Lenovo

Guía del usuario de XClarity Controller 3

Nota: Antes de utilizar esta información, lea la información general incluida en el apartado Apéndice B “Avisos” en la página 185.

Primera edición (Octubre 2024)

Contenido

Capítulo 1. Introducción

Lenovo XClarity Controller 3 (XCC3) es el controlador de gestión de próxima generación para los servidores Lenovo ThinkSystem.

El controlador consolida la funcionalidad del procesador de servicio, súper E/S, el controlador de video y las funciones de presencia remota en un solo chip en la placa del sistema del servidor. Proporciona las siguientes características:

- 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 a 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.

Notas:

- XClarity Controller admite en la actualidad Redfish Scalable Platforms Management API especificación 1.16.0 y esquema 2022.2.
- 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 a XClarity Controller mediante un puerto de red compartido con el sistema operativo del servidor.

Este documento explica cómo utilizar las funciones de XClarity Controller en un servidor ThinkSystem. XClarity Controller trabaja con 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 y Premier de XClarity Controller

Con XClarity Controller, se ofrecen los niveles Estándar y Premier de la funcionalidad XClarity Controller. Consulte la documentación de su servidor para obtener más información acerca del nivel de funcionalidad de 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

Características de nivel estándar de XClarity Controller

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

Interfaces de gestión estándar de la industria

- Interfaz IPMI 2.0
- Redfish
- DCMI 1.5
- SNMPv3

Otras interfaces de gestión

- Web
- SSH CLI
- 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 eventos

- IPMI SEL
- Registro legible humano
- Registro de auditoría
- Miniregistro

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
- Proceso de vigilancia del SO
- Captura de pantalla azul (error de SO, en FFDC)
- Herramientas de diagnóstico integradas
- Llamar a casa

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
- SSL
- SSH
- SMTP
- Cliente LDAP
- NTP
- SSDP
- LLDP

Alertas

- Interrupciones PET
- SNMP v1, v2c t v3 TRAP

- Correo electrónico
- Suscripciones a notificaciones de Redfish

Presencia remota

- Disco remoto en tarjeta (RDOC)

Redirección serie

- IPMI SOL
- Configuración de puerto serie que incluye autoridad y velocidad
- Búfer de consola serie (120 s)

Seguridad

- Procesador no host 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
- NIST SP 800-131a
- Detección de intrusión del chasis (si es compatible con el hardware del servidor)
- Solo protocolos seguros y cifrados habilitados
- Registro de auditoría de cambios de configuración y acciones del servidor
- Autenticación de clave pública (PK)
- Retiro/reasignación del sistema (RTD/ERTD)
- Soporte de PFR
- FIPS 140-3
- Modos de seguridad y panel de seguridad
- Almacenamiento seguro de contraseñas

Gestión de alimentación

- Medidor de alimentación en tiempo real

Features on Demand

- Repositorio de claves de activación

Implementación y configuración

- Configuración remota
- Traspaso del SO
- Paquetes de herramientas y controladores integrados de despliegue y configuración
- Copia de seguridad y restauración de la configuración
- Tamaño extendido del RDOC (con tarjeta MicroSD)
- Perfiles térmicos configurables

Actualizaciones de firmware

- Actualización de agente libre
- Actualización remota

Características del nivel Premier de XClarity Controller

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

Todas las "Características de nivel estándar de XClarity Controller" en la página 2.

Registros de eventos

- Registro de sustitución de componente

RAS

- Captura de arranque
- Captura de video del error

Alertas

- Syslog

Presencia remota

- KVM remoto
- Montaje de imágenes ISO/IMG de cliente local
- Control de calidad/ancho de banda
- Medio virtual de montaje de archivos ISO/IMG remotos http, Samba y NFS

Redirección serie

- Redirección serie sobre SSH-CLI

Seguridad

- Inicio de sesión único
- Security Key Lifecycle Manager (SKLM/KMIP)
- Bloqueo de dirección IP
- Modo de seguridad estricto empresarial (cumplimiento con CNSA)
- Protección del sistema

