertical de la forma **snmpalerts -sys custom:lo|tio**, donde los valores personalizados son: • lo: inicio de sesión remoto correcto • tio: tiempo de espera del sistema operativo • ot: todos los otros sucesos de información y sistema • po: encendido/apagado del sistema • bf: error de arranque del sistema operativo • til: tiempo de espera del proceso de vigilancia del cargador del sistema operativo • pf: falla prevista (PFA) • el: registro de sucesos 75 % lleno • ne: cambio de red
-sysen	Envía alertas de sucesos de rutina	habilitado, deshabilitado

Sintaxis:
```
snmpalerts [options]
   options:
     -status status
     -crt event_type
     -crten state
     -wrn event_type
     -wrnen state
     -sys event_type
     -sysen state
```

Comando srcfg

Utilice este comando para indicar la secuencia de teclas para entrar al CLI a través del modo de redirección de serie.

Para cambiar la configuración de redirección de serie, escriba las opciones, seguidas por los valores. Para cambiar la configuración de redirección de serie, debe tener al menos la autoridad de Configuración del adaptador de redes y seguridad.

Nota: El hardware del IMM no posee la capacidad de conexión de puerto de serie a puerto de serie. Por lo tanto las opciones `-passthru` y `entercliseq` presentes en el Remote Supervisor Adapter II CLI no están soportadas.

Ejecutar el comando **srcfg** sin las opciones muestra la secuencia de teclas de redirección de serie actual. En la tabla siguiente se muestran los argumentos para la opción del comando `srcfg -entercliseq`.

Tabla 47. Comando srcfg

La tabla siguiente es una tabla de tres columnas y una fila que consta de la opción, la descripción de la opción y los valores para la opción.

Tabla 47. Comando srcfg (continuación)

Opción	Descripción	Valores
-entercliseq	Escribir una secuencia de teclas de CLI	Secuencia de teclas definida por el usuario para ingresar a CLI. **Nota:** Esta secuencia debe tener al menos un carácter y un máximo de 15 caracteres. El símbolo de punto de intercalación (^) tiene un significado especial en esta secuencia. Denota Ctrl para las teclas que se correlacionan con las secuencias de Ctrl (por ejemplo, ^[para la tecla de escape y la tecla ^M para el retorno). Todas las apariciones de ^ se interpretan como parte de una secuencia de Ctrl. Consulte una tabla de conversión de ASCII a teclas para ver una lista de secuencias de Ctrl. El valor predeterminado para este campo es el ^ [(que es salida seguida por (.

Sintaxis:
```
srcfg [options]
options:
-entercliseq entercli_keyseq
```

Ejemplo:
```
system> srcfg
-entercliseq ^[Q
system>
```

Comando sshcfg

Use este comando para mostrar y configurar los parámetros de SSH.

Ejecutar el comando **sshcfg** sin opciones muestra todos los parámetros de SSH. En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 48. Comando sshcfg

La tabla siguiente es una tabla de tres columnas y varias filas que consta de las opciones, las descripciones de las opciones y los valores asociados para las opciones.

Opción	Descripción	Valores
-cstatus	Estado de SSH CLI	habilitado, deshabilitado
-hk gen	Generar la clave privada del servidor SSH	
-hk rsa	Muestra la clave pública RSA del servidor	

Sintaxis:
```
sshcfg [options]
option:
  -cstatus state
  -hk gen
  -hk rsa
```

Ejemplo:
```
system> sshcfg
-cstatus enabled
CLI SSH port 22
ssh-rsa 2048 bit fingerprint: b4:a3:5d:df:0f:87:0a:95:f4:d4:7d:c1:8c:27:51:61
1 SSH public keys installed
```

```
system>
```

Comando ssl

Use este comando para mostrar y configurar los parámetros de SSL.

Para habilitar un cliente SSL, un certificado de cliente debe estar instalado. Ejecutar el comando **ssl** sin opciones muestra los parámetros de SSL. En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 49. Comando ssl

La tabla siguiente es una tabla de tres columnas y varias filas que consta de las opciones, las descripciones de las opciones y los valores asociados para las opciones.

Opción	Descripción	Valores
-ce	Habilita o deshabilita un cliente SSL	encendido, apagado
-se	Habilita o deshabilita un servidor SSL	encendido, apagado
-cime	Habilita o deshabilita el CIM sobre HTTPS en el servidor SSL.	encendido, apagado

Sintaxis:

```
portcfg [options]
 options:
  -ce state
  -se state
  -cime state
```

Parámetros: los parámetros siguientes se presentan en la pantalla de estado de la opción para el comando **ssl** y se muestran desde la CLI:

Transporte seguro de servidor habilitado
Esta visualización de estado es de solo lectura y no se puede establecer directamente.

Estado de la clave del servidor web/CMD
Esta visualización de estado es de solo lectura y no se puede establecer directamente. Los posibles valores de salida de la línea de comandos son los siguientes:

Clave privada y certificado/CSR no disponibles

Clave privada y certificado firmado por CA instalados

Clave privada y certificado autofirmado generado automáticamente instalados

Clave privada y certificado autofirmado instalados

Clave privada almacenada, CSR disponible para descargarse

Estado de la clave CSR del servidor SSL
Esta visualización de estado es de solo lectura y no se puede establecer directamente. Los posibles valores de salida de la línea de comandos son los siguientes:

Clave privada y certificado/CSR no disponibles

Clave privada y certificado firmado por CA instalados

Clave privada y certificado autofirmado generado automáticamente instalados

Clave privada y certificado autofirmado instalados

Clave privada almacenada, CSR disponible para descargarse

Estado de la clave de cliente SSL de LDAP

Esta visualización de estado es de solo lectura y no se puede establecer directamente. Los posibles valores de salida de la línea de comandos son los siguientes:

Clave privada y certificado/CSR no disponibles

Clave privada y certificado firmado por CA instalados

Clave privada y certificado autofirmado generado automáticamente instalados

Clave privada y certificado autofirmado instalados

Clave privada almacenada, CSR disponible para descargarse

Estado de la clave de cliente SSL de CSR

Esta visualización de estado es de solo lectura y no se puede establecer directamente. Los posibles valores de salida de la línea de comandos son los siguientes:

Clave privada y certificado/CSR no disponibles

Clave privada y certificado firmado por CA instalados

Clave privada y certificado autofirmado generado automáticamente instalados

Clave privada y certificado autofirmado instalados

Clave privada almacenada, CSR disponible para descargarse

Comando sslcfg

Utilice este comando para visualizar y configurar el SSL para el IMM y gestionar los certificados.

Ejecutar el comando **sslcfg** sin opciones muestra toda la información de configuración de SSL. El comando **sslcfg** se usa para generar una nueva clave de cifrado y el certificado autofirmado o solicitud de firma de certificado (CSR). En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 50. Comando sslcfg

La tabla siguiente es una tabla de tres columnas y varias filas que consta de las opciones, las descripciones de las opciones y los valores asociados para las opciones.

Opción	Descripción	Valores
-server	Estado de servidor SSL	habilitado, deshabilitado **Nota:** El servidor SSL puede habilitarse solo si hay un certificado válido establecido.
-client	Estado de cliente SSL	habilitado, deshabilitado **Nota:** El cliente SSL puede habilitarse solo si hay un servidor o certificado de cliente válido establecido.
-cim	Estado de CIM sobre HTTPS	habilitado, deshabilitado **Nota:** CIM sobre HTTPS puede habilitarse solo si hay un servidor o certificado de cliente válido establecido.
-cert	Generar certificado autofirmado	servidor, cliente, sysdir, storekey **Notas:** • Se requieren los valores para las opciones de comando **-c**, **-sp**, **-cl**, **-on** y **-hn** al generar un certificado autofirmado. • Los valores para las opciones de comando **-cp**, **-ea**, **-ou**, **-s**, **-gn**, **-in** y **-dq** son opcionales al generar un certificado autofirmado.

Tabla 50. Comando sslcfg (continuación)

Opción	Descripción	Valores
-csr	Generar una CSR	servidor, cliente, sysdir, storekey **Notas:** • Se requieren los valores para las opciones de comando **-c**, **-sp**, **-cl**, **-on** y **-hn** al generar una CSR. • Los valores para las opciones de comando **-cp**, **-ea**, **-ou**, **-s**, **-gn**, **-in**, **-dq**, **-cpwd** y **-un** son opcionales al generar una CSR.
-i	Dirección IP para el servidor TFTP/SFTP	Dirección IP válida **Nota:** Se debe especificar una dirección IP para el servidor TFTP o SFTP al cargar un certificado o descargar un certificado o CSR.
-pn	Número de puerto del servidor TFTP/SFTP	Número de puerto válido (predeterminado 69/22)
-u	Nombre de usuario para el servidor SFTP	Nombre de usuario válido
-pw	Contraseña para el servidor SFTP	Contraseña válida
-l	Nombre de archivo del certificado	Nombre de archivo válido **Nota:** Se requiere un nombre de archivo al descargar o cargar un certificado o una CSR. Si no se especifica ningún nombre de archivo para una descarga, se utiliza y se visualiza el nombre predeterminado para el archivo.
-dnld	Descargar archivo de certificado	Esta opción no toma ningún argumento; pero también debe especificar los valores para la opción de comando **-cert** o **-csr** (en función del tipo de certificado que se descarga). Esta opción no toma ningún argumento; pero también se deben especificar valores para la opción de comando **-i** y **-l** (opcional).
-upld	Importar archivo de certificado	Esta opción no toma ningún argumento; pero también se deben especificar valores para las opciones de comando **-cert**, **-i** y **-l**.
-tc**x**	Certificado de confianza **x** para el cliente SSL	importar, descargar, eliminar **Nota:** El número de certificado de confianza, **x**, se especifica como entero entre 1 y 3 en la opción de comando.
-c	País	Código de país (2 letras) **Nota:** Requerido al generar un certificado autofirmado o una CSR.
-sp	Estado o provincia	Cadena entre comillas (máximo de 60 caracteres) **Nota:** Requerido al generar un certificado autofirmado o una CSR.
-cl	Ciudad o localidad	Cadena entre comillas (máximo de 50 caracteres) **Nota:** Requerido al generar un certificado autofirmado o una CSR.
-on	Nombre de la organización	Cadena entre comillas (máximo de 60 caracteres) **Nota:** Requerido al generar un certificado autofirmado o una CSR.
-hn	Nombre de host del IMM	Cadena (máximo de 60 caracteres) **Nota:** Requerido al generar un certificado autofirmado o una CSR.
-cp	Persona de contacto	Cadena entre comillas (máximo de 60 caracteres) **Nota:** Opcional al generar un certificado autofirmado o una CSR.
-ea	Dirección de correo electrónico de la persona de contacto	Dirección de correo electrónico válida (máximo de 60 caracteres) **Nota:** Opcional al generar un certificado autofirmado o una CSR.

Tabla 50. Comando sslcfg (continuación)

Opción	Descripción	Valores
-ou	Unidad organizativa	Cadena entre comillas (máximo de 60 caracteres) **Nota:** Opcional al generar un certificado autofirmado o una CSR.
-s	Apellido	Cadena entre comillas (máximo de 60 caracteres) **Nota:** Opcional al generar un certificado autofirmado o una CSR.
-gn	Nombre	Cadena entre comillas (máximo de 60 caracteres) **Nota:** Opcional al generar un certificado autofirmado o una CSR.
-in	Iniciales	Cadena entre comillas (máximo de 20 caracteres) **Nota:** Opcional al generar un certificado autofirmado o una CSR.
-dq	Calificador de nombre de dominio	Cadena entre comillas (máximo de 60 caracteres) **Nota:** Opcional al generar un certificado autofirmado o una CSR.
-cpwd	Contraseña de desafío	Cadena (mínimo de 6 caracteres y máximo de 30 caracteres) **Nota:** Opcional a generar una CSR.
-un	Nombre no estructurado	Cadena entre comillas (máximo de 60 caracteres) **Nota:** Opcional a generar una CSR.

Sintaxis:

```
sslcfg [options]
option:
  -server state
  -client state
  -cim state
  -cert certificate_type
  -csr certificate_type
  -i ip_address
portin number
username
  -pw password
  -l filename
  -dnld
  -upld
  -tc xaction
  -c country_code
  -sp state_or_province
  -cl city_or_locality
  -on organization_name
  -hn bmc_hostname
  -cp contact_person
  -ea email_address
  -ou organizational_unit
  -s surname
  -gn given_name
  -in initials
  -dq dn_qualifier
  -cpwd challenge_password
  -un unstructured_name
```

Ejemplos:

```
system> sslcfg
-server enabled
-client disabled
-sysdir enabled
SSL Server Certificate status:
```

```
 A self-signed certificate is installed
SSL Client Certificate status:
 A self-signed certificate is installed
SSL CIM Certificate status:
 A self-signed certificate is installed
SSL Client Trusted Certificate status:
 Trusted Certificate 1: Not available
 Trusted Certificate 2: Not available
 Trusted Certificate 3: Not available
 Trusted Certificate 4: Not available
```

Ejemplos de certificados de cliente:

- Para generar una CSR para una clave de almacenamiento, especifique el comando siguiente:
  ```
  system> sslcfg
  -csr storekey -c US -sp NC -cl rtp -on Lenovo -hn XCC-5cf3fc6e0c9d
  -cp Contact -ea "" -ou""
  ok
  ```

El ejemplo anterior se muestra en varias líneas, debido a las limitaciones de espacio.

- Para descargar un certificado desde el IMM a otro servidor, especifique el comando siguiente:
  ```
  system> sslcfg
  -csr storekey -dnld -i 192.168.70.230 -l storekey.csr
  ok
  ```
- Para cargar el certificado procesado por la autoridad de certificación (CA), especifique el comando siguiente:
  ```
  system> sslcfg
  -cert storekey -upld -i 192.168.70.230 -l tklm.der
  ```
- Para generar un certificado autofirmado, especifique el comando siguiente:
  ```
  system> sslcfg
  -cert storekey -c US -sp NC -cl rtp -on Lenovo -hn XCC-5cf3fc6e0c9d
  -cp Contact -ea "" -ou "
  ok
  ```

  El ejemplo anterior se muestra en varias líneas, debido a las limitaciones de espacio.

Ejemplo de certificado de servidor SKLM:

- Para importar el certificado de servidor SKLM, especifique el comando siguiente:
  ```
  system> storekeycfg
  -add -ip 192.168.70.200 -f tklm-server.der
  ok
  ```

Comando storekeycfg

Utilice este comando para configurar el nombre de host o la dirección IP y el puerto de red para un servidor SKLM.

Puede configurar hasta cuatro destinos de servidor SKLM. El comando **storekeycfg** también se utiliza para instalar y eliminar los certificados que utiliza el IMM para la autenticación en el servidor SKLM.

En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 51. Comando storekeycfg

La tabla siguiente es una tabla de tres columnas y varias filas que consta de las opciones, las descripciones de las opciones y los valores asociados para las opciones.

Tabla 51. Comando storekeycfg (continuación)

Opción	Descripción	Valores
-add	Añadir la clave de activación	Los valores para las opciones de comando son -ip, -pn, -u, -pw y -f
-ip	Nombre de host o dirección IP para el servidor TFTP/ SFTP	Nombre de host o dirección IP válida para el servidor TFTP/SFTP
-pn	Número de puerto del servidor TFTP o SFTP	Número de puerto válido para el servidor de TFTP/SFTP (valor predeterminado 69/22)
-u	Nombre de usuario para el servidor SFTP	Nombre de usuario válido para el servidor SFTP
-pw	Contraseña para el servidor SFTP	Contraseña válida para el servidor FTP
-f	Nombre de archivo para la clave de activación	Nombre de archivo válido para el archivo de clave de activación
-del	Utilice este comando para eliminar la clave de activación por número de índice	Número de índice válido de clave de activación de keycfg
-dgrp	Añade el grupo de dispositivos	Nombre del grupo de dispositivos
-sxip	Añade el nombre de host o dirección IP para el servidor SKLM	Nombre de host o dirección IP válida para el servidor SKLM. Valor numérico de 1, 2, 3 o 4.
-sxpn	Añade el número de puerto del servidor SKLM	Número de puerto válido para el servidor SKLM. Valor numérico de 1, 2, 3 o 4.
-testx	Prueba la configuración y la conexión con el servidor SKLM	Valor numérico de 1, 2, 3 o 4
-h	Visualizar uso y opciones del comando	

Sintaxis:

```
storekeycfg [options]
 options:
  -add state
  -ip ip_address
  -pn port_number
  -u username
  -pw password
  -f filename
  -del key_index
  -dgrp device_group_name
  -sxip ip_address
  -sxpn port_number
  -testx numeric value of SKLM server
  -h
```

Ejemplos:

Para importar el certificado de servidor SKLM, especifique el comando siguiente:

```
system> storekeycfg
add -ip 192.168.70.200 -f tklm-server.der
```

```
system> ok
```

Para configurar la dirección y el número de puerto del servidor SKLM, especifique el comando siguiente:

```
system> storekeycfg
-s1ip 192.168.70.249
system> ok
```

Para establecer el nombre de grupo de dispositivo, especifique el comando siguiente:

```
system> storekeycfg
-dgrp IBM_SYSTEM_X_SED
system> ok
```

Comando syncrep

Utilice este comando para iniciar la sincronización de firmware desde el repositorio remoto.

En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 52. Comando syncrep

La tabla siguiente es una tabla de tres columnas y varias filas que consta de las opciones, las descripciones de las opciones y los valores asociados para las opciones.

Opción	Descripción	Valores
-t	Protocolo para conectar el repositorio	samba, nfs
-l	Ubicación del repositorio remoto	En formato URL
-u	Usuario	
-p	Contraseña	
-o	Opción	Cadena de opción adicional para montaje de samba y nfs
-d	Dominio	Dominio para montaje samba
-q	Estado de actualización actual de la consulta	
-c	Cancelar el proceso de sincronización	

Sintaxis

```
syncrep [options]  Launch firmware sync from remote repository
options:
     -t <samba|nfs> protocol to connect repository
     -l location of remote repository (URL format)
     -u User
     -p Password
     -o option (extra option string for samba and nfs mounts)
     -d domain (domain for samba mount)
     -q query current update status
     -c cancel the sync process
```

Ejemplo

```
(1) start sync with repository
system> syncrep -t samba -l url -u user -p password
(2) query current update status
system> syncrep -q
(3)cancel the sync process
system> syncrep -c
```

Comando thermal

Utilice este comando para visualizar y configurar la política de modo térmico del sistema host.

Ejecutar el comando **thermal** sin opciones muestra la política de modo térmico. En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 53. Comando thermal

La tabla siguiente es una tabla de tres columnas y varias filas que consta de las opciones, las descripciones de las opciones y los valores asociados para las opciones.

Opción	Descripción	Valores
-mode	Selección de modo térmico	normal, rendimiento, mínimo, eficacia, personalizado
-table	Proveedor, identificación de dispositivo (Id.) y tabla térmica alternativa	

Sintaxis:
```
thermal [options]
option:
  -mode thermal_mode
  -table vendorID_devicetable_number
```

Ejemplo:
```
system> thermal
-mode normal
-table 80860126 1 10DE0DFA 3
system>
```

Comando timeouts

Utilice este comando para visualizar o cambiar los valores de tiempo de espera.

- Para mostrar los tiempos de espera, escriba `timeouts`.
- Para cambiar los valores de tiempo de espera, escriba las opciones, seguidas por los valores.
- Para cambiar los valores de tiempo de espera, debe contar con una autoridad mínima de configuración del adaptador.

En la tabla siguiente se muestran los argumentos para los valores de tiempo de espera. Estos valores coinciden con las opciones graduadas de escala hacia abajo para los tiempos de espera del servidor en la interfaz de la web.

Tabla 54. Comando timeouts

La tabla siguiente es una tabla de cuatro columnas y varias filas que consta de las opciones, las descripciones de las opciones y los valores asociados para las opciones.

Opción	Tiempo de espera	Unidades	Valores
-f	Retardo de apagado	minutos	disabled, 0.5, 1, 2, 3, 4, 5, 7.5, 10, 15, 20, 30, 60, 120
-l	Tiempo de espera del cargador	minutos	disabled, 0.5, 1, 1.5, 2, 2.5, 3, 3.5, 4, 4.5, 5, 7.5, 10, 15, 20, 30, 60, 120

Tabla 54. Comando timeouts (continuación)

Opción	Tiempo de espera	Unidades	Valores
-o	Tiempo de espera del sistema operativo	minutos	disabled, 2.5, 3, 3.5, 4
-s	Captura de pantalla de error del SO con error de hardware	/	disabled, enabled

Sintaxis:
```
timeouts [options]
options:
-f power_off_delay_watchdog_option
-o OS_watchdog_option
-l loader_watchdog_option
-s OS failure screen capture with HW error
```

Ejemplo:
```
system> timeouts
-o disabled
-l 3.5
-f disabled
-s disabled
system> timeouts -o 2.5
ok
system> timeouts
-o 2.5
-l 3.5
-f disabled
-s disabled
```

Comando tls

Utilice este comando para establecer el nivel mínimo de TLS.

En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 55. Comando tls

La tabla siguiente es una tabla de tres columnas y varias filas que consta de las opciones, las descripciones de las opciones y los valores asociados para las opciones.

Opción	Descripción	Valores
-min	Seleccione el nivel mínimo de TLS	1.0, 1.1, 1.2[1], 1.3
-h	Enumera el uso y las opciones	

Notas:

1. Cuando la modalidad de criptografía está definida en modo de conformidad de NIST-800-131A, la versión de TLS debe establecerse en 1.2.

Utilización:
```
tls [-options] - configures the minimum TLS level
   -min <1.0 | 1.1 | 1.2 | 1.3> - Selects the minimum TLS level
   -h - Lists usage and options
```

Ejemplos:

Para obtener el uso para el comando tls, emita el comando siguiente:
```
system> tls
-h
system>
```

Para obtener la versión actual de tls, emita el comando siguiente:
```
system> tls
-min 1.2
system>
```

Para cambiar la versión actual de tls a 1.2, emita el comando siguiente:
```
system> tls
-min 1.2
ok
system>
```

Comando trespass

Use este comando para configurar y mostrar los mensajes de advertencia de intrusión.

El comando **trespass** se puede usar para configurar y mostrar los mensajes de advertencia de intrusión. Los mensajes de advertencia de intrusión se mostrarán a cualquier usuario que inicie sesión a través de la interfaz WEB o CLI.

En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 56. Comando uefipw

La tabla siguiente es una tabla de dos columnas y varias filas que consta de las opciones y las descripciones asociadas.

Opción	Descripción
-s	Configurar mensajes de advertencia de intrusión
-h	Enumera el uso y las opciones

Sintaxis:
```
usage:
   trespass display the trespass message
   -s <trespass message> configure trespass message
   -h - Lists usage and options
```

Ejemplo:

Nota: El mensaje de advertencia de intrusión no contiene espacios.

```
system> trespass -s testingmessage
ok
system> trespass
testingmessage

The trespass message contains spaces:
system> trespass -s "testing message"
ok
system> trespass
testing message
```

Comando uefipw

Utilice este comando para configurar las contraseñas de gestión de UEFI. La contraseña es de solo escritura.

El comando **uefipw** puede utilizarse con la opción “-p” para configurar la contraseña de administrador de UEFI para XCC o con la opción “-ep” para LXCA para configurar la contraseña de administrador de UEFI mediante la interfaz CLI. La contraseña es de solo escritura.

En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 57. Comando uefipw

La tabla siguiente es una tabla de dos columnas y varias filas que consta de las opciones y las descripciones asociadas.

Opción	Descripción
-cp	Contraseña actual (limitada a 20 caracteres)
-p	Nueva contraseña (limitada a 20 caracteres)
-cep	Contraseña actual cifrada
-ep	Nueva contraseña cifrada

Sintaxis:

```
usage:
   uefipw [-options] - Configure the UEFI admin password
options:
   -cp      - current password (limited to 20 characters)
   -p       - new password (limited to 20 characters)
   -cep     - current password encrypted
   -ep      - new password encrypted
```

Comando usbeth

Use este comando para habilitar o deshabilitar la interfaz en banda de LAN sobre USB.

Sintaxis:

```
usbeth [options]
options:
-en <enabled|disabled>
```

Ejemplo:

```
system>usbeth
-en : disabled
system>usbeth -en enabled
ok
system>usbeth
-en : disabled
```

Comando usbfp

Utilice este comando para controlar el uso de BMC del puerto USB del panel frontal

En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 58. Comando usbfp

La tabla siguiente es una tabla de dos columnas y varias filas que consta de las opciones y las descripciones asociadas.

Opción	Descripción
-mode <bmc | server | shared>	Establece el modo de uso a BMC, servidor o compartido
-it <minutes>	Tiempo de espera por inactividad en minutos (modo compartido)
-btn <on | off>	Habilitar utilizando el botón de ID para alternar propietario (modo compartido)
-own <bmc | server >	Establecer propietario a bmc o servidor (modo compartido)

Comando users

Utilice este comando para acceder a todas las cuentas de usuario y a sus niveles de autoridad.

El comando **users** también se utiliza para crear nuevas cuentas de usuario y de modificar las cuentas existentes. Ejecutar el comando **users** sin opciones muestra una lista de usuarios e información básica sobre el usuario. En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 59. Comando users

La tabla siguiente es una tabla de tres columnas y varias filas que consta de las opciones, las descripciones de las opciones y los valores asociados para las opciones.

Opción	Descripción	Valores
-**user_index**	Número de índice de cuenta de usuario	1 a 12, incluido, o `all` para todos los usuarios.
-n	Nombre de cuenta de usuario	Cadena única que contiene solo números, letras, puntos, y guiones bajos. Mínimo de 4 caracteres y máximo de 16 caracteres.
-p	Contraseña de cuenta de usuario	Cadena que contiene al menos un carácter alfabético y uno no alfabético. Mínimo de 6 caracteres y máximo de 20 caracteres. Cero crea una cuenta sin contraseña que el usuario debe establecer durante el primer inicio de sesión.
-a	Nivel de autoridad	El nivel de autoridad puede ser uno de los siguientes niveles: • `super` (supervisor) • `ro` (solo lectura) • Cualquier combinación de los siguientes valores, separados por |: – `am` (acceso de gestión de cuenta de usuario) – `rca` (acceso a consola remota) – `rcvma` (acceso a consola remota y medio virtual) – `pr` (acceso a alimentación/reinicio remoto del servidor) – `cel` (capacidad de borrar registros de sucesos) – `bc` (configuración del adaptador [básica]) – `nsc` (configuración del adaptador [red y seguridad]) – `ac` (configuración del adaptador [avanzada])
-ep	Contraseña de cifrado (para copia de seguridad/ restauración)	Contraseña válida

Tabla 59. Comando users (continuación)

Opción	Descripción	Valores
-clear	Borra la cuenta de usuario especificada Si cuenta con la autorización, puede eliminar su propia cuenta o la cuenta de otros usuarios, incluso si inició sesión, a menos que sea la única cuenta restante con privilegios de gestión de cuentas de usuario. Las sesiones que ya están en progreso cuando se eliminan las cuentas de usuario no se finalizarán automáticamente.	Se debe especificar el número de índice de la cuenta de usuario a borrar, siguiendo la forma: `users -clear -`**user_index**
-curr	Muestra los usuarios actualmente conectados	
-sauth	Protocolo de autenticación SNMPv3	HMAC-SHA, ninguno
-spriv	Protocolo de privacidad SNMPv3	CBC-DES, AES, ninguno
-spw	Contraseña de privacidad SNMPv3	Contraseña válida
-sepw	Contraseña de privacidad SNMPv3 (cifrada)	Contraseña válida
-sacc	Tipo de acceso de SNMPv3	get, set
-strap	Nombre de host de interrupción SNMPv3	Nombre de host válido
-pk	Mostrar clave pública SSH para el usuario	Número de índice de cuenta de usuario. **Notas:** • Se muestra cada clave SSH asignada al usuario, junto con un número de índice de clave de identificación. • Al usar las opciones de clave pública SSH, se debe usar la opción `-pk` después del índice de usuario (opción -**userindex**), de la forma: `users -2 -pk`. • Todas las claves están en formato OpenSSH. • Para los nodos Flex, los comandos de usuarios solo se limitan a las cuentas IPMI y SNMP locales. La opción `-pk` no es compatible con Flex Systems.
-e	Muestra la clave SSH completa en formato OpenSSH **(Opción clave pública SSH)**	Esta opción no toma ningún argumento y se debe utilizar en forma exclusiva del resto de las opciones `users -pk`. **Nota:** Al usar las opciones de clave pública SSH, se debe usar la opción `-pk` después del índice de usuario (opción -**userindex**), de la forma: `users -2 -pk -e`.

Tabla 59. Comando users (continuación)

Opción	Descripción	Valores
-remove	Quitar clave pública SSH del usuario **(Opción clave pública SSH)**	Se debe entregar el número de índice de clave pública a eliminar como un -**key_index** específico o `-all` o para todas las claves asignadas al usuario. **Notas:** • Al usar las opciones de clave pública SSH, se debe usar la opción `-pk` después del índice de usuario (opción -**userindex**), de la forma: `users -2 -pk -remove -1`. • Para los nodos Flex, los comandos de usuarios solo se limitan a las cuentas IPMI y SNMP locales. La opción `-remove` no es compatible con Flex Systems.
-add	Añadir clave pública SSH para el usuario **(Opción clave pública SSH)**	Clave entre comillas en formato OpenSSH **Notas:** • La opción `-add` no se puede ejecutar al mismo tiempo que otras opciones de comando `users -pk`. • Al usar las opciones de clave pública SSH, se debe usar la opción `-pk` después del índice de usuario (opción -**userindex**), de la forma: `users -2 -pk -add "AAAAB3NzC1yc2EAAAABIwAAA QEAvfnTUzRF7pdBuaBy4dO/aIFasa/Gtc+o/wlZnuC4aD HMA1UmnMyLOCiIaNOy4OOICEKCqjKEhrYymtAoVtfKApv Y39GpnSGRC/ qcLGWLM4cmirKL5kxHNOqIcwbT1NPceoKH j46X7E +mqlfWnAhhjDpcVFjagM3Ek2y7w/tBGrwGgN7DP HJU1tzcJy68mEAnIrzjUoR98Q3/B9cJD77ydGKe8rPdI2 hIEpXR5dNUiupA1Yd8PSSMgdukASKEd3eRRZTBl3SAtMu cUsTkYjlXcqex1OQz4+N5OR6MbNcwlsx+mTEAvvcpJhug a7OUNPGhLJMl6k7jeJiQ8Xd2p XbOZQ=="` • Para los nodos Flex, los comandos de usuarios solo se limitan a las cuentas IPMI y SNMP locales. La opción `-add` no es compatible con Flex Systems.
-upld	Cargar una clave pública SSH **(Opción clave pública SSH)**	Requiere las opciones `-i` y `-l` para especificar la ubicación de la clave. **Notas:** • La opción `-upld` no se puede ejecutar al mismo tiempo que otras opciones de comando `users -pk` (excepto para `-i` y `-l`). • Para sustituir una clave por una nueva clave, debe especificar -**key_index**. Para añadir una clave al final de la lista de claves actuales, no especifique un índice de claves. • Al usar las opciones de clave pública SSH, se debe usar la opción `-pk` después del índice de usuario (opción -**userindex**), de la forma: `users -2 -pk -upld -i tftp://9.72.216.40/ -l file.key`. • Para los nodos Flex, los comandos de usuarios solo se limitan a las cuentas IPMI y SNMP locales. La opción `-upld` no es compatible con Flex Systems.
-dnld	Descarga la clave pública SSH especificada **(Opción clave pública SSH)**	Requiere -**key_index** para especificar la clave a descargar y las opciones `-i` y `-l` para especificar la ubicación de descarga en otro equipo que ejecute un servidor TFTP. **Notas:** • La opción `-dnld` no se puede ejecutar al mismo tiempo que otras opciones de comando `users -pk` (excepto para `-i`, `-l` y -**key_index**). • Al usar las opciones de clave pública SSH, se debe usar la opción `-pk` después del índice de usuario (opción -**userindex**), de la forma: `users -2 -pk -dnld -1 -i tftp://9.72.216.40/ -l file.key`.