Gestión de alimentación

- Limitación de alimentación
- Supervisión de rendimiento OOB: métricas de rendimiento del sistema
- Gráficos de alimentación en tiempo real
- Gráficos de temperatura

Implementación y configuración

- Despliegue del SO remoto

Actualizaciones de firmware

- Sincronización con repositorio

- Actualización del paquete de firmware de System Pack
- Reversión del firmware desde el repositorio local en tarjeta MicroSD

Actualización de XClarity Controller

Si el servidor se entregó con el nivel estándar 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 9 “Gestión de licencia” en la página 87.

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 de XClarity Controller requiere uno de los siguientes navegadores web:

- Chrome 64.0 o versiones posteriores (64.0 o versiones posteriores para consola remota)
- Firefox ESR 78.0 o versiones posteriores
- Microsoft Edge 79.0 o versiones posteriores
- Safari 12.0 o versiones posteriores (iOS 7 o versiones posteriores 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 de XClarity Controller. El firmware de XClarity Controller se puede modificar periódicamente para incluir soporte para otros navegadores.

Dependiendo de la versión de firmware de 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 de 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:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_8_SHA256
- TLS_AES_128_CCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305
- 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

Nota: 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 de XClarity Controller, es posible que el navegador continúe utilizando la información de la memoria caché en lugar de recuperarlo de XClarity Controller. Después de actualizar el firmware de 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 XClarity Controller.

De forma predeterminada, el idioma elegido para la interfaz web de 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 de 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 de XClarity Controller, pero que 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 de XClarity Controller.

XClarity Controller combina funciones de procesador de servicios, controlador de video y la función de presencia remota en un único chip. Primero debe iniciar sesión con la interfaz web de XClarity Controller para tener acceso remoto a XClarity Controller. Este capítulo describe los procedimientos de inicio de sesión y las acciones que puede realizar desde la interfaz web de XClarity Controller.

Acceder a la interfaz web de XClarity Controller

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

XClarity Controller admite el direccionamiento IPv4 del protocolo de configuración de host dinámico y estático (DHCP). La dirección estática IPv4 predeterminada asignada a 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 a 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 a 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 de XClarity Controller a través de XClarity Provisioning Manager

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

Después de que se inicie el servidor, puede utilizar XClarity Provisioning Manager para configurar la conexión de red de 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 de XClarity Controller. Para configurar la conexión de red de 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.