Tabla 59. Comando users (continuación)

Opción	Descripción	Valores
-i	Dirección IP del servidor TFTP/SFTP para cargar o descargar un archivo de clave **(Opción clave pública SSH)**	Dirección IP válida **Nota:** La opción `-i` es necesaria por las opciones de comando `users -pk -upld` y `users -pk -dnld`.
-pn	Número de puerto del servidor TFTP/SFTP **(Opción clave pública SSH)**	Número de puerto válido (predeterminado 69/22) **Nota:** Un parámetro opcional para las opciones de comando `users -pk -upld` y `users -pk -dnld`.
-u	Nombre de usuario para el servidor SFTP **(Opción clave pública SSH)**	Nombre de usuario válido **Nota:** Un parámetro opcional para las opciones de comando `users -pk -upld` y `users -pk -dnld`.
-pw	Contraseña para el servidor SFTP **(Opción clave pública SSH)**	Contraseña válida **Nota:** Un parámetro opcional para las opciones de comando `users -pk -upld` y `users -pk -dnld`.
-l	Nombre de archivo para cargar o descargar un archivo de clave a través de TFTP o SFTP **(Opción clave pública SSH)**	Nombre de archivo válido **Nota:** La opción `-l` es necesaria por las opciones de comando `users -pk -upld` y `users -pk -dnld`.
-af	Acepta conexiones de host **(Opción clave pública SSH)**	Una lista separada por comas de nombres de host y de direcciones IP, limitada a 511 caracteres. Caracteres válidos incluye: alfanuméricos, la coma, el asterisco, el signo de interrogación, el signo de exclamación, el guion, el punto, los dos puntos y el porcentaje.
-cm	Comentario **(Opción clave pública SSH)**	Cadena entre comillas de hasta 255 caracteres. **Nota:** Al usar las opciones de clave pública SSH, se debe usar la opción `-pk` después del índice de usuario (opción **-userindex**), de la forma: `users -2 -pk -cm "This is my comment."`.

Sintaxis:

```
users [-options] - display/configure user accounts
options:
   -[1-12]  - user account number
   -l       - display password expiration days
   -n       - username (limited to 16 characters)
   -p       - password (limited to 32 characters)
   -shp     - set hashpassword (total 64 characters)
   -ssalt   - set salt (limited to 64 characters)
   -ghp     - get hashpassword
   -gsalt   - get salt
   -ep      - encrypted password (used with backup/restore )

   -a       - authority level (super, ro, custom:am|rca|rcvma|pr|cel|bc|nsc|ac)
       -am    - User account management access
       -rca   - Remote console access
       -rcvma - Remote console and remote disk (virtual media) access
       -pr    - Remote server power/restart access
       -cel   - Ability to clear event logs
```

```
      -bc    - Adapter Configuration (basic)
      -nsc   - Adapter Configuration (network and security)
      -ac    - Adapter Configuration (advanced)

   -clear   - clear user account
   -curr    - display current users
   -sauth   (none|HMAC-SHA)           - snmpv3 authentication protocol
   -spriv   (none|CBC-DES|AES)        - snmpv3 privacy protocol
   -spw     password                    - snmpv3 privacy password
   -sepw    encryptedpassword          - snmpv3 privacy password (encrypted)
   -sacc    (Get)                  - snmpv3 Access type
   -strap   hostname                    - snmpv3 trap hostname

   -pk      - SSH public keys options:
       -e       - Displays the entire key in OpenSSH format
       -remove  - Removes the specified key for the specified user
       -add     - Adds a public key for the specified user
       -upld    - Used to upload a public key in OpenSSH/RFC4716 format
       -dnld    - Used to download the specified public key to a TFTP/SFTP server
       -i       - IP address of the TFTP/SFTP
       -pn      - port number of tftp/sftp server (default 69/22)
       -u       - username for sftp server
       -pw      - password for sftp server
       -l       - Filename of the key file when uploading or downloading via TFTP/SFTP
       -af      - accept connections from host, in the format: from="<list>", where
                  <list> is a comma-separated list of hostnames and IP addresses
                  (limited to 511 characters)
       -cm      - comment (limited to 255 characters, must be quote-delimited)
```

Nota: -un indicadore de permisos personalizados se puede utilizar en cualquier combinación.

Ejemplo:

```
system> users
 Account      Login ID      Advanced Attribute              Role             Password Expires
 -------      --------       ------------------             ------             ----------------
    1           USERID                   Native                 Administrator                    89 day(s)
system> users -2 -n sptest -p PasswOrd12 -a super
The user is required to change the password when the user logs in to the management server for the first time
ok
system> users
 Account      Login ID      Advanced Attribute             Role               Password Expires
 -------      --------       ------------------            ------              ----------------
    1           USERID                   Native           Administrator                   90 day(s)
2           sptest                  Native                 Administrator            Password expired
system> hashpw -sw enabled -re enabled
system> users -5 -n guest5 -shp 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee -ssalt abc -a super
system> users -5 ghp
292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee
system> users -5 gsalt
abc
system> users -2 -n sptest -p PasswOrd12 -a custom:am|rca
The user is required to change the password when the user logs in to the management server for the first time
ok
```

Comandos de control del IMM

Este tema proporciona una lista alfabética de los comandos de control CLI del IMM.

Actualmente, hay 7 comandos de control IMM:

Comando alertentries

Utilice este comando para gestionar los destinatarios de alertas.

- **alertentries** sin opciones muestra todos los valores de entrada de las alertas.
- **alertentries -number -test** genera una alerta de prueba para el número de índice del destinatario dado.
- **alertentries -number** (con número de 0 a 12) muestra los valores de entrada de alerta para el número de índice del destinatario especificado o permite que se modifiquen los valores de alertas para ese destinatario.

En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 60. Comando alertentries

La tabla siguiente es una tabla de tres columnas y varias filas que consta de las opciones, las descripciones de las opciones y los valores asociados para las opciones.

Opción	Descripción	Valores
-number	El número de índice del destinatario de alerta para visualizar, añadir, modificar o eliminar.	1 a 12
-status	Estado de destinatario de alerta	encendido, apagado
-type	Tipo de alerta	correo electrónico, syslog
-log	Incluir el registro de sucesos del correo electrónico de alerta	encendido, apagado
-n	Nombre del destinatario de alerta	Cadena
-e	Dirección de correo electrónico del destinatario de alerta	Dirección de correo electrónico válida
-ip	Dirección IP o nombre de host de Syslog	Nombre de host o dirección IP válida
-pn	Número de puerto de Syslog	Número de puerto válido
-del	Elimina el número de índice del destinatario especificado	
-test	Genera una alerta de prueba al número de índice del destinatario especificado	

Tabla 60. Comando alertentries (continuación)

Opción	Descripción	Valores
-crt	Establece sucesos críticos que envían alertas	all, none, custom:te|vo|po|di|fa|cp|me|in|re|ot Las configuraciones de alertas críticas personalizadas se especifican utilizando una lista de valores separados por una barra vertical de la forma **alertentries -crt custom:te|vo**, donde los valores personalizados son: • te: umbral superado de temperatura crítica • vo: umbral superado de voltaje crítico • po: error crítico de alimentación • di: error de la unidad de disco duro • fa: error del ventilador • cp: error del microprocesador • me: error de memoria • in: incompatibilidad de hardware • re: error de redundancia de alimentación • ot: todos los otros sucesos críticos
-crten	Envía alertas de sucesos críticos	habilitado, deshabilitado
-wrn	Establece sucesos de advertencia que envían alertas	all, none, custom:rp|te|vo|po|fa|cp|me|ot Las configuraciones de alertas de advertencia personalizadas se especifican utilizando una lista de valores separados por una barra vertical de la forma **alertentries -wrn custom:rp|te**, donde los valores personalizados son: • rp: advertencia de redundancia de alimentación • te: umbral superado de temperatura de advertencia • vo: umbral superado de voltaje de advertencia • po: umbral superado de alimentación de advertencia • fa: suceso no crítico del ventilador • cp: microprocesador en estado degradado • me: advertencia de memoria • ot: todos los otros sucesos de advertencia
-wrnen	Envía alertas de sucesos de advertencia	habilitado, deshabilitado

Tabla 60. Comando alertentries (continuación)

Opción	Descripción	Valores
-sys	Establece sucesos de rutina que envían alertas	all, none, custom:lo|tio|ot|po|bf|til|pf|el|ne Las configuraciones de alertas de rutina personalizadas se especifican utilizando una lista de valores separados por una barra vertical de la forma **alertentries -sys custom:lo|tio**, donde los valores personalizados son: • lo: inicio de sesión remoto correcto • tio: tiempo de espera del sistema operativo • ot: todos los otros sucesos de información y sistema • po: encendido/apagado del sistema • bf: error de arranque del sistema operativo • til: tiempo de espera del proceso de vigilancia del cargador del sistema operativo • pf: falla prevista (PFA) • el: registro de sucesos 75 % lleno • ne: cambio de red
-sysen	Envía alertas de sucesos de rutina	habilitado, deshabilitado

Sintaxis:

```
alertentries [options]
   options:
   -number recipient_number
      -status status
      -type alert_type
      -log include_log_state
      -n recipient_name
      -e email_address
      -ip ip_addr_or_hostname
      -pn port_number
      -del
      -test
      -crt event_type
      -crten state
      -wrn event_type
      -wrnen state
      -sys event_type
      -sysen state
```

Ejemplo:

```
system> alertentries
1. test
2. <not used>
3. <not used>
4. <not used>
5. <not used>
6. <not used>
7. <not used>
8. <not used>
9. <not used>
10. <not used>
11. <not used>
12. <not used>
```

```
system> alertentries -1
-status off
-log off
-n test
-e test@mytest.com
-crt all
-wrn all
-sys none
system>
```

Comando batch

Utilice este comando para ejecutar uno o varios comandos CLI en un archivo.

- Las líneas de comentario en el archivo de lote comienzan con #.
- Al ejecutar un archivo de lotes, los comandos que fallan se regresan junto con un código de retorno de falla.
- Los comandos de archivo de lote que contienen las opciones de comando desconocidas podrían generar avisos.

En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 61. Comando batch

La tabla siguiente es una tabla de tres columnas y varias filas que consta de las opciones, las descripciones de las opciones y los valores asociados para las opciones.

Opción	Descripción	Valores
-f	Nombre de archivo de lote	Nombre de archivo válido
-ip	Dirección IP del servidor TFTP/SFTP	Dirección IP válida
-pn	Número de puerto del servidor TFTP/SFTP	Número de puerto válido (predeterminado 69/22)
-u	Nombre de usuario para el servidor SFTP	Nombre de usuario válido
-pw	Contraseña para el servidor SFTP	Contraseña válida

Sintaxis:

```
batch [options]
option:
  -f filename
  -ip ip_address
  -pn port_number
 username
  -pw password
```

Ejemplo:

```
system> batch -f sslcfg.cli -ip 192.168.70.200
1 : sslcfg client dnld ip 192.168.70.20
Command total/errors/warnings: 8 / 1 / 0
system>
```

Comando clearcfg

Utilice este comando para establecer la configuración de IMM a sus valores predeterminados de fábrica.

Para emitir este comando al menos debe contar permiso para realizar una configuración avanzada del adaptador. Una vez borrada la configuración del IMM,IMM este se reinicia.

Comando clock

Use este comando para mostrar la fecha y hora actual. Puede establecer el ajuste de UTC y los valores de horario de verano

El BMC obtiene la hora del servidor host o del servidor NTP.

La hora del host puede ser hora local u hora UTC. La opción del host debe establecerse en UTC si el NTP no se utiliza y al formato de UTC de las aplicaciones de host. El ajuste de UTC puede estar en formato de +0200, +2:00, +2, or 2 para los ajustes positivos y -0500, -5:00 o -5 para los ajustes negativos. El desplazamiento del UTC y las horas del horario de verano se utilizan con el NTP o cuando el modo de host es UTC.

Para un ajuste de UTC de +2, -7, -6, -5, -4 y -3, se necesitan configuraciones especiales de horario de verano.

- Para +2, las opciones de horario de verano son los siguientes: off, ee (Europa Oriental), tky (Turquía), bei (Beirut), amm (Amman), jem (Jerusalén).
- Para -7, los valores de horario de verano son los siguientes: off, mtn (montaña), maz (Mazatlan).
- Para -6, los valores de horario de verano son los siguientes: off, mex (México), cna (Norteamérica central).
- Para -5, los valores de horario de verano son los siguientes: off, cub (Cuba), ena (Norteamérica oriental).
- Para -4, los valores de horario de verano son los siguientes: off, asu (Asunción), cui (Cuiaba), san (Santiago), cat (Canadá, Atlántico).
- Para -3, los valores de horario de verano son los siguientes: off, gtb (Godthab), bre (Brasil, este).

Sintaxis:
```
clock [options]
options:
-u UTC offset
-dst on/off/special case
-host - local | utc , format of time obtained from host (default: utc)
Windows systems use local, Linux uses utc
```

Ejemplo:
```
system> clock
12/12/2011 13:15:23 GMT-5:00 dst on
```

Comando identify

Utilice este comando para encender y apagar el LED de identifican del chasis, o para que parpadee.

La opción **-d** se puede usar con la opción **-s on** para encender el LED solo durante el número de segundos especificados con la opción **-d**. El LED se apaga después de transcurrido el número de segundos.

Sintaxis:
```
identify [options]
options:
-s on/off/blink
-d seconds
```

Ejemplo:
```
system> identify
-s off
```

```
system> identify -s on -d 30
ok
system>
```

Comando info

Use este comando para mostrar y configurar información sobre el IMM.

Ejecutar el comando **info** sin opciones muestra toda la información de ubicación y contacto de IMM. En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 62. Comando info

La tabla siguiente es una tabla de tres columnas y varias filas que consta de las opciones, las descripciones de las opciones y los valores asociados para las opciones.

Opción	Descripción	Valores
-name	Nombre de IMM	Cadena
-contact	Nombre de la persona de contacto del IMM	Cadena
-location	Ubicación de IMM	Cadena
-room[1]	Identificador de sala del IMM	Cadena
-rack[1]	Identificador de bastidor del IMM	Cadena
-rup[1]	Posición del IMM en el bastidor	Cadena
-ruh	Altura de la unidad de bastidor	Solo lectura
-bbay	Ubicación de la bahía blade	Solo lectura

1. El valor es de solo lectura y no se puede reiniciar si el IMM reside en un Flex System.

Sintaxis:

```
info [options]
option:
  -name xcc_name
  -contact contact_name
  -location xcc_location
  -room room_id
  -rack rack_id
  -rup rack_unit_position
  -ruh rack_unit_height
  -bbay blade_bay
```

Comando spreset

Use este comando para reiniciar el IMM.

Para emitir este comando al menos debe contar permiso para realizar una configuración avanzada del adaptador.

Comandos sin agente

Este tema proporciona una lista alfabética de los comandos sin agente.

Actualmente, hay 3 comandos sin agente:

Comando storage

Utilice este comando para visualizar y para configurar (si es compatible con la plataforma) información sobre los dispositivos de almacenamiento del servidor que gestiona el IMM.

En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 63. Comando storage

La tabla siguiente es una tabla de tres columnas y varias filas que consta de las opciones, las descripciones de las opciones y los valores asociados para las opciones.