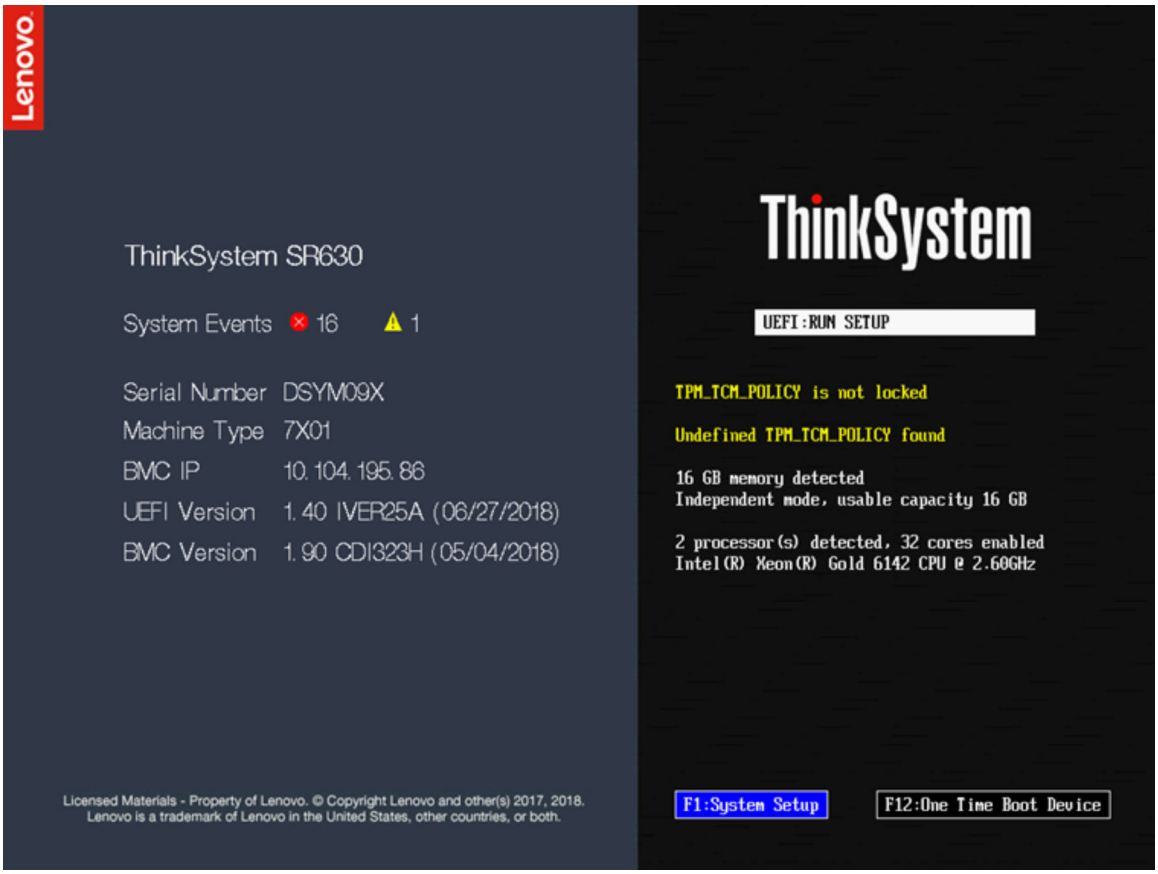


Figura 1. Pantalla de bienvenida de ThinkSystem

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, pulse **Network Settings**.

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

- IP estática

- DHCP habilitado
- DHCP con regreso

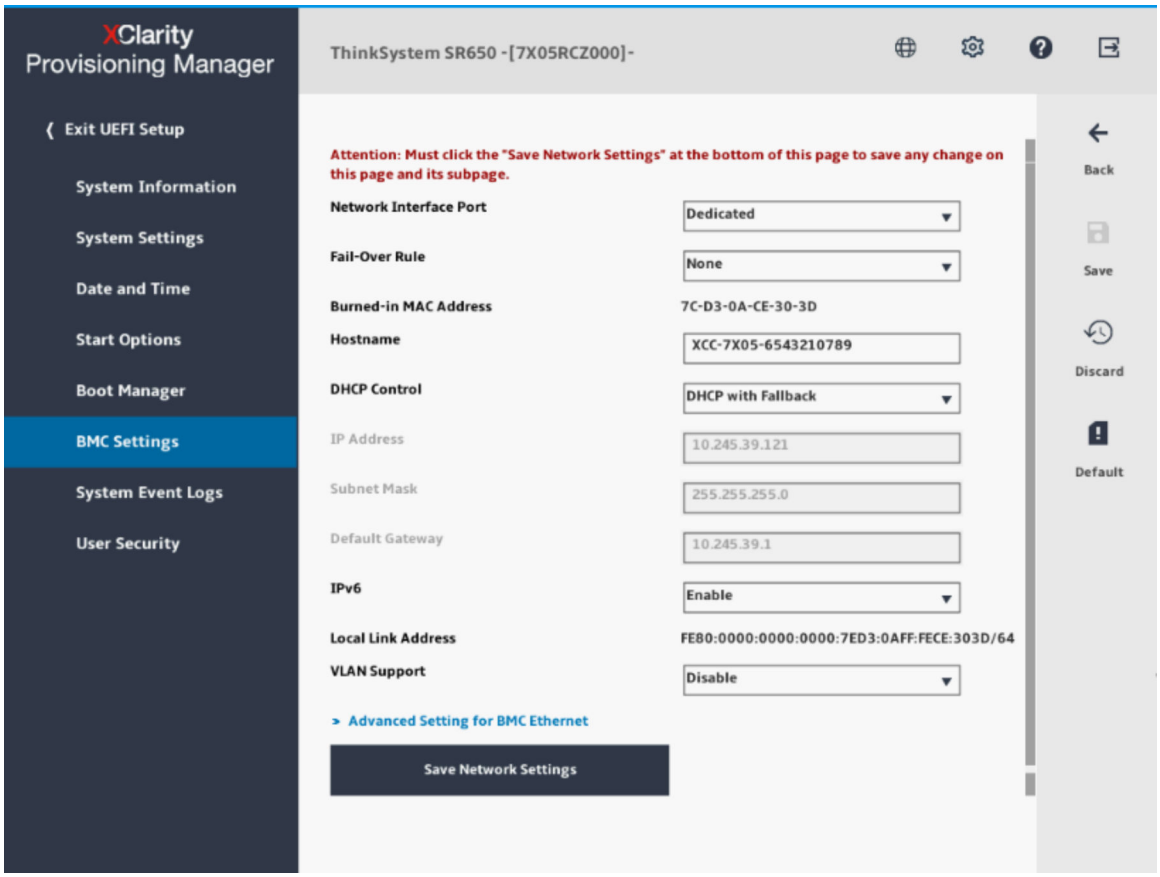


Figura 2. Configuración de conexión de red

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 XClarity Controller, consulte la documentación incluida con el servidor.

Paso 9. Pulse **Guardar**.

Paso 10. Salga de 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 de XClarity Controller a través de la interfaz web o la interfaz de la línea de comandos (CLI) de XClarity Controller. En la interfaz web de 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 XClarity Controller

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

Importante: 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.