Opción	Descripción	Valores
-list	Enumera los destinos de almacenamiento gestionados por el IMM.	**controllers|pools|volumes|drives** Donde **target** es: • **controllers**: enumera los controladores RAID admitidos[1] • **pools**: enumera los grupos de almacenamiento asociados al controlador RAID[1] • **volumes**: enumera los volúmenes de almacenamiento asociados al controlador RAID[1] • **drives**: enumera las unidades de almacenamiento asociadas al controlador RAID[1]
-list -target **target_id**	Enumera los **targets** de almacenamiento gestionados por el IMM de acuerdo con el **target_id**.	**pools|volumes|drives ctrl[x]|pool[x]** Donde **target** y **target_id** son: • **pools ctrl[x]**: enumera los grupos de almacenamiento asociados con el controlador RAID, según el target_id[1] • **volumes ctrl[x]|pool[x]**: enumera los volúmenes de almacenamiento asociados con el controlador RAID, según el target_id[1] • **drives ctrl[x]|pool[x]**: enumera las unidades de almacenamiento asociadas con el controlador RAID, según el target_id[1]
-list flashdimms	Enumera los DIMM flash gestionados por el IMM.	
-list devices	Muestra el estado de todos los discos y DIMM flash gestionados por el IMM.	
-show **target_id**	Muestra información para el destino seleccionado gestionado por el IMM.	Donde **target_id** es: **ctrl[x]|vol[x]|disk[x]|pool[x]** **|flashdimm[x]** 3
-show **target_id** info	Muestra información detallada para el destino seleccionado gestionado por el IMM.	Donde **target_id** es: **ctrl[x]|vol[x]|disk[x]|pool[x]** **|flashdimm[x]** 3
-show **target_id firmware**[3]	Muestra información de firmware para el destino seleccionado gestionado por el IMM.	Donde **target_id** es: **ctrl[x]|disk[x]|flashdimm[x]**[2]

Tabla 63. Comando storage (continuación)

Opción	Descripción	Valores
-showlog **target_id<m:n|all>**[3]	Muestra los registros de sucesos del destino seleccionado gestionado por el IMM.	Donde **target_id** es: **ctrl[x]**[4] **m:n**|**all** Donde **m:n** es el número máximo de registros de sucesos Donde **all** corresponde a todos los registros de sucesos
-config ctrl -scanforgn -target **target_id**[3]	Detecta la configuración RAID externa.	Donde **target_id** es: **ctrl[x]**[5]
-config ctrl -imptforgn -target **target_id**[3]	Importa la configuración RAID externa.	Donde **target_id** es: **ctrl[x]**[5]
-config ctrl -clrforgn -target **target_id**[3]	Borra la configuración RAID externa.	Donde **target_id** es: **ctrl[x]**[5]
-config ctrl -clrcfg -target **target_id**[3]	Borrar la configuración RAID.	Donde **target_id** es: **ctrl[x]**[5]
-config drv -mkoffline -target **target_id**[3]	Cambia el estado de la unidad de en línea a fuera de línea.	Donde **target_id** es: **disk[x]**[5]
-config drv -mkonline -target **target_id**[3]	Cambia el estado de la unidad de fuera de línea a en línea.	Donde **target_id** es: **disk[x]**[5]
-config drv -mkmissing -target **target_id**[3]	Marca la unidad fuera de línea como una unidad en buen estado sin configurar.	Donde **target_id** es: **disk[x]**[5]
-config drv -prprm -target **target_id**[3]	Prepara una unidad en buen estado sin configurar para la extracción.	Donde **target_id** es: **disk[x]**[5]
-config drv -undoprprm -target **target_id**[3]	Cancela la preparación de una unidad en buen estado sin configurar para la operación de extracción.	Donde **target_id** es: **disk[x]**[5]
-config drv -mkbad -target **target_id**[3]	Cambia la unidad en buen estado sin configurar a una unidad en mal estado sin configurar.	Donde **target_id** es: **disk[x]**[5]
-config drv -mkgood -target **target_id**[3]	Cambia una unidad en mal estado sin configurar a una unidad en buen estado sin configurar. o bien Convierte únicamente la unidad de solo un paquete de discos (JBOD) a una unidad en buen estado sin configurar.	Donde **target_id** es: **disk[x]**[5]
-config drv -addhsp -**[dedicated pools]** -target **target_id**[3]	Asigna la unidad seleccionada como repuesto dinámico a un controlador o grupos de almacenamiento existentes.	Donde **target_id** es: **disk[x]**[5]
-config drv -rmhsp -target **target_id**[3]	Quita el repuesto dinámico.	Donde **target_id** es: **disk[x]**[5]

Tabla 63. Comando storage (continuación)

Opción	Descripción	Valores
-config vol -remove -target **target_id**[3]	Quita un volumen.	Donde **target_id** es: **vol[x]**[5]
-config vol -set [-N] [-w] [-r] [-i] [-a] [-d] [-b] -target **target_id**[3]	Modifica las propiedades de un volumen.	• [-N **volume_name**] es el nombre del volumen • [-w **<0|1|2>**] es la política de escritura de memoria caché: – Escriba **0** para la política Escritura directa – Escriba **1** para la política Escritura no simultánea – Escriba **2** para la política Escritura no simultánea con unidad de batería de reserva (BBU) • [-r **<0|1|2>**] es la política de lectura de la memoria caché: – Escriba **0** para la política Sin lectura anticipada – Escriba **1** para la política Lectura anticipada – Escriba **2** para la política Lectura anticipada adaptable • [-i **<0|1>**] es la política de E/S de la memoria caché: – Escriba **0** para la política E/S directa – Escriba **1** para la política E/S en memoria caché • [-a **<0|2|3>**] es la política de acceso: – Escriba **0** para la política Lectura de escritura – Escriba **2** para la política Solo lectura – Escriba **3** para la política Bloqueada • [-d **<0|1|2>**] es la política de memoria caché del disco: – Escriba **0** si la política no tiene cambios – Escriba **1** para habilitar la política[6] – Escriba **2** para deshabilitar la política • [-b **<0|1>**] es la inicialización en segundo plano: – Escriba **0** para habilitar la inicialización – Escriba **1** para deshabilitar la inicialización • **-target_id** es **vol[x]**[5]

Tabla 63. Comando storage (continuación)

Opción	Descripción	Valores
-config vol -add<[-R] [-D disk] [-H disk] [-1 hole]> [-N] [-w] [-r][3],[7]	Crea un volumen para un nuevo grupo de almacenamiento, cuando el destino es un controlador. o bien Crea un volumen con un grupo de almacenamiento existente, cuando el destino es un grupo de almacenamiento.	• [-R **<0|1|5|1E|6|10|50|60|00|1ERLQ0|1E0RLQ0>**] Esta opción define el nivel de RAID y solo se usa con un grupo de almacenamiento nuevo • [-D disk **[id11]:disk[id12]:..disk[id21]:disk [id22]:..**] Esta opción define el grupo de unidades (incluyendo los lapsos) y se utiliza únicamente con un nuevo grupo de almacenamiento • [-H disk **[id1]:disk[id2]:..**]Esta opción define el grupo de repuestos dinámicos y se utiliza únicamente con un nuevo grupo de almacenamiento • [-1 hole] Esta opción define el número de índice del espacio libre para un grupo de almacenamiento existente • [-N **volume_name**] es el nombre del volumen • [-w **<0|1|2>**] es la política de escritura de memoria caché: – Escriba **0** para la política Escritura directa – Escriba **1** para la política Escritura no simultánea – Escriba **2** para la política Escritura no simultánea con unidad de batería de reserva (BBU) • [-r **<0|1|2>**] es la política de lectura de la memoria caché: – Escriba **0** para la política Sin lectura anticipada – Escriba **1** para la política Lectura anticipada – Escriba **2** para la política Lectura anticipada adaptable
-config vol -add[-i] [-a] [-d] [-f] [-S] [-P] -target **target_id**[3]	Crea un volumen para un nuevo grupo de almacenamiento, cuando el destino es un controlador. o bien Crea un volumen con un grupo de almacenamiento existente, cuando el destino es un grupo de almacenamiento.	• [-i **<0|1>**] es la política de E/S de la memoria caché: – Escriba **0** para la política E/S directa – Escriba **1** para la política E/S en memoria caché • [-a **<0|2|3>**] es la política de acceso: – Escriba **0** para la política Lectura de escritura – Escriba **2** para la política Solo lectura – Escriba **3** para la política Bloqueada • [-d **<0|1|2>**] es la política de memoria caché del disco: – Escriba **0** si la política se mantiene igual – Escriba **1** para habilitar la política[6] – Escriba **2** para deshabilitar la política • [-f **<0/1/2>**] es el tipo de inicialización:

Tabla 63. Comando storage (continuación)

Opción	Descripción	Valores
		– Escriba **0** para ninguna inicialización – Escriba **1** para inicialización rápida – Escriba **2** para inicialización completa • [-S **volume_size**] es el tamaño del nuevo volumen en MB • [-P **strip_size**] es el tamaño de banda del volumen, por ejemplo 128K o 1M • -target **target_id** es: – **ctrl[x]** (nuevo grupo de almacenamiento)[5] – **pool[x]** (grupo de almacenamiento existente)[5]
-config vol -getfreecap [-R] [-D disk] [-H disk] -target **target_id**[3]	Obtiene la capacidad libre del grupo de unidades.	• [-R **<0|1|5|1E|6|10|50|60|00|1ERLQ0|1E0RLQ0>**] Esta opción define el nivel de RAID y solo se usa con un grupo de almacenamiento nuevo • [-D disk **[id11]:[id12]:..[id21]:[id22]:..**] Esta opción define el grupo de unidades (incluyendo los lapsos) y se utiliza únicamente con un nuevo grupo de almacenamiento • [-H disk **[id1]:[id2]:..**]Esta opción define el grupo de repuestos dinámicos y se utiliza únicamente con un nuevo grupo de almacenamiento • -target **target_id** es: – **ctrl[x]**[5]
-help	Visualizar uso y opciones del comando	

Notas:
1. Este comando solo se admite en servidores donde el IMM puede acceder al controlador RAID.
2. La información de firmware se muestra únicamente para controladores, discos y DIMM de memoria flash asociados. No se muestra la información de firmware para los grupos y volúmenes asociados.
3. La información se muestra en varias líneas, debido a las limitaciones de espacio.
4. Este comando solo se admite en servidores compatibles con los registros RAID.
5. Este comando solo se admite en servidores compatibles con las configuraciones RAID.
6. El valor **Enable** no admite configuraciones RAID de nivel 1.
7. Aquí se muestra una lista parcial de las opciones disponibles. El resto de las opciones para el comando **storage -config vol -add** aparecen en la fila siguiente.

Sintaxis:

```
storage [options]
option:
  -config ctrl|drv|vol -option [-options] -target target_id
  -list controllers|pools|volumes|drives
  -list pools -target ctrl[x]
  -list volumes -target ctrl[x]|pool[x]
  -list drives -target ctrl[x]|pool[x]
  -list devices
  -list flashdimms
  -show target_id
  -show {ctrl[x]|pool[x]|disk[x]|vol[x]|flashdimm[x]} info
  -show {ctrl[x]|disk[x]|flashdimm[x]}firmware
  -showlog ctrl[x]m:n|all
  -h help
```

Ejemplos:

```
system> storage
-config ctrl -clrcfg -target ctrl[0]
ok
system>
system> storage
-config ctrl -clrforgn -target ctrl[0]
ok
system>
system> storage
-config ctrl -imptforgn -target ctrl[0]
ok
system>
system> storage
-config ctrl -scanforgn -target ctrl[0]
Detect 1 foreign configuration(s) on controller ctrl[0]
system>
system> storage
-config drv -addhsp -dedicated pool[0-1] -target disk[0-0]
ok
system>
system> storage
-config drv -addhsp -target disk[0-0]
ok
system>
system> storage
-config drv -mkbad -target disk[0-0]
ok
system>
system> storage
-config drv -mkgood -target disk[0-0]
ok
system>
system> storage
-config drv -mkmissing -target disk[0-0]
ok
system>
system> storage
-config drv -mkoffline -target disk[0-0]
ok
system>
system> storage
-config drv -mkonline -target disk[0-0]
ok
system>
system> storage
-config drv -prprm -target disk[0-0]
ok
system>
system> storage
-config drv -rmhsp -target disk[0-0]
ok
system>
system> storage
-config drv -undoprprm -target disk[0-0]
ok
system>
system> storage
-config vol -add -1 1 -target pool[0-1]
ok
system>
```

```
system> storage
-config vol -add -R 1 -D disk[0-0]:disk[0-1] -w 1 -r 2 -i 0 -a 0 -d 0 -f 0
-N LD_volume -S 100000 -P 64K -H disk[0-2] -target ctrl[0]
ok
system>
system> storage
-config vol -getfreecap -R 1 -D disk[0-0]:disk[0-1] -H disk[0-2] -target ctrl[0]
The drive group configuration is good with free capacity 500000MB
system>
system> storage
-config vol -remove -target vol[0-1]
ok
system>
system> storage
-config vol -set -N LD_volume -w 0 -target vol[0-0]
ok
system>
system> storage
-list controllers
ctrl[0]    ServerRAID M5110e(Slot No. 0)
ctrl[1]    ServerRAID M5110f(Slot No. 1)
system>
system> storage
-list drives
disk[0-0]    Drive 0
disk[0-1]    Drive 1
disk[0-2]    Drive 2
system>
system> storage
-list flashdimms
flashdimm[1]    Flash DIMM 1
flashdimm[4]    Flash DIMM 4
flashdimm[9]    Flash DIMM 9
system>
system> storage
-list pools
pool[0-0]    Storage Pool 0
pool[0-1]    Storage Pool 1
system>
system> storage
-list volumes
system>storage -list volumes
vol[0-0]    Volume 0
vol[0-1]    Volume 1
Vol[0-2]    Volume 2
system>
system> storage
-list drives -target ctrl[0]
disk[0-0]    Drive 0
disk[0-1]    Drive 1
disk[0-2]    Drive 2
system>
system> storage
-list drives -target pool[0-0]
disk[0-0]    Drive 0
disk[0-1]    Drive 1
system>
system> storage
-list pools -target ctrl[0]
pool[0-0]    Storage Pool 0
system>
```

```
system> storage
-list volumes -target ctrl[0]
vol[0-0]    Volume 0
vol[0-1]    Volume 1
system>
system> storage
-list volumes -target pool[0-0]
vol[0-0]    Volume 0
vol[0-1]    Volume 1
system>
system> storage
-show ctrl[0] firmware
Total Firmware number: 2
Name: RAID Firmware1
Description: RAID Firmware
Manfacture: IBM
Version: 4.01(3)T
Release Date: 01/05/2013
Name: RAID Firmware2
Description: RAID Firmware
system>
system> storage
-show ctrl[0] info
Product Name: ServerRAID M5110e
Firmware Package Version: 23.7.0.1.2
Battery Backup: Installed
Manufacture: IBM
UUID: 1234567890123456
Model Type / Model: 1234AHH
Serial No.: 12345678901
FRU No.: 5005076049CC4
Part No.: LSI2004
Cache Model Status: Unknown
Cache Model Memory Size: 300MB
Cache Model Serial No.: PBKUD0XTA0P04Y
PCI Slot Number: 0
PCI Bus Number: 2
PCI Device Number: 2
PCI Function Number: 10
PCI Device ID: 0x1000
PCI Subsystem Device ID: 0x1413
Ports: 2
Port 1: 12345678901234
Port 2: 12345678901235
Storage Pools: 2
pool[0-0]    Pool 0
pool[0-1]    Pool 1
Drives: 3
disk[0-0]    Drive 0
disk[0-1]    Drive 1
disk[0-2]    Drive 2
system>
system> storage
-show disk[0-0] firmware
Total Firmware number: 1
Name: Drive
Description:
Manufacture:
Version: BE24
Release Date:
system>
```

```
system> storage
-show disk[0-0] info
Product Name: ST98394893
State: Online
Slot No.: 0
Disk Type: SATA
Media Type: HHD
Health Status: Normal
Capacity: 100.000GB
Speed: 6.0Gb/s
Current Temperature: 33C
Manufacture: ATA
Device ID: 5
Enclusure ID: 0x00FC
Machine Type:
Model:
Serial No.: 9XKJKL
FRU No.:
Part No.:
system>
system> storage
-show flashdimm[15]
Name: CPU1 DIMM 15
Health Status: Normal
Operational Status: Online
Capacity(GB): 400GB
Model Type: DDR3
Part Number: 93E40400GGM101PAT
FRU S/N: 44000000
Manuf ID: Diablo Technologies
Temperature: 0C
Warranty Writes: 100%
Write Endurance: 100%
F/W Level: A201.0.0.49152
system>
system> storage
-show pool[0-0]
RAID State: RAID 0
RAID Capacity: 67.000GB (0.000GB free)
Drives: 2
disk[0-0]    Drive 0
disk[0-1]    Drive 1
Volumes: 2
vol[0-0]    Volume 0
vol[0-1]    Volume 1
system>
system> storage
-show pool[0-1] info
RAID State: RAID 1
RAID Capacity: 231.898GB (200.000GB free)
Holes: 2
#1 Free Capacity: 100.000GB
#2 Free Capacity: 100.000GB

Drives: 2
disk[0-1]    Drive 1
disk[0-2]    Drive 2

Volume: 1
vol[0-1]    LD_volume
system>
```

```
system> storage
-show vol[0-0]
Name: Volume 0
Stripe Size: 64KB
Status: Offline
Capacity: 100.000GB
system>
system> storage
-show vol[0-0] info
Name: LD_volume
Status: Optimal
Stripe Size: 64KB
Bootable: Not Bootable
Capacity: 231.898GB
Read Policy: No Read Ahead
Write Policy: Write Through
I/O Policy: Direct I/O
Access Policy: Read Write
Disk Cache Policy: Unchanged
Background Initialization: Enable
system>
```

Comando adapter

Se utiliza este comando para visualizar la información de inventario del adaptador PCIe.

Si no se admite el comando **adapter**, el servidor responde con el mensaje siguiente cuando se emite el comando:
`Your platform does not support this command.`
Si elimina, sustituye o configura adaptadores, debe reiniciar el servidor (al menos una vez) para ver la información actualizada del adaptador.

En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 64. Comando adapter

La tabla siguiente es una tabla de tres columnas y varias filas que consta de las opciones, las descripciones de las opciones y los valores asociados para las opciones.