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

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

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

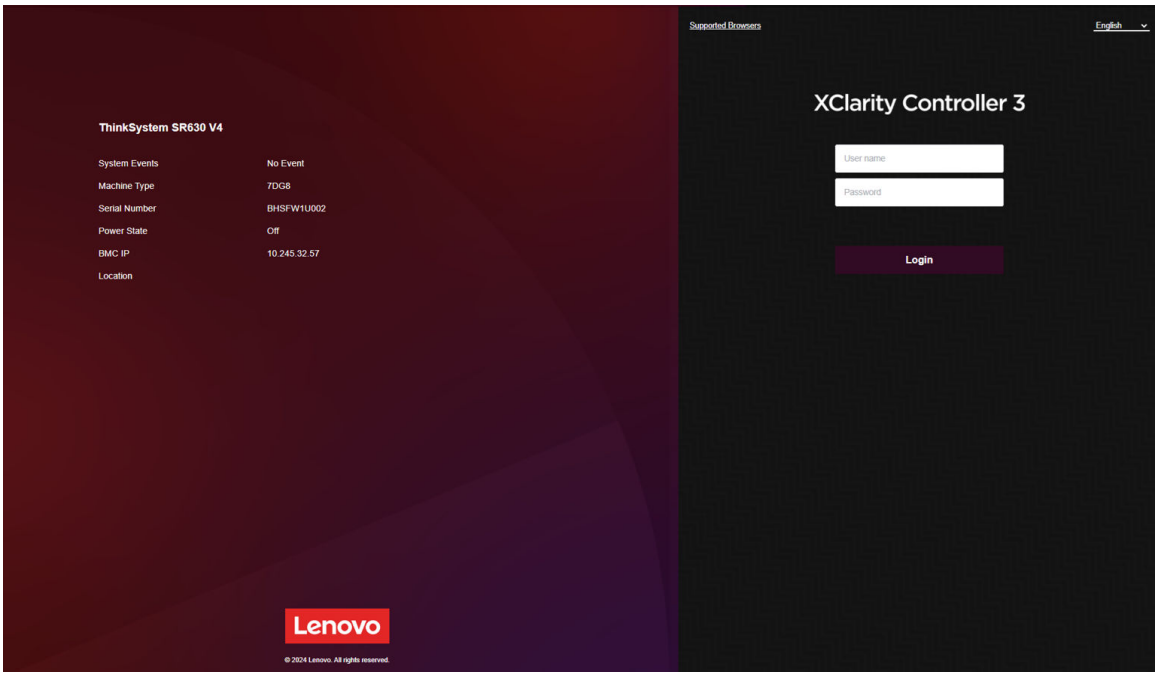


Figura 3. Página de inicio de sesión

Paso 3. Escriba el nombre de usuario y la contraseña en la ventana de inicio de sesión de 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 eventos. 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. Pulse **Iniciar sesión** para iniciar la sesión. El navegador abre la página inicial de XClarity Controller, tal como se muestra en la ilustración siguiente. La página de inicio muestra información sobre el sistema que 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.

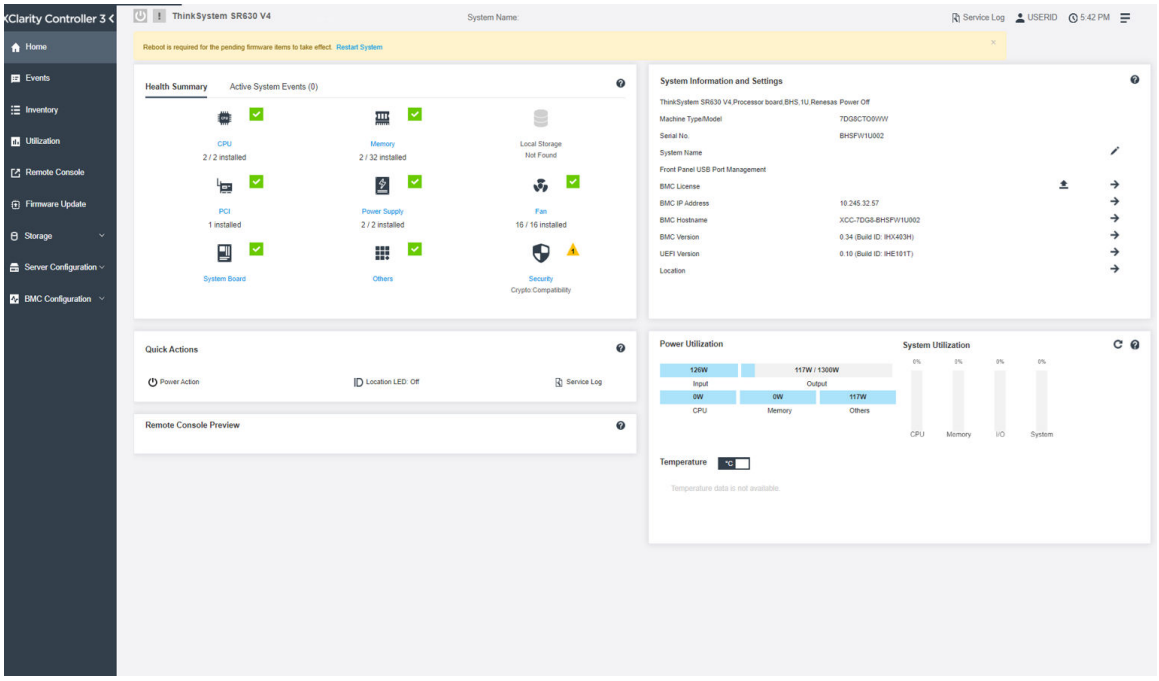


Figura 4. Página de inicio

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 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 información de este tema explica 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.

Pestaña	Selección	Descripción
Inicio	Resumen de estado/eventos activos del sistema	Muestra el estado actual de los componentes de hardware principales del sistema.
	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.
	Consumo de energía	Proporciona una visión general rápida de la utilización de alimentación actual.
	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 de XClarity Controller muestra una imagen un botón de arranque.
Eventos	Registro de eventos	Proporciona un listado histórico de todos los eventos de hardware y de gestión.
	Registro de auditoría	Proporciona un registro histórico de las acciones del usuario.
	Historial de mantenimiento	Muestra todo el historial de actualización de firmware, la configuración y sustitución de hardware.
	Destinatarios de alerta **Nota:** Esta característica se admitirá en una actualización futura.	Gestionar a quién se le notificarán los eventos del sistema. Le permite configurar a cada receptor y gestionar valores que se aplican a todos los destinatarios de eventos. Puede también generar un evento 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 SMM3 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 e información de la velocidad del ventilador del servidor y sus componentes en formatos gráficos o tabulares.
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 o DVD ROM que está conectada al servidor.
Actualización de firmware		• Muestra los niveles de firmware. • Actualiza el firmware de XClarity Controller y el firmware del servidor. • Actualización del firmware de XClarity Controller desde el repositorio.
Almacenamiento	Detalle	Muestra la estructura física de los dispositivos de almacenamiento y la configuración de almacenamiento.

Pestaña	Selección	Descripción
	Configuración de RAID	Vea o modifique la configuración RAID actual, incluyendo información de los discos virtuales y dispositivos de almacenamiento físicos.
Configuración del servidor	Adaptadores	Muestra la información de adaptadores de red instalados y los valores que se pueden configurar mediante 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.
	Directiva de alimentación	• Configure la redundancia de alimentación durante el evento de un error de fuente de alimentación. • Configure la directiva de limitación de alimentación. • Configure la directiva de restauración de alimentación. **Nota:** Consulte la interfaz web de SMM3 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 retrasos de apagado 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 XClarity Controller.
	Chasis **Nota:** Este elemento solo está disponible en los nodos compatibles con el chasis D3 V2.	• Muestra la información del chasis. • Reinicia el nodo o simula una reubicación física del nodo. • Muestra las preferencias de selección del encargado del chasis. • Muestra el historial de mantenimiento del chasis.
Configuración BMC	Copia de seguridad y restauración	Restablezca la configuración de 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 de XClarity Controller.
	Red	Configure las propiedades, estado y los valores de red para XClarity Controller.
	Seguridad	Configure las propiedades, estado y los valores de seguridad para XClarity Controller.
	Usuario/LDAP	• Configure los perfiles de inicio de sesión de XClarity Controller y la configuración de inicio de sesión global. • Vea las cuentas de usuario que se registran actualmente a 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.

Pestaña	Selección	Descripción
	Llamar a casa **Nota:** Esta característica se admitirá en una actualización futura.	Configure la opción Llamar a casa para recopilar información acerca del sistema y enviarla a Lenovo para servicios.

Capítulo 3. Configuración de XClarity Controller

Utilice la información de este capítulo para comprender las opciones disponibles para las configuraciones de 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 a 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 XClarity Controller puede utilizar para autenticar los intentos de inicio de sesión.

Pulse el menú desplegable junto a **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 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 de 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 un rol nuevo

Utilice la información en este tema para crear un rol nuevo.

Crear rol

Pulse la pestaña **Roles** y pulse **Crear** para crear un rol personalizado.

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

El rol creado se proporciona al usuario en el menú desplegable de roles de la sección de usuario.

Nota: El rol utilizado en el Usuario y LDAP no tiene permiso para editar y eliminar el nombre del rol, pero tiene acceso a modificar el permiso personalizado correspondiente.

Nivel de autoridad

Un rol personalizado puede habilitar cualquier combinación de los privilegios siguientes:

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

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: básico
Un usuario puede modificar los parámetros de configuración en las páginas de Propiedades del servidor y Eventos.

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

Configuración: avanzado (actualización de firmware, reiniciar el BMC, restaurar la configuración)
Un usuario no tiene restricciones al configurar XClarity Controller. Además, el usuario tiene acceso administrativo a XClarity Controller. El acceso administrativo incluye las siguientes funciones avanzadas: actualizaciones de firmware, arranque de la red PXE, restaurar XClarity Controller a los valores de fábrica, modificar y restaurar la configuración de XClarity Controller desde un archivo de configuración y reiniciar o restablecer XClarity Controller.