Opción	Descripción	Valores
-list	Lista todos los adaptadores PCIe en el servidor	
-show **target_id**	Muestra información detallada del adaptador PCIe de destino	**target_id [info|firmware|ports|chips]** Donde: • **info**: muestra información de hardware para el adaptador • **firmware**: muestra toda la información de firmware para el adaptador • **ports**: muestra toda la información de puerto Ethernet para el adaptador • **chips**: muestra toda la información de chip GPU para el adaptador
-h	Visualizar uso y opciones del comando	

Sintaxis:

```
adapter [options]
option:
  -list
  -show target_id [info|firmware|ports|chips]
  -h help
```

Ejemplos:

```
system> adapter
list
ob-1     Flex System CN4054 10Gbps Virtual Fabric Adapter
ob-2     GPU Card 1
slot-1   Raid Controller 1
slot-2   Adapter 01:02:03
system> adapter
show ob-1 info
Product Name: Flex System CN4054 10Gbps Virtual Fabric Adapter
Card Interface: PCIe x 16
Function Count: 2

Function Name: xxx Emulx xx component1
Segment Number: 2348
Bus Number: 23949
Device Number: 1334
Function Number: 21
Vendor Id: 12
Device Id: 33
Revision Id: 1
Class Code: 2
Sub Vendor: 334
Sub Device: 223
Slot Description: a slot
Slot Type: 23
Slot Data Bus Width: 0
Hot Plug: 12
PCI Type: 11
Blade Slot Port: xxx
UUID: 39302938485
Manufacturer: IBM
Serial Number: 998AAGG
Part Number: ADB233
Model: 345
Function Sku: 221
Fod Uid: 2355
Required Daughter: 0
Max Data Width: 0
Connector Layout: pci x

Package Type: dici
Function Name: xxx nVidia xx component2
Segment Number: 2348
Bus Number: 23949
Device Number: 1334
Function Number: 21
Vendor Id: 12
Device Id: 33
Revision Id: 1
Class Code: 2
Sub Vendor: 334
Sub Device: 223
Slot Description: a slot
Slot Type: 23
```

```
Slot Data Bus Width: 0
Hot Plug: 12
PCI Type: 11
Blade Slot Port: xxx
UUID: 39302938485
Manufacturer: IBM
Serial Number: 998AAGG
Part Number: ADB233
Model: 345
Function Sku: 221
Fod Uid: 2355
Required Daughter: 0
Max Data Width: 0
Connector Layout: pci x
Package Type: dici
```

Comando m2raid

Utilice este comando para obtener la información del inventario relacionada con M.2 y gestionar los volúmenes virtuales.

En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 65. Comando m2raid

La tabla siguiente es una tabla de dos columnas y varias filas que consta de las opciones y las descripciones asociadas.

Opción	Descripción
-h/?	Imprimir la información de ayuda para este comando
-version	Mostrar la información de firmware del controlador
-disks	Mostrar la información de los discos de medios
-volumes	Mostrar la información de los volúmenes virtuales
-create	Crear un volumen virtual, se pueden especificar VD_Name, RaidLevel y StripeSize
-delete	Eliminar un volumen virtual
-import	Importar un volumen virtual externo. Después de importar el volumen virtual, el reinicio del sistema volverá a generar automáticamente el volumen virtual.

Utilización

```
m2raid [-options] - raid configuration for M.2 adapter with Mirroring Enablem
options:
   -version                    - displays controller firmware version.
   -disks                      - displays information of media disks.
   -volumes                    - displays information of virtual volumes
   -create -VD_Name <nameStr> -RaidLevel <0|1> -StripeSize <32|64>  - create virt
   -delete -VD_ID <0|1>       - delete the virtual volume
   -import -VD_ID <0|1>       - import a foreign virtual volume
```

Ejemplo

```
system> m2raid -version
    ThinkSystem M.2 with Mirroring Enablement Kit
 Firmware Version = 2.3.10.1193

system> m2raid -disks
```

```
    M.2 Bay0          32GB M.2 SATA SSD     LEN      100%
M.2 Bay1          32GB M.2 SATA SSD     LEN      100%

system> m2raid -volumes
    VD_ID    VD_Name    RaidLevel    StripSize    VD Capacity    Status
     0       M2RAID       1             64k          29 GB           Optimal

system> m2raid -delete -VD_ID 0
VD_ID 0 is deleted

system> m2raid -create -VD_Name M2RAID -RaidLevel 1 -StripeSize 64
New volume is created

system> m2raid -import -VD_ID 0
VD_ID 0 is imported
```

Comandos de soporte

Este tema proporciona una lista alfabética de los comandos de soporte.

Existe solo un comando de soporte: “Comando dbgshimm” en la página 183.

Comando dbgshimm

Utilice este comando para desbloquear el acceso de red a la depuración segura de carcasa.

Nota: Este comando está diseñado solo para el uso del personal de soporte.

En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 66. Comando dbgshimm

La tabla siguiente es una tabla de dos columnas y varias filas que consta de las opciones y las descripciones asociadas.

Opción	Descripción
estado	Mostrar estado
habilitar	Habilitar el acceso a la depuración (predeterminado si no se especifica ninguna opción)
deshabilitar	Deshabilitar el acceso a la depuración

Capítulo 11. Interfaz IPMI

Este capítulo describe la interfaz IPMI compatible con XClarity Controller.

Para conocer los detalles de los comandos IPMI estándar, consulte el documento de especificación de la interfaz inteligente de gestión de plataforma (IPMI) (versión 2.0 o posterior). Este documento proporciona descripciones de los parámetros OEM que se utilizan con los comandos IPMI y OEM IPMI estándar admitidos por el firmware de XClarity Controller.

Gestión del XClarity Controller con la IPMI

Utilice la información en este tema para gestionar el XClarity Controller utilizando la Intelligent Platform Management Interface (IPMI).

El XClarity Controller viene con un Id. de usuario establecido inicialmente con un nombre de usuario de USERID y una contraseña de PASSW0RD (con un cero, no con la letra O). Este usuario tiene acceso de supervisor.

Importante: Con el fin de obtener una seguridad ampliada, cambie este nombre de usuario y esta contraseña durante la configuración inicial.

En Flex System, un usuario puede configurar un CMM de Flex System para gestionar de forma central las cuentas de usuario de la IPMI de XClarity Controller. En esta circunstancia es posible que no pueda acceder al XClarity Controller usando la IPMI hasta que el CMM haya configurado las Id. de usuario de la IPMI.

Nota: Las credenciales de Id. de usuario que se hayan configurado en el CMM pueden ser diferentes que la combinación de USERID/PASSW0RD descrita arriba. Si no se han configurad los Id. de usuario de la IPMI por el CMM, el puerto de red asociado al protocolo IPMI estará cerrado.

XClarity Controller también proporciona las siguientes funciones de gestión de servidor remoto IPMI:

Interfaces de la línea de comandos IPMI
La interfaz de la línea de comandos IPMI proporciona acceso directo a las funciones de gestión de servidor mediante el protocolo IPMI 2.0. Puede utilizar IPMItool para emitir comandos a fin de controlar la alimentación del servidor, mostrar la información del servidor e identificar el servidor. Para obtener más información acerca de IPMItool, consulte “Uso de IPMItool” en la página 185.

Serie sobre IP
Para gestionar servidores desde una ubicación remota, use IPMItool para establecer una conexión Serial Over LAN (SOL). Para obtener más información acerca de IPMItool, consulte “Uso de IPMItool” en la página 185.

Uso de IPMItool

Utilice la información de este tema para acceder a la información sobre IPMItool.

IPMItool proporciona varias herramientas que puede utilizar para gestionar y configurar un sistema IPMI. Puede utilizar IPMItool en banda o fuera de banda para gestionar y para configurar XClarity Controller.

Para obtener más información sobre IPMItool, o para descargar IPMItool, vaya a https://github.com/ipmitool/ipmitool.

Comandos IPMI con parámetros OEM

Obtener/definir parámetros de configuración de LAN

Para reflejar las capacidades proporcionadas por el XCC para algunos de los valores de red, los valores para algunos de los datos del parámetro se definen como se indica a continuación.

DHCP

Además de los métodos usuales para obtener una dirección IP, el XCC proporciona un modo en el que intenta obtener una dirección IP de un servidor DHCP por un período de tiempo determinado y, si no lo consigue, conmuta por error al uso de una dirección IP estática.

La tabla siguiente es una tabla de tres columnas y varias filas que consta de las opciones, las descripciones de las opciones y los valores asociados para las opciones.

Parámetro	#	Datos de parámetro
Fuente de dirección IP	4	datos 1 [7:4] – reservado [3:0] – fuente de dirección 0h = no especificado 1h = dirección estática (configurada manualmente) 2h = dirección obtenida por XCC ejecutando DHCP 3h = dirección obtenida por el BIOS o el software del sistema 4h = dirección obtenida por XCC ejecutando otro protocolo de asignación de direcciones. El XCC utiliza el valor 4h para indicar el modo de dirección de DHCP con conmutación por error a estático.

Selección de la interfaz de Ethernet

El hardware XCC contiene Ethernet Mac doble de 10/100 con interfaces RMII. El hardware XCC también contiene Ethernet Mac dual de 1 Gbps con interfaces RGMII. Uno de los MAC suele estar conectado a la NIC del servidor compartido y el otro MAC se utiliza como puerto de gestión del sistema dedicado. Solo hay un puerto Ethernet activo en un servidor en un momento determinado. No se habilitarán ambos puertos simultáneamente.

En algunos servidores, es posible que los diseñadores del sistema opten por conectar solo una de las interfaces de Ethernet en el sistema planar. En estos sistemas, solo la interfaz Ethernet que está conectada en el planar es compatible con el XCC. Una solicitud para utilizar el puerto no conectado devuelve un código de finalización de CCh.

Los ID. de paquete de todas las tarjetas de red opcionales se enumeran de la siguiente manera:

- tarjeta opcional n.° 1, ID. de paquete = 03h (eth2),
- tarjeta opcional n.° 2, ID. de paquete = 04h (eth3),

La tabla siguiente es una tabla de tres columnas y varias filas que consta de las opciones, las descripciones de las opciones y los valores asociados para las opciones.

Parámetro	#	Datos de parámetro
Parámetro OEM El XCC utiliza este número de parámetro para indicar cuál de los puertos Ethernet posibles (paquetes lógicos) se debe utilizar. Este parámetro del comando Get/ Set LAN Configuration Parameters no utiliza un Selector de conjuntos ni requiere un Selector de bloques, por lo que estos campos deben configurarse en 00h. Los datos de la respuesta arrojarán 3 bytes u, opcionalmente, 4 bytes si el dispositivo está en un paquete de NCSI. Byte 1 = código de finalización Byte 2 = revisión Byte 3 = 00h para eth0, o 01h para eth1, etc... Byte 4 = (opcional) número de canal, si el dispositivo es un paquete de NCSI	C0h	data1 00h = eth0 01h = eth1 02h = eth2 etc... FFh = deshabilitar todos los puertos de red externos) XCC admite un segundo byte de datos opcional para especificar qué canal de un paquete se utilizará data2 00h = canal 0 01h = canal 1 etc... Si no se especifica data2 en la solicitud, se asumirá el canal 0.

El byte de data1 se utiliza para especificar el paquete lógico. Puede ser una NIC de gestión de sistemas dedicada o una interfaz de NCSI en la NIC compartida con el servidor.

El byte de data2 se usa para especificar el canal para el paquete lógico, si el paquete es un dispositivo NCSI. Si no se especifica data2 en la solicitud y el paquete lógico es un dispositivo de NCSI, se supone el canal 0. Si se especifica data2 en la solicitud pero el paquete lógico no es un dispositivo de NCSI, se ignora la información del canal.

Ejemplos:

Apéndice A. Si el canal 2 de la NIC compartida en el planar (ID. del paquete = 0, eth0) se va a utilizar como puerto de gestión, los datos de entrada serían: 0xC0 0x00 0x02

Apéndice B: si se va a utilizar el primer canal de la primera tarjeta secundaria de red, la entrada sería: 0xC0 0x02 0x0

Habilitación/deshabilitación de Ethernet sobre USB

El siguiente parámetro se utiliza para habilitar o deshabilitar la interfaz en banda del XCC.

La tabla siguiente es una tabla de tres columnas y varias filas que consta de las opciones, las descripciones de las opciones y los valores asociados para las opciones.

Parámetro	#	Datos de parámetro
Parámetro OEM (El valor de este parámetro es utilizado por XCC para habilitar o deshabilitar la interfaz Ethernet sobre USB.) Este parámetro del comando Get LAN Configuration Parameters no utiliza un Selector de conjuntos ni requiere un Selector de bloques, por lo que estos campos deben configurarse en 00h. Los datos de la respuesta devuelven 3 bytes: Byte 1 = código de finalización Byte 2 = revisión Byte 3 = 00h (deshabilitado) o 01h (habilitado)	C1h	datos 1 0x00 = deshabilitado 0x01 = habilitado

El byte de data1 se utiliza para especificar el paquete lógico. Puede ser una NIC de gestión de sistemas dedicada o una interfaz de NCSI en la NIC compartida con el servidor.

El byte de data2 se usa para especificar el canal para el paquete lógico, si el paquete es un dispositivo NCSI. Si no se especifica data2 en la solicitud y el paquete lógico es un dispositivo de NCSI, se supone el canal 0. Si se especifica data2 en la solicitud pero el paquete lógico no es un dispositivo de NCSI, se ignora la información del canal.

Ejemplos:

Apéndice A. Si el canal 2 de la NIC compartida en el planar (ID. del paquete = 0, eth0) se va a utilizar como puerto de gestión, los datos de entrada serían: 0xC0 0x00 0x02

Apéndice B: si se va a utilizar el primer canal de la primera tarjeta secundaria de red, la entrada sería: 0xC0 0x02 0x0

Opción IPMI para obtener el DUID-LLT

Un valor adicional de solo lectura que debe exponerse a través de IPMI es el DUID. De acuerdo con RFC3315, este formato de DUID se basa en la dirección de la capa de enlace más la hora.

Parámetro	#	Datos de parámetro
Parámetro OEM (El valor de este parámetro es utilizado por XCC para habilitar o deshabilitar la interfaz Ethernet sobre USB.) Este parámetro del comando Get LAN Configuration Parameters no utiliza un Selector de conjuntos ni requiere un Selector de bloques, por lo que estos campos deben configurarse en 00h. Los datos de la respuesta devuelven 3 bytes: Byte 1 = código de finalización Byte 2 = revisión de parámetros (como en la especificación IPMI) Byte 3 = longitud de los siguientes bytes de datos (actualmente, 16 bytes) Byte 4-n DUID_LLT	C2h	

Parámetros de configuración de Ethernet

Los parámetros que se incluyen a continuación se pueden utilizar para configurar valores Ethernet específicos.

Parámetro	#	Datos de parámetro
Parámetro OEM (El valor de este parámetro es utilizado por XCC para habilitar o deshabilitar la configuración de negociación automática para la interfaz de Ethernet.) Los datos de la respuesta devuelven 3 bytes: Byte 1 = código de finalización Byte 2 = revisión Byte 3 = 00h (deshabilitado) o 01h (habilitado)	C3h	datos 1 0x00 = deshabilitado 0x01 = habilitado Nota: en los sistemas Flex y ThinkSystem D2 Enclosure (ThinkSystem SD530 Compute Node), la configuración de la negociación automática no se puede cambiar porque podría romper la ruta de comunicación de red a través de CMM y SMM.
Parámetro OEM (El valor de este parámetro es utilizado por XCC para obtener o establecer la velocidad de datos de la interfaz Ethernet.) Los datos de la respuesta devuelven 3 bytes: Byte 1 = código de finalización Byte 2 = revisión Byte 3 = 00h (10 Mb) o 01h (100 Mb)	C4h	datos 1 0x00 = 10 Mbit 0x01 = 100 Mbit
Parámetro OEM (El valor de este parámetro es utilizado por XCC para obtener o establecer la configuración dúplex de datos de la interfaz Ethernet.) Los datos de la respuesta devuelven 3 bytes: Byte 1 = código de finalización Byte 2 = revisión Byte 3 = 00h (dúplex medio) o 01h (dúplex completo)	C5h	datos 1 0x00 = dúplex medio 0x01 = dúplex completo

Parámetro	#	Datos de parámetro
Parámetro OEM (El valor de este parámetro es utilizado por XCC para obtener o establecer la Unidad de transmisión máxima (MTU) de la interfaz Ethernet.) Los datos de la respuesta devuelven 3 bytes: Byte 1 = código de finalización Byte 2 = revisión Byte 3-4 = tamaño de MTU	C6h	datos 1 Tamaño de MTU
Parámetro OEM (El XCC utiliza este número de parámetro para obtener o establecer la dirección MAC de administración local.) Los datos de la respuesta devuelven 3 bytes: Byte 1 = código de finalización Byte 2 = revisión Byte 3 – 8 = dirección Mac	C7h	datos 1 - 6 Dirección Mac

Opción IPMI para obtener la dirección de enlace local

Este es un parámetro de solo lectura para recuperar la dirección de enlace local IPV6.