Configuración: seguridad de UEFI
Un usuario puede modificar la configuración de seguridad de UEFI.

Roles predefinidos

Los roles siguientes están predefinidos y no se pueden editar ni eliminar:

Administrador
El rol de administrador no tiene restricciones y puede realizar todas las operaciones.

Solo lectura
El rol de solo lectura puede mostrar información del servidor, pero no puede realizar la operación que afecta al estado del sistema, como guardar, modificar, borrar, rearrancar y actualizar firmware.

Operador
El usuario con rol Operador tiene los siguientes privilegios:

- Configuración: seguridad de redes y BMC
- Alimentación de servidor remoto/Reiniciar
- Configuración: básico
- Capacidad de borrar registros de eventos
- Configuración: avanzado (actualización de firmware, reiniciar el BMC, restaurar la configuración)

Creación de una nueva cuenta de usuario

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

Crear usuario

Pulse la pestaña **usuarios locales** y pulse **Crear** para crear una nueva cuenta de usuario.

Complete los campos siguientes: **Nombre de usuario**, **Contraseña**, **Confirmar contraseña** y seleccione un **rol** en el menú desplegable. Para conocer más detalles sobre el **rol**, consulte la sección siguiente.

Rol

Los roles siguientes están predefinidos mientras que el nuevo rol personalizado puede crearse de acuerdo con las necesidades del usuario:

Administrador
El rol de administrador no tiene restricciones y puede realizar todas las operaciones.

Solo lectura
El rol de solo lectura puede mostrar información del servidor, pero no puede realizar la operación que afecta al estado del sistema, como guardar, modificar, borrar, rearrancar y actualizar firmware.

Operador
El usuario con rol Operador tiene los siguientes privilegios:

- Configuración: seguridad de redes y BMC
- Alimentación de servidor remoto/Reiniciar
- Configuración: básico
- Capacidad de borrar registros de eventos
- Configuración: avanzado (actualización de firmware, reiniciar el BMC, restaurar la configuración)

Configuración de SNMPv3

Para habilitar acceso a SNMPv3 para un usuario, pulse el botón **Editar** que está junto al usuario correspondiente y, luego, seleccione **SNMP** en la lista desplegable de la opción **Interfaz accesible de usuario**. 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.

Protocolo de autenticación
El modelo de seguridad SNMPv3 utiliza este algoritmo para la autenticación. Se admiten los siguientes protocolos:

- Ninguno
- HMAC-SHA (predeterminado)
- HMAC-SHA224
- HMAC-SHA256
- HMAC-SHA384
- HMAC-SHA512

Protocolo de privacidad
La transferencia de datos entre el cliente de SNMP y el agente se puede proteger mediante cifrado. Se admiten los siguientes métodos:

- Ninguno
- CBC-DES
- AES (predeterminado)
- AES192
- AES256
- AES192C
- AES256C

Notas: Incluso si un usuario de SNMPv3 usa cadenas repetitivas de una contraseña, aún se permitirá el acceso a 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 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 a XClarity Controller si la contraseña se ingresa accidentalmente como "**bertbertbert**". Se considerará que ambas contraseñas tienen la misma clave.

Para obtener más detalles, consulte **Consideraciones de seguridad** 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 la cuenta de usuario local, pulse el botón **Editar** junto al usuario correspondiente, luego marque **Clave SSH** en la lista desplegable de **Interfaz accesible de usuario**. Se proporcionan las siguientes dos opciones:

Seleccionar archivo de clave
Seleccione el archivo de clave SSH para importar a 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 a 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 a XClarity Controller en la interfaz Ethernet sobre USB interna y solo para las interfaces Redfish 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, 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, a menos que sea la única cuenta restante con privilegios de **gestión de cuentas de usuario**.