Parámetro	#	Datos de parámetro
Parámetro OEM Este parámetro se usa para obtener la dirección de enlace local del XCC: Los datos de la respuesta arrojan lo siguiente: Byte 1 = código de finalización Byte 2 = revisión de parámetros (como en la especificación IPMI) Byte 3 = longitud de prefijo de dirección IPV6 Dirección de vínculo local de byte 4-19 en formato binario	C8h	

Opción IPMI para habilitar/deshabilitar IPv6

Este es un parámetro de lectura/escritura para habilitar/deshabilitar IPV6 en el XCC.

Parámetro	#	Datos de parámetro
Parámetro OEM Este parámetro se usa para habilitar/deshabilitar IPv6 en el XCC Los datos de la respuesta arrojan lo siguiente: Byte 1 = código de finalización Byte 2 = revisión de parámetros (como en la especificación IPMI) Byte 3 = 00h (deshabilitado) o 01h (habilitado)	C9h	datos 1 0x00 = deshabilitado 0x01 = habilitado

Transferencia de Ethernet sobre USB a la red externa

El siguiente parámetro se utiliza para configurar la conmutación de Ethernet sobre USB a la transferencia Ethernet externa.

Parámetro	#	Datos de parámetro
Parámetro OEM Este parámetro del comando Get/Set LAN Configuration Parameters no utiliza un Selector de conjuntos ni requiere un Selector de bloques, por lo que estos campos deben configurarse en 00h. Los datos de Obtener respuesta arrojan lo siguiente: Byte 1 = código de finalización Byte 2 = revisión Byte 3 = reservado (00h) Bytes 4:5 = número de puerto de Ethernet sobre USB (LSByte primero) Bytes 6:7 = número de puerto de Ethernet externo (LSByte primero) El número de bytes a seguir puede variar (1, 4 o 16 bytes) según el modo de direccionamiento: • Byte 8 = modos predefinidos: 00h = el paso a través está deshabilitado 01h = se usa la dirección IP de CMM Bytes 8:11 = dirección IP de red externa IPv4 en formato binario Bytes 8:23 = dirección IP de red externa IPv6 en formato binario Códigos de finalización: 00h: correcto 80h: no se admite el parámetro C1h: no se admite el comando C7h: longitud de datos de solicitud no válida	CAh	Establecer parámetros de configuración LAN: datos 1 reservado (= 00h) datos 2:3 Número de puerto de Ethernet sobre USB, LSByte primero datos 4:5 Número de puerto de Ethernet externo, LSByte primero El número de bytes a seguir puede variar (1, 4 o 16 bytes) según el modo de direccionamiento: datos 6 00h = deshabilitar la transferencia 01h = usar la dirección IP de CMM datos 6:9 Dirección IP de red externa IPv4 en formato binario datos 6:21 Dirección IP de red externa IPv6 en formato binario
Parámetro OEM Este parámetro se usa para establecer y obtener la dirección IP de LAN sobre USB y la máscara de red del XCC: Los datos de la respuesta arrojan lo siguiente: Byte 1 = código de finalización Byte 2 = revisión de parámetros (como en la especificación IPMI)	CBh	Datos 1:4 Dirección IP de la interfaz LAN sobre USB del XCC Datos 5:8 Máscara de red de la interfaz LAN sobre USB del XCC

Parámetro	#	Datos de parámetro
Byte 3:10 = dirección IP y valor de máscara de bits (MS-byte) primero		
Parámetro OEM Este parámetro se usa para establecer y obtener la dirección IP de LAN sobre USB del SO de host: Los datos de la respuesta arrojan lo siguiente: Byte 1 = código de finalización Byte 2 = revisión de parámetros (como en la especificación IPMI) Byte 3:6 = dirección IP (MS-byte) primero	CCh	Datos 1:4 Dirección IP de la interfaz LAN sobre USB del host

Consulta de inventario de paquetes lógicos

El siguiente parámetro se utiliza para consultar el inventario de paquetes de NCSI.

Parámetro	#	Datos de parámetro
Parámetro OEM Este parámetro del comando Get/ Set LAN Configuration Parameters no utiliza un Selector de conjuntos ni requiere un Selector de bloques, por lo que estos campos deben configurarse en 00h. Operación de consulta de inventario de paquete La operación de consulta de información del paquete se realiza emitiendo la solicitud con dos bytes de datos de 0x00, además del número del parámetro D3h. Inventario de paquete de consulta: --> 0x0C 0x02 0x00 0xD3 0x00 0x00 La respuesta XCC incluye un byte de información para cada paquete que está presente: bits 7:4 = número de canales de NCSI en el paquete bits 3:0 = el número de paquete lógico Respuesta --> 0x00 0x00 0x40 0x01 0x32 indica que hay 3 paquetes lógicos presentes: el paquete 0 tiene 4 canales NCSI el paquete 1 no es una NIC de NCSI, por lo que no es compatible con canales de NCSI. el paquete 2 tiene 3 canales NCSI	D3h	Obtener/definir parámetros de configuración de LAN:

Obtiene o establece los datos de un paquete lógico

El siguiente parámetro se utiliza para leer y establecer la prioridad asignada a cada paquete.

Parámetro	#	Datos de parámetro
Parámetro OEM Este parámetro del comando Get/ Set LAN Configuration Parameters no utiliza un Selector de conjuntos ni requiere un Selector de bloques, por lo que estos campos deben configurarse en 00h. El comando admite solo 2 operaciones: • Leer prioridad del paquete • Establecer prioridad del paquete Operación de lectura de prioridad del paquete La operación de lectura de prioridad del paquete se realiza emitiendo la solicitud con dos bytes de datos de 0x00, además del número del parámetro D4h. Leer prioridad del paquete: --> 0x0C 0x02 0x01 0xD4 0x00 0x00 Respuesta --> 0x00 0x00 0x00 0x12 0x23 paquete lógico 0 = prioridad 0 paquete lógico 2 = prioridad 1 paquete lógico 3 = prioridad 2 Operación de establecimiento de prioridad del paquete La operación de establecimiento de prioridad del paquete se realiza emitiendo la solicitud con uno o más parámetros además del número del parámetro D4h. Establecer prioridad del paquete: --> 0x0C 0x01 0x01 0xD4 0x00 0x12 0x23 establecer paquete lógico 0 = prioridad 0 establecer paquete lógico 2 = prioridad 1	D4	Obtener/definir parámetros de configuración de LAN: Bit [7-4] = prioridad del paquete lógico (1 = mayor, 15 = menor) Bit [3-0] = el número de paquete lógico

Parámetro	#	Datos de parámetro
establecer paquete lógico 3 = prioridad 2 Respuesta: solo código de finalización, sin datos adicionales		

Obtener/establecer estado de sincronización de la red de XCC

Parámetro	#	Datos de parámetro
Parámetro OEM El byte se usa para configurar para sincronizar la configuración de red entre el modo de NIC dedicado y compartido Este parámetro del comando Get LAN Configuration Parameters no utiliza un Selector de conjuntos ni requiere un Selector de bloques, por lo que estos campos deben configurarse en 00h. Los datos de la respuesta devuelven 3 bytes: Byte 1 = código de finalización Byte 2 = revisión Byte 3 = 00h (habilitado) o 01h (deshabilitado)	D5h	datos 1 0x00 = sincronización 0x01 = independencia

El byte se usa para configurar para sincronizar la configuración de red entre el modo NIC dedicado y compartido; el valor predeterminado fue 0h aquí, significa que XCC actualizará automáticamente la configuración de red entre el cambio de modo y utilizará la NIC compartida (incorporada) como referencia importante, si se establece como 1h, cada configuración de red será independiente en este caso, lo que permite configurar diferentes valores de red entre modos, como la habilitación de VLAN en dedicado y la configuración de VLAN deshabilitada en el modo NIC compartido.

Obtener/establecer el modo de red XCC

Parámetro	#	Datos de parámetro
Parámetro OEM Este parámetro se utiliza para obtener o establecer el modo de red de la NIC de gestión de XCC. Los datos de la respuesta devuelven 4 bytes: Byte 1 = código de finalización Byte 2 = revisión Byte 3 = modo de red aplicado/especificado Byte 4 = ID. de paquete del modo de red aplicado Byte 5 = ID. de canal del modo de red aplicado	D6h	Establecer parámetros de configuración LAN: datos 1 Modo de red para establecer Obtener parámetros de configuración LAN: datos 1 Modo de red para obtener, Se trata de datos opcionales, valores predeterminados para consultar el modo de red actual

Comandos IPMI OEM

El XCC es compatible con los siguientes comandos IPMI OEM. Cada comando requiere un nivel de privilegio diferente, como se indica a continuación.

Código	Comandos Netfn 0x2E	Privilegio
0xCC	Restablecer XCC en valores predeterminados	PRIV_USR

Código	Comandos Netfn 0x3A	Privilegio
0x00	Consultar versión de firmware	PRIV_USR
0x0D	Información de placa	PRIV_USR
0x1E	Opciones de retardo de restauración de alimentación del chasis	PRIV_USR
0x38	NMI y restablecimiento	PRIV_USR
0x49	Iniciar recopilación de datos	PRIV_USR
0x4A	Insertar archivo	PRIV_USR
0x4D	Estado de recopilación de datos	PRIV_USR
0x50	Obtener información sobre el build	PRIV_USR
0x55	Obtener/establecer nombre de host	PRIV_USR

Código	Comandos Netfn 0x3A	Privilegio
0x6B	Consultar nivel de revisión de firmware de FPGA	PRIV_USR
0x6C	Consulta de nivel de revisión del hardware de placa	PRIV_USR
0x6D	Consultar nivel de revisión de firmware de PSoC	PRIV_USR
0x98	Control de puerto USB FP	PRIV_USR
0xC7	Conmutador IPMI NM nativo	PRIV_ADM

Restablecer XCC a la configuración predeterminada

Este comando restablece el valor de la configuración XCC a los valores predeterminados.

Función de red = 0x2E			
Código	**Comando**	**Solicitud, datos de respuesta**	**Descripción**
0xCC	Restablecer XCC en valores predetermi-nados	**Solicitud:** Byte 1 – 0x5EByte 2 – 0x2B Byte 3 – 0x00 Byte 4 – 0x0AByte 5 – 0x01 Byte 6 – 0xFF Byte 7 – 0x00Byte 8 – 0x00 Byte 9 – 0x00 **Respuesta:** Byte 1 – Código de finalizaciónByte 2 – 0x5EByte 3 – 0x2B Byte 4 – 0x00 Byte 5 – 0x0AByte 6 – 0x01 Byte 7 – datos de respuesta 0 = correcto distinto de cero = error	Este comando restablece el valor de la configuración XCC a los valores predeterminados.

Comandos de información de firmware/placa

Esta sección enumera los comandos para consultar la placa y la información de firmware.

Función de red = 0x3A			
Código	**Comando**	**Solicitud, datos de respuesta**	**Descripción**
0x00	Consultar versión de firmware	**Solicitud**: No hay datos en la solicitud **Respuesta**: Byte 1 – Código de finalización Byte 2 – Versión mayor Byte 3 – Versión menor	Este comando arroja los números de versión principal y secundaria del firmware. Si el comando se realiza con el byte opcional 1 de la solicitud de datos, la respuesta XCC también arroja el tercer campo (revisión) de la versión. (Mayor.Menor.Revisión)
0x0D	Consultar información de placa	**Solicitud**: N/A **Respuesta**: Byte 1 – ID del sistema Byte 2 – revisión de la placa	Este comando arroja el ID de la placa y la revisión plana.
0x50	Consultar información de build	**Solicitud**: N/A **Respuesta**: Byte 1 – código de finalización. Bytes 2:10 – nombre de build ASCIIZ Bytes 11:23 – fecha de build ASCIIZ Bytes 24:31: tiempo de build ASCII	Este comando arroja el nombre del build, la fecha del build y la hora del build. El nombre del build y las cadenas de fecha del build tienen cero finalización. El formato de la fecha de build es AAAA-MM-DD. por ej. “ZUBT99A” “2005-03-07” “23:59:59”

Función de red = 0x3A			
Código	**Comando**	**Solicitud, datos de respuesta**	**Descripción**
0x6B	Consultar nivel de revisión de firmware de FPGA	**Solicitud**: Byte 1 – Tipo de dispositivo FPGA* Tipo de dispositivo FPGA 0 = local (nivel activo) 1 = tarjeta de CPU 1 (nivel activo) 2 = tarjeta de CPU 2 (nivel activo) 3 = tarjeta de CPU 3 (nivel activo) 4 = tarjeta de CPU 4 (nivel activo) 5 = ROM principal local 6 = ROM de recuperación local **Respuesta**: Byte 1 – Código de finalización Byte 2 – nivel de revisión principal Byte 3 – nivel de revisión menor Byte 4 – nivel de revisión submenor (Byte de prueba en plataformas XCC)	Este comando arroja el nivel de revisión del firmware de FPGA. Si se omite el byte 1, se seleccionará Local (nivel activo)
0x6C	Consulta de nivel de revisión del hardware de placa	**Solicitud**: Sin datos. **Respuesta**: Byte 1 – Código de finalización Byte 2 – nivel de revisión	Este comando arroja el nivel de revisión del hardware de la placa donde reside el FPGA.
0x6D	Consultar nivel de revisión de firmware de PSoC	**Solicitud**: Ninguno **Respuesta**: Byte 1 – Código de finalización Byte 2 – n.° de bin Byte 3 – APID Byte 4 – Rev	Este comando arroja el nivel de revisión de todos los dispositivos PSoC detectados. Nota: el n.º bin representa una ubicación física. Consulte la especificación del sistema para obtener más detalles.

Función de red = 0x3A			
Código	**Comando**	**Solicitud, datos de respuesta**	**Descripción**
		Byte 5-6 – ID. FRU Bytes 6:N – se repiten bytes 2-6 por cada PSoC detectado	

Comandos de control del sistema

La especificación IPMI proporciona un control de encendido y restablecimiento básico. Lenovo añade funciones de control adicionales.

<table>
<tr><th colspan="4">Función de red = 0x3A</th></tr>
<tr><th>Código</th><th>Comando</th><th>Solicitud, datos de respuesta</th><th>Descripción</th></tr>
<tr><td>0x1E</td><td>Opciones de retardo de restauración de alimentación del chasis</td><td>Solicitud:<table><tr><td>Byte 1</td><td>Tipo de solicitud:

0x00 = establecer opciones de retardo

0x01 = consultar opciones de retraso</td></tr><tr><td>Byte 2</td><td>(si el byte 1 = 0x00)

0x00 = Deshabilitado (predetermina-do)

0x01 = Aleatorio

0x02 - 0xFF Reservado</td></tr></table>Respuesta:

Byte 1 – Código de finalización

Byte 2 – Opciones de retraso (solo para solicitud de consulta)</td><td>Este valor se utiliza cuando la política de restauración de la alimentación del chasis está configurada en siempre encender o restaurar a encendido (si se ha encendido previamente), una vez que se aplica/devuelve el CA. Hay 2 opciones: Deshabilitado (el valor predeterminado, sin demora al encender) y Aleatorio. El valor de demora aleatoria proporciona una demora aleatoria entre 1 y 15 segundos, desde el momento en que se aplica/regresa la CA y cuando el servidor se enciende automáticamente.

XCC solo admite el comando en servidores de bastidor.</td></tr>
<tr><td>0x38</td><td>NMI y restableci-miento</td><td>Solicitud:

Byte 1 – Número de segundos
0 = Solo NMI

Byte 2 – Tipo de restablecimiento
0 = restablecimiento suave
1 = ciclo de alimentación

Respuesta :

Byte 1 – Código de finalización</td><td>Este comando se utiliza para la realizar un NMI de sistema. Opcionalmente, el sistema puede restablecerse (rearrancar) o encenderse después del NMI.

Si el campo “Número de segundos” no es 0, el sistema se restablecerá o se realizará un ciclo de alimentación después de un número especificado de segundos.

El byte 2 de la solicitud es opcional. Si no se proporciona el byte 2 o si tiene un valor de 0x00, se realiza un restablecimiento parcial. Si el 2 de bytes es 0x01, el sistema se recorre.</td></tr>
</table>

Comandos varios

Esta sección contiene los comandos que no entran en ninguna otra sección.

<table>
<tr><th colspan="4">Función de red = 0x3A</th></tr>
<tr><th>Código</th><th>Comando</th><th>Solicitud, datos de respuesta</th><th>Descripción</th></tr>
<tr><td>0x55</td><td>Obtener/ establecer nombre de host</td><td>Longitud de solicitud =0:

Datos de la solicitud vacíos

Respuesta:

<table><tr><td>Byte 1</td><td>Código de finalización</td></tr><tr><td>Bytes 2-65</td><td>Nombre de host actual.

ASCIIZ, cadena terminada en nulo.</td></tr></table>
Longitud de solicitud 1-64:

<table><tr><td>Bytes 1-64</td><td>Nombre de host de DHCP

ASCIIZ finalizar con 00h</td></tr></table></td><td>Utilice este comando para obtener/establecer el nombre de host.

Al establecer el nombre de host, el valor deseado debe terminar con un 00h. El nombre de host está limitado a 63 caracteres más el valor nulo.</td></tr>
<tr><td>0x98</td><td>Control de puerto USB FP</td><td>Solicitud:

Byte 1

<table><tr><td>01h:</td><td>Obtener el propietario actual del puerto USB del panel frontal</td></tr></table>
Respuesta:

Byte 1 – Código de finalización

Byte 2

<table><tr><td>00h:</td><td>Propiedad del host</td></tr><tr><td>01h:</td><td>Propiedad del BMC</td></tr></table>
Solicitud:

Byte 1

<table><tr><td>02h:</td><td>Obtener la configuración del puerto</td></tr></table></td><td>Este comando se utiliza para el consultar el estado o la configuración del puerto USB FP, configurar el modo/tiempo de espera del puerto USB de FP y cambiar el propietario del puerto USB del host y BMC

En la configuración, el USB FP puede tener 3 modos: dedicado al host, propiedad exclusiva del BMC o modo compartido, que permite que el propietario cambie entre el host y el BMC.

Si el modo compartido está habilitado, el puerto USB se conecta al BMC cuando el servidor se apaga y se conecta al servidor cuando la alimentación del servidor está encendida.

Cuando el modo compartido está habilitado y la alimentación del servidor está activada, el BMC devuelve el puerto USB al servidor después de que se agota el tiempo de espera por inactividad en la configuración.</td></tr>
</table>

<table>
<tr><th colspan="4">Función de red = 0x3A</th></tr>
<tr><th>Código</th><th>Comando</th><th>Solicitud, datos de respuesta</th><th>Descripción</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td></td><td>USB del panel frontal</td></tr>
</table>
Respuesta:

Byte 1 – Código de finalización

Byte 2
<table>
<tr><td>00h:</td><td>Dedicado al host</td></tr>
<tr><td>01h:</td><td>Dedicado a BMC</td></tr>
<tr><td>02h:</td><td>Modo compartido</td></tr>
</table>
Byte 3:4 – Tiempo de espera de inactividad en minutos (primero MSB)

Byte 5 – Habilitar botón de ID.
<table>
<tr><td>00h:</td><td>Deshabilitado</td></tr>
<tr><td>01h:</td><td>Habilitado</td></tr>
</table>
Byte 6 – Histéresis (opcional) en segundos

Solicitud:

Byte 1

03h: establecer la configuración del puerto USB del panel frontal

Byte 2
<table>
<tr><td>00h:</td><td>Dedicado al host</td></tr>
<tr><td>01h:</td><td>Dedicado a BMC</td></tr>
<tr><td>02h:</td><td>Modo compartido</td></tr>
</table>
Byte 3:4 – Tiempo de espera de inactividad en minutos (primero MSB)

Byte 5 – Habilitar botón de ID.
<table>
<tr><td>00h:</td><td>Deshabilitado</td></tr>
</table>
</td><td>Si el servidor tiene un botón de identificación, los usuarios pueden habilitar/deshabilitar el Botón de ID. para cambiar el propietario del puerto USB FP al mantener pulsado el Botón de ID. durante más de 3 segundos.

Histéresis en segundos se establecerá al cambiar automáticamente el puerto durante el ciclo de alimentación. Este es un parámetro opcional.

Servidores SD530

En la plataforma SD530, el puerto es opcional y si está presente, está conectado directamente al XCC y solo al XCC. Cambio del puerto al host no disponible.

Cuando se emite el comando con el byte 1 = 1, el XCC siempre responderá que el puerto es propiedad del BMC.
Cuando se emite el comando con el byte 1 = 2, el XCC siempre responderá que el puerto está dedicado al BMC.
Cuando se emite el comando con el byte 1 = 3 o el byte 1 = 4, el XCC responderá con el código de finalización D6h.

Servidores no SD530

En la plataforma no SD530, el uso del XCC del puerto USB del panel frontal puede deshabilitarse cambiando al modo “Solo host”.

Cuando se emite el comando con el byte 1 = 5 o el byte 1 = 6, el XCC responderá con el código de finalización D6h.</td></tr>
</table>

<table>
<tr><th colspan="4">Función de red = 0x3A</th></tr>
<tr><th>Código</th><th>Comando</th><th>Solicitud, datos de respuesta</th><th>Descripción</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td>01h:</td><td>Habilitado</td></tr>
</table>
Byte 6 – Histéresis (opcional) en segundos
Respuesta:
Byte 1 – Código de finalizaciónByte 2
<table>
<tr><td>00h:</td><td>Cambiar a host</td></tr>
<tr><td>01h:</td><td>Cambiar a BMC</td></tr>
</table>
Respuesta:
Byte 1 – Código de finalización
Byte 1
<table>
<tr><td>05h:</td><td>Habilitar/ deshabilitar el puerto USB del panel frontal</td></tr>
</table>
Byte 2
<table>
<tr><td>00h:</td><td>Función</td></tr>
<tr><td>01h:</td><td>Función</td></tr>
</table>
Respuesta:
Byte 1 – Código de finalización
Solicitud:
Byte 1
<table>
<tr><td>06h:</td><td>Leer el estado habilitado/ deshabilitado del puerto USB del panel frontal</td></tr>
</table>
Respuesta:
Byte 1 – Código de finalización
Byte 2
</td><td></td></tr>
</table>

<table>
<tr><th colspan="4">Función de red = 0x3A</th></tr>
<tr><th>Código</th><th>Comando</th><th>Solicitud, datos de respuesta</th><th>Descripción</th></tr>
<tr><td>0xC7</td><td>Conmutador IPMI NM nativo</td><td>Longitud de solicitud = 0:

Datos de la solicitud vacíos

Respuesta:

<table><tr><td>Byte 1</td><td>Código de finalización</td></tr><tr><td>Bytes 2</td><td>Estado de habilitación/ deshabilita- ción actual</td></tr></table>
Longitud de solicitud= 1:

<table><tr><td>Byte 1</td><td>Atributo de Habilitación/ deshabilita- ción de la interfaz IPMI NM nativa

00h – Deshabilitar

01h – Habilitar</td></tr></table>
Respuesta:

<table><tr><td>Byte 1</td><td>Código de finalización</td></tr></table></td><td>Este comando se utiliza para habilitar/deshabilitar la función de puente de XCC para los comandos nativos de Intel IPMI.</td></tr>
</table>

Capítulo 12. Servidores Edge

En este tema se describen las funciones específicas de los servidores Edge.

Notas:

1. El sistema requiere que cambie la contraseña XCC en su primer inicio de sesión.
2. IPMI sobre LAN está deshabilitado de manera predeterminada.
3. IPMI sobre KCS está deshabilitado de manera predeterminada.

Modo de bloqueo del sistema

Cuando el **Modo de bloqueo del sistema** está en estado activo, significa que el sistema está en modo de bloqueo. Puede activar el sistema y desbloquearlo; de lo contrario, el sistema de host no tendrá permiso para arrancar.

Nota: El modo de bloqueo del sistema solo está disponible para SE350 con Paquete de seguridad, pero no el estándar SE350. La versión se puede comprobar en la pestaña **Inicio** en **Información del sistema y Configuración**.

Haga clic en **Seguridad** en **Configuración de BMC** y desplácese al **Modo de bloqueo de sistema**.

Modo de bloqueo del sistema

Para activar el sistema y salir del **Modo de bloqueo del sistema**, lleve a cabo los pasos siguientes.

1. Haga clic en el botón **Inactivo** y aparecerá una ventana emergente de **Activación de Key Vault** para mostrar el **Texto de desafío**.
2. Póngase en contacto con su administrador de TI y proporcione **Texto de desafío**.
3. Obtenga la **Respuesta de desafío** de su administrador de TI y escríbala en la ventana de **Activación de Key Vault**..
4. Haga clic en el botón **Aceptar** y, a continuación, haga clic en **Aplicar**.
5. Si todos los valores de configuración funcionan correctamente, verá los cambios del **Modo de bloqueo del sistema** a **Inactivo**.

Nota: Cuando el modo de bloqueo del sistema está en estado activo, se **niega** el acceso a los secretos del sistema, como las claves SED.

Para obligar al sistema a entrar en el Modo de bloqueo del sistema, lleve a cabo los pasos siguientes.

1. Haga clic en el botón **Activo**.
2. Haga clic en el botón **Aceptar** y, a continuación, haga clic en **Aplicar**.

Detección de movimiento

Puede habilitar esta función para proteger el servidor detectando cualquier movimiento físico del servidor.

Si la Detección de movimiento está habilitada, puede establecer los siguientes elementos dependiendo de su preferencia y de la configuración.

- **Nivel de sensibilidad**: seleccione el nivel de sensibilidad de **Bajo**, **Medio** y **Alto**, de acuerdo con su preferencia.
- **Orientación**: seleccione la configuración del **Pedestal para escritorio**, **Montaje de pared (horizontal)**, **Montaje de pared (vertical)**, **Estante** y **Montaje de techo**.

Nota: La detección de movimiento se deshabilitará automáticamente cuando el sistema entra en el modo de bloqueo.

Detección de intrusión de chasis
Puede habilitar esta función para proteger el servidor detectando cualquier movimiento físico de la cubierta superior.

Configuraciones adicionales
Si se instala el paquete LOM habilitado inalámbrico, hay tres valores que puede elegir para un suceso de alteración detectado.
En algunas circunstancias inusuales, es posible que no se pueda verificar el **Texto de desafío** en ThinkShield Key Vault Portal, podría ser necesario restablecer el contador interno del dispositivo antes de activar el dispositivo bajo la solicitud del administrador de TI.

Gestor de claves de autenticación de SED (AK)

Al sistema instalado con SED (unidad de autocifrado), esta función controla el BMC para desplegar la clave SED. Puede utilizar la clave SED para cifrar las unidades de arranque y de datos, así como para arrancar el sistema sin intervención manual.

Nota: Esta operación no está permitida cuando el sistema no está activado (se ha declarado el modo de bloqueo de sistema) o el usuario actual no tiene permiso para gestionar la clave SED.

Nota: El modo de bloqueo del sistema solo está disponible para SE350 con Paquete de seguridad, pero no el estándar SE350. La versión se puede comprobar en la pestaña **Inicio** en **Información del sistema y Configuración**.

Nota: El SE350 también admite una función de copia de seguridad automática siempre que el kit de habilitación ThinkSystem M.2 o el kit de habilitación de duplicación ThinkSystem M.2 se realicen en un estado correcto. Si el hardware está dañado, pero tanto el kit SED como el M.2 están en un estado correcto, se pueden instalar en otro SE350 y se puede restaurar el SED AK. Sin embargo, para prepararse para un bloqueo completo del hardware, Lenovo recomienda hacer una copia de seguridad de SED AK.

Haga clic en **Seguridad** en **Configuración de BMC** y desplácese hasta el **Gestor de claves de autenticación de sed (AK)**.

Cambiar el SED AK
Generar SED AK a partir de la frase de contraseña: establezca la contraseña y vuelva a introducirla para la confirmación. Haga clic en **Volver a generar** para obtener la nueva SED AK.
Generar SED AK aleatoria: haga clic en **Volver a generar** para obtener una SED AK aleatoria.
Crear copia de seguridad de SED AK: establezca la contraseña y vuelva a introducirla para la confirmación. Haga clic en **Iniciar copia de seguridad** para crear una copia de seguridad de SED AK; luego descargue el archivo SED AK y guárdelo de forma segura para utilizarlo en el futuro.

Nota: Si utiliza el archivo de copia de seguridad SED AK para restaurar una configuración, el sistema le pedirá la contraseña que estableció.

Recuperar el SED AK: solo puede realizar esta tarea mientras el SED no está funcionando correctamente. Hay dos formas de recuperar el SED AK:

- **Recuperar SED AK con frase de contraseña**: utilice la contraseña que estableció en el modo **Generar SED AK desde frase de contraseña** para recuperar la SED AK.
- **Recuperar SED AK desde el archivo de copia de seguridad**: cargue el archivo de copia de seguridad generado en el modo **Realizar copia de seguridad del SED AK** e ingrese la contraseña del archivo de copia de seguridad correspondiente para recuperar la SED AK.

Redes Edge

Esta página de función solo se admite mientras el paquete LOM habilitado inalámbrico está instalado.

Para conocer las tablas de valores predeterminados de la topología de red, consulte https://thinksystem.lenovofiles.com/help/topic/SE350/pdf_files.html para obtener más detalles.

Conectividad Wi-Fi
Haga clic en **Habilitado** y podrá configurar los valores de acuerdo con su configuración de Wi-Fi.

Conectividad LTE
Esto le permite controlar la conectividad de LTE para la placa de red Edge.

Dirección de la placa de red Edge

Estado de **IPv4 o IPv6**	Estado de **servidor DHCP**	**Método**
Deshabilitado	**Deshabilitado**	**Obtener IP de DHCP**
Habilitado	**Habilitado**	**Usar dirección IP estática**
Habilitado	**Deshabilitado**	**Obtener IP de DHCP** o **Utilizar dirección IP estática** en función de su uso.

Puente de red de BMC
Puede acceder al BMC a través de los **Puertos de enlace de bajada**, **Puertos Wi-Fi**, **Puertos de enlace de subida** o **Ninguno**.

Nota: Seleccionar **None** hace referencia a que esta función está deshabilitada.

Resolución de problemas de la placa de red Edge
Reiniciar inmediatamente: puede reiniciar la placa de red con este botón.
Restablecer a valores predeterminados de fábrica: puede restablecer la placa de red a los valores predeterminados mediante este botón.

Apéndice A. Obtención de ayuda y asistencia técnica

Si necesita ayuda, servicio o asistencia técnica, o simplemente desea obtener más información acerca de los productos de Lenovo, encontrará una amplia variedad de fuentes disponibles en Lenovo que le asistirán.

En la siguiente dirección de la World Wide Web, encontrará información actualizada acerca de los sistemas, los dispositivos opcionales, los servicios y el soporte de Lenovo:

http://datacentersupport.lenovo.com

Nota: Esta sección incluye referencias a sitios web de IBM e información sobre cómo obtener servicio. IBM es el proveedor de servicios preferido de Lenovo para ThinkSystem.

Antes de llamar

Antes de llamar, existen varios pasos que debe tomar para intentar resolver el problema usted mismo. Si decide que necesita solicitar asistencia, recopile la información necesaria para el técnico de servicio para facilitar la resolución expedita del problema.

Intente resolver el problema usted mismo

Usted puede resolver muchos problemas sin asistencia externa siguiendo los procedimientos de resolución de problemas que Lenovo proporciona en la ayuda en línea o en la documentación del producto Lenovo. La documentación del producto Lenovo también describe las pruebas de diagnóstico que usted puede realizar. La documentación de la mayoría de sistemas, sistemas operativos y programas contiene procedimientos de resolución de problemas y explicaciones de mensajes de error y códigos de error. Si sospecha que tiene un problema de software, consulte la documentación del sistema operativo o del programa.

Encontrará documentación de producto para los productos ThinkSystem en la siguiente ubicación

https://pubs.lenovo.com/

Puede realizar estos pasos para intentar solucionar el problema usted mismo:

- Compruebe todos los cables para asegurarse de que están correctamente conectados.
- Compruebe los interruptores de alimentación para asegurarse de que el sistema y los posibles dispositivos opcionales están encendidos.
- Revise los controladores de dispositivo actualizados de software, firmware y sistema operativo para su producto Lenovo. Los términos y condiciones de Lenovo Warranty establecen que usted, el propietario del producto Lenovo, es responsable del mantenimiento y la actualización de todo el software y firmware para el producto (excepto que esté cubierto por un contrato de mantenimiento adicional). Su técnico de servicio le solicitará que actualice su software y firmware si el problema posee una solución documentada dentro de una actualización de software.
- Si ha instalado hardware o software nuevos en su entorno, revise http://www.lenovo.com/serverproven/ para asegurarse de que el hardware y software son compatibles con su producto.
- Vaya a http://datacentersupport.lenovo.com y revise la información sobre cómo resolver el problema.
  - Revise los foros de Lenovo en https://forums.lenovo.com/t5/Datacenter-Systems/ct-p/sv_eg para ver si otro se encontró con un problema similar.

Usted puede resolver muchos problemas sin asistencia externa siguiendo los procedimientos de resolución de problemas que Lenovo proporciona en la ayuda en línea o en la documentación del producto Lenovo. La documentación del producto Lenovo también describe las pruebas de diagnóstico que usted puede realizar.

La documentación de la mayoría de sistemas, sistemas operativos y programas contiene procedimientos de resolución de problemas y explicaciones de mensajes de error y códigos de error. Si sospecha que tiene un problema de software, consulte la documentación del sistema operativo o del programa.

Recopilación de información necesaria para llamar a Soporte

Si cree que requiere servicio de garantía para su producto Lenovo, los técnicos de servicio estarán disponibles para ayudarlo de forma más eficaz si usted se prepara antes de llamar. También puede consultar http://datacentersupport.lenovo.com/warrantylookup para obtener más información sobre la garantía del producto.

Reúna la siguiente información para proporcionar al técnico de servicio. Esta información ayudará al técnico de servicio a proporcionar rápidamente una solución para su problema y asegurar que usted reciba el nivel de servicio que ha contratado.

- Números de contrato del acuerdo de Mantenimiento de hardware y software, si corresponde
- Número del tipo de equipo (identificador de 4 dígitos del equipo Lenovo)
- Número de modelo
- Número de serie
- Niveles de firmware para el sistema actual y UEFI
- Otra información pertinente, como mensajes y registros de errores

Como alternativa a llamar a soporte de Lenovo, puede ir a https://www-947.ibm.com/support/servicerequest/Home.action para enviar una solicitud de servicio electrónico. Al enviar una Solicitud de servicio electrónico se inicia el proceso para determinar una solución a su problema poniendo la información relevante a disposición de los técnicos de servicio. Los técnicos de servicio de Lenovo podrán empezar a trabajar en la búsqueda de una solución en cuanto haya completado y enviado una Solicitud de servicio electrónico.

Recopilación de datos de servicio

Para identificar claramente la causa de un problema de servidor o para atender a una petición del soporte técnico de Lenovo, es posible que deba recopilar datos del servicio que se pueden utilizar para un análisis posterior. Los datos de servicio incluyen información como registros de eventos e inventario de hardware.

Los datos de servicio se pueden recopilar a través de las siguientes herramientas:

- **Lenovo XClarity Controller**

  Puede utilizar la interfaz web de Lenovo XClarity Controller o la CLI para recopilar datos de servicio del servidor. El archivo se puede guardar y enviar a soporte técnico de Lenovo.

  - Para obtener más información sobre cómo usar la interfaz web para recopilar datos del servicio, consulte https://pubs.lenovo.com/xcc/NN1ia_c_servicesandsupport.html.
  - Para obtener más información sobre el uso de la CLI para recopilar datos del servicio, consulte https://pubs.lenovo.com/xcc/nn1ia_r_ffdccommand.html.

- **Lenovo XClarity Administrator**

  Lenovo XClarity Administrator se puede configurar para que automáticamente recopile y envíe archivos de diagnóstico al soporte técnico de Lenovo cuando ocurran ciertos eventos de mantenimiento en Lenovo XClarity Administrator y en los puntos finales gestionados. Puede elegir enviar los archivos de diagnóstico a Soporte técnico de Lenovo mediante Call Home o a otro proveedor de servicio mediante SFTP. También puede recopilar los archivos de diagnóstico de forma manual, abrir un registro de problemas y enviar archivos de diagnóstico al centro de soporte de Lenovo.

  Puede encontrar más información acerca de la configuración de notificaciones automáticas en Lenovo XClarity Administrator en https://pubs.lenovo.com/lxca/admin_setupcallhome.html.

- **Lenovo XClarity Provisioning Manager**

  Utilice la función de recopilación de datos del servicio de Lenovo XClarity Provisioning Manager para recopilar datos del servicio del sistema. Puede recopilar datos existentes del registro del sistema o ejecutar un nuevo diagnóstico para recopilar nuevos datos.

- **Lenovo XClarity Essentials**

  Lenovo XClarity Essentials puede ejecutarse en banda desde el sistema operativo. Además de datos de servicio de hardware, Lenovo XClarity Essentials puede recopilar información sobre el sistema operativo, como el registro de sucesos del sistema operativo.

  Para obtener datos del servicio, puede ejecutar el comando `getinfor`. Para obtener más información acerca de la ejecución de `getinfor`, consulte https://pubs.lenovo.com/lxce-onecli/onecli_r_getinfor_command.html.

Ponerse en contacto con soporte

Puede ponerse en contacto con soporte para obtener ayuda para su problema.

Puede recibir servicio para hardware a través de un proveedor de servicio autorizado de Lenovo. Para localizar a un proveedor de servicio autorizado por Lenovo para prestar servicio de garantía, visite la página https://datacentersupport.lenovo.com/us/en/serviceprovider y use los filtros de búsqueda para diferentes países. Para obtener los números de teléfono de soporte de Lenovo, consulte https://datacentersupport.lenovo.com/us/en/supportphonelist para ver los detalles de soporte de su región.

Apéndice B. Avisos

Puede que Lenovo no comercialice en todos los países los productos, servicios o características a los que se hace referencia en este documento. Póngase en contacto con su representante local de Lenovo para obtener información acerca de los productos y servicios disponibles actualmente en su zona.

Las referencias a productos, programas o servicios de Lenovo no pretenden afirmar ni implicar que solo puedan utilizarse esos productos, programas o servicios de Lenovo. En su lugar, puede utilizarse cualquier producto, programa o servicio funcionalmente equivalente que no infrinja ninguno de los derechos de propiedad intelectual de Lenovo. Sin embargo, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier otro producto, programa o servicio.

Lenovo puede tener patentes o solicitudes de patentes pendientes que aborden temas descritos en este documento. La posesión de documento no constituye una oferta y no le otorga ninguna licencia sobre ninguna patente o solicitud de patente. Puede enviar sus consultas, por escrito, a:

Lenovo (United States), Inc.
1009 Think Place
Morrisville, NC 27560
U.S.A.
Attention: Lenovo VP of Intellectual Property

LENOVO PROPORCIONA ESTA PUBLICACIÓN “TAL CUAL” SIN GARANTÍA DE NINGUNA CLASE, NI EXPLÍCITA NI IMPLÍCITA, INCLUIDAS, PERO SIN LIMITARSE A, LAS GARANTÍAS IMPLÍCITAS DE NO VULNERACIÓN DE DERECHOS, COMERCIABILIDAD O IDONEIDAD PARA UNA FINALIDAD DETERMINADA. Algunas legislaciones no contemplan la exclusión de garantías, ni implícitas ni explícitas, por lo que puede haber usuarios a los que no afecte dicha norma.

Esta información podría incluir inexactitudes técnicas o errores tipográficos. La información aquí contenida está sometida a modificaciones periódicas, las cuales se incorporarán en nuevas ediciones de la publicación. Lenovo se reserva el derecho a realizar, si lo considera oportuno, cualquier modificación o mejora en los productos o programas que se describen en esta publicación.

Los productos descritos en este documento no están previstos para su utilización en implantes ni otras aplicaciones de reanimación en las que el funcionamiento incorrecto podría provocar lesiones o la muerte a personas. La información contenida en este documento no cambia ni afecta a las especificaciones o garantías del producto de Lenovo. Ninguna parte de este documento deberá regir como licencia explícita o implícita o indemnización bajo los derechos de propiedad intelectual de Lenovo o de terceros. Toda la información contenida en este documento se ha obtenido en entornos específicos y se presenta a título ilustrativo. Los resultados obtenidos en otros entornos operativos pueden variar.

Lenovo puede utilizar o distribuir la información que le suministre el cliente de la forma que crea oportuna, sin incurrir con ello en ninguna obligación con el cliente.

Las referencias realizadas en esta publicación a sitios web que no son de Lenovo se proporcionan únicamente en aras de la comodidad del usuario y de ningún modo pretenden constituir un respaldo de los mismos. La información de esos sitios web no forma parte de la información para este producto de Lenovo, por lo que la utilización de dichos sitios web es responsabilidad del usuario.

Los datos de rendimiento incluidos en este documento se han obtenido en un entorno controlado. Así pues, los resultados obtenidos en otros entornos operativos pueden variar de forma significativa. Es posible que algunas mediciones se hayan realizado en sistemas en desarrollo, por lo que no existen garantías de que estas sean las mismas en los sistemas de disponibilidad general. Además, es posible que la estimación de

algunas mediciones se haya realizado mediante extrapolación. Los resultados reales pueden variar. Los usuarios de la presente publicación deben verificar los datos pertinentes en su entorno de trabajo específico.

Marcas registradas

Lenovo, el logotipo de Lenovo, ThinkSystem, Flex System, System x, NeXtScale System y x-Architecture son marcas registradas de Lenovo en Estados Unidos, en otros países o en ambos.

Intel e Intel Xeon son marcas registradas de Intel Corporation en Estados Unidos y/o en otros países.

Internet Explorer, Microsoft y Windows son marcas registradas del grupo de empresas Microsoft.

Linux es una marca registrada de Linus Torvalds.

Otros nombres de empresas, productos o servicios pueden ser marcas registradas o marcas de servicio de otras compañías.

Notas importantes

La velocidad del procesador indica la velocidad del reloj interno del microprocesador; también hay otros factores que afectan al rendimiento de la aplicación.

La velocidad de la unidad de CD o DVD es la velocidad de lectura variable. Las velocidades reales varían y con frecuencia son inferiores a la velocidad máxima posible.

Cuando se hace referencia al almacenamiento del procesador, al almacenamiento real y virtual o al volumen del canal, KB representa 1.024 bytes, MB representa 1.048.576 bytes y GB representa 1.073.741.824 bytes.

Cuando se hace referencia a la capacidad de la unidad de disco duro o al volumen de comunicaciones, MB representa 1 000 000 bytes y GB representa 1 000 000 000 bytes. La capacidad total a la que puede acceder el usuario puede variar en función de los entornos operativos.

Las capacidades máximas de las unidades de disco internas suponen sustituir cualquier unidad de disco duro estándar y llenar todas las bahías de unidad de disco duro con las unidades de mayor tamaño admitidas actualmente y disponibles en Lenovo.

Es posible que la memoria máxima requiera la sustitución de la memoria estándar por un módulo de memoria opcional.

Cada celda de memoria de estado sólido cuenta con un número finito e intrínseco de ciclos de escritura en los que la celda puede incurrir. Por lo tanto, un dispositivo de estado sólido tiene un número máximo de ciclos de escritura a los que puede estar sujeto. Estos se expresan como `total bytes written` (total de bytes escritos, TBW). Un dispositivo que excede este límite puede no responder a los mandatos generados por el sistema o bien no se podrá escribir en él. Lenovo no se hace responsable de la sustitución de un dispositivo que haya excedido el número garantizado máximo de ciclos de programa/eliminación, como está documentado en las Especificaciones oficiales publicadas para el dispositivo.

Lenovo no ofrece declaraciones ni garantía de ningún tipo respecto a productos que no sean de Lenovo. El soporte (si existe) para productos que no sean de Lenovo lo proporcionan terceros y no Lenovo.

Es posible que parte del software difiera de su versión minorista (si está disponible) y que no incluya manuales de usuario o todas las funciones del programa.

Contaminación por partículas

Atención: Las partículas que transporta el aire (incluyendo partículas o escamas metálicas) o gases reactivos, bien por sí solos o en combinación con otros factores del entorno como la humedad o la temperatura, pueden representar un riesgo para el dispositivo que se describe en este documento.

Los riesgos que representan la presencia de concentraciones o niveles excesivos de partículas o gases perjudiciales incluyen daños que pueden hacer que el dispositivo funcione incorrectamente o deje de funcionar completamente. Esta especificación establece los límites que deben mantenerse para estos gases y partículas a fin de evitar estos daños. Dichos límites no se deben considerar ni utilizar como límites definitivos, ya que muchos otros factores, como la temperatura o el contenido de humedad en el aire, pueden influir en el efecto que tiene la transferencia de partículas o de contaminantes gaseosos o corrosivos del entorno. A falta de límites específicos establecidos en este documento, debe implementar métodos que mantengan unos niveles de partículas y gases que permitan garantizar la protección de la seguridad y de la salud de las personas. Si Lenovo determina que los niveles de partículas o gases del entorno han causado daños en el dispositivo, Lenovo puede condicionar el suministro de la reparación o sustitución de los dispositivos o las piezas a la implementación de las medidas correctivas adecuadas para mitigar dicha contaminación ambiental. La implementación de estas medidas correctivas es responsabilidad del cliente.

Tabla 67. Límites para partículas y gases

Contaminante	Límites
Partícula	• El aire de la sala se debe filtrar continuamente con una eficacia de detección de polvo atmosférico del 40 % (MERV 9) conforme a la norma ASHRAE 52.2[1]. • El aire que entra en el centro de datos se debe filtrar con una eficacia del 99,97 % o superior, mediante filtros HEPA (filtros de aire de partículas de alta eficacia) que cumplan la norma MIL-STD-282. • La humedad relativa delicuescente de la contaminación por partículas debe ser superior al 60 %[2]. • La sala no debe tener contaminación conductiva, como son los hilos de zinc.
Gaseosa	• Cobre: Clase G1 según ANSI/ISA 71.04-1985[3] • Plata: Tasa de corrosión inferior a 300 Å en 30 días

[1] ASHRAE 52.2-2008: **Método de prueba de los dispositivos de limpieza del aire de ventilación general para la eficacia de la eliminación por tamaño de partícula**. Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.

[2] La humedad relativa delicuescente de contaminación por partículas es la humedad relativa a la que el polvo absorbe agua suficiente para estar húmedo y favorecer la conducción iónica.

[3] ANSI/ISA-71.04-1985. **Condiciones del entorno para sistemas de control y medición del proceso: contaminantes transportados por el aire**. Instrument Society of America, Research Triangle Park, Carolina del Norte, EE. UU.

Declaración sobre la regulación de telecomunicaciones

Este producto puede no estar certificado en su país para la conexión por cualquier medio con interfaces de redes de telecomunicaciones públicas. Es posible que la ley exija una certificación adicional antes de realizar dicha conexión. Póngase en contacto con un representante o revendedor de Lenovo si tiene preguntas.

Avisos de emisiones electrónicas

Cuando fija un monitor al equipo, debe utilizar el cable de monitor asignado y todos los dispositivos de supresión de interferencia que se proveen con él.

Los avisos electrónicos adicionales acerca de las emisiones están disponibles en:

https://pubs.lenovo.com/

Declaración de RoHS de BSMI de Taiwán

單元 Unit	限用物質及其化學符號 Restricted substances and its chemical symbols					
	鉛Lead (Pb)	汞Mercury (Hg)	鎘Cadmium (Cd)	六價鉻 Hexavalent chromium (Cr^{+6})	多溴聯苯 Polybrominated biphenyls (PBB)	多溴二苯醚 Polybrominated diphenyl ethers (PBDE)
機架	○	○	○	○	○	○
外部蓋板	○	○	○	○	○	○
機械組合件	–	○	○	○	○	○
空氣傳動設備	–	○	○	○	○	○
冷卻組合件	–	○	○	○	○	○
內存模塊	–	○	○	○	○	○
處理器模塊	–	○	○	○	○	○
鍵盤	–	○	○	○	○	○
調製解調器	–	○	○	○	○	○
監視器	–	○	○	○	○	○
滑鼠	–	○	○	○	○	○
電纜組合件	–	○	○	○	○	○
電源	–	○	○	○	○	○
儲備設備	–	○	○	○	○	○
電池匣組合件	–	○	○	○	○	○
有mech的電路卡	–	○	○	○	○	○
無mech的電路卡	–	○	○	○	○	○
雷射器	–	○	○	○	○	○

備考1. 〝超出0.1 wt %〞及〝超出0.01 wt %〞係指限用物質之百分比含量超出百分比含量基準值。

Note1 : “exceeding 0.1wt%” and “exceeding 0.01 wt%” indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition.

備考2. 〝○〞係指該項限用物質之百分比含量未超出百分比含量基準值。

Note2 : “○”indicates that the percentage content of the restricted substance does not exceed the percentage of reference value of presence.

備考3. 〝-〞係指該項限用物質為排除項目。

Note3 : The “-“ indicates that the restricted substance corresponds to the exemption.

Información de contacto de importación y exportación de Taiwán

Existen contactos disponibles para la información de importación y exportación para Taiwán.

委製商/進口商名稱: 台灣聯想環球科技股份有限公司
進口商地址: 台北市南港區三重路 66 號 8 樓
進口商電話: 0800-000-702

Índice

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

X

Lenovo

Número de pieza: SP47A30085

Printed in China

(1P) P/N: SP47A30085