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, 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. 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

Pulse **Seguridad** en **Configuración del BMC** y desplácese hasta la sección **Security Password Manager** para habilitar o deshabilitar la función de **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**, pulse **Usuario/LDAP** en **Configuración del 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** estarán 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 característica

  ```
  $ 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 característica

  ```
  > 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 de 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 de XClarity Controller que se actualiza automáticamente, su sesión web no se apagará automáticamente debido a la inactividad.

Configuración de la directiva de seguridad de la cuenta

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

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 dice hacer la casilla de verificación habilitar.

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 255 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 255 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.

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.

Longitud mínima de la contraseña (caracteres)

Este campo contiene la longitud mínima de contraseña.

Ciclo mínimo de reutilización de la contraseña (veces)
Este campo contiene el número de contraseñas anteriores que no se pueden reutilizar.

Intervalo mínimo de cambio de contraseña (horas)
Este campo contiene cuánto tiempo debe esperar un usuario entre los cambios de contraseña.

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.

Periodo de bloqueo tras superar el número máximo de errores de inicio de sesión (minutos)
Este campo especifica cuánto tiempo (en minutos), el subsistema de 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.

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 (Windows 2003, Windows 2008)
- Servicio Microsoft Lightweight Directory (Windows 2008, Windows 2012, Windows 2016, Windows 2019)
- Novell eDirectory Server, versión 8.7 y 8.8
- Servidor OpenLDAP 2.1, 2.2, 2.3, 2.4, 2.5 y 2.6

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. Se pueden designar privilegios para cada cuenta de usuario utilizando el valor de “Atributo de permiso de inicio de sesión”. 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 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 a XClarity Controller utilizar las credenciales únicamente para autenticar con el servidor LDAP y para recuperar información de membresía de grupo. Los nombre y roles de grupo se pueden configurar en la sección **Grupos para autorización local**.

- **Usar el servidor LDAP para autenticación y autorización**: esta selección indica a 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 tres servidores LDAP ingresando la dirección IP o el nombre de host de cada servidor si DNS está 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 “Manejo de certificados SSL” en la página 43.

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

Tipo de LDAP

Seleccione el tipo de servidor LDAP para la autenticación basada en LDAP. Están disponibles los siguientes tipos de servidor:

- **OpenLDAP**

  OpenLDAP
- **Active Directory**

  Directorio: Windows Active Directory
- **Otros**

  Directorio: Apache Directory, eDirectory, etc.

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:

- **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 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 la vinculación inicial se completa correctamente, se realiza una búsqueda para buscar una entrada en el servidor LDAP que pertenezca al usuario que inicia la sesión. De ser necesario, se realiza un segundo intento de vinculación, esta vez con el nombre distinguido recuperado del registro LDAP del usuario y la contraseña ingresada durante el proceso de inicio de sesión. Si falla un segundo intento de vinculación, se rechaza el acceso al usuario. La segunda vinculación solo se realiza cuando se utilizan los métodos de vinculación de **Usar credenciales configuradas**.

Nombre distinguido del cliente

Nombre distintivo de cliente (DN) que se va a usar para la vinculación inicial. Y está limitado a un máximo de 300 caracteres.

Contraseña del cliente

La contraseña de este cliente 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 del nombre de inicio de sesión del usuario

Cuando el método de vinculación está configurado como **Credenciales configuradas por el usuario**, una solicitud de búsqueda sigue el vínculo 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 **CN** o **sAMAccountName**. En los servidores Novell eDirectory y OpenLDAP, el nombre del atributo es uid. Si se deja en blanco este campo, el valor predeterminado es **sAMAccountName**.

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.

Atributo de búsqueda de pertenencia a grupo

El campo **Atributo de búsqueda de grupos** especifica el nombre del atributo que se utiliza para identificar los grupos a los que pertenece el usuario. En los servidores de Active Directory, el nombre de atributo generalmente es **memberOf**. En los servidores Novell eDirectory, el nombre del atributo es **groupMembership**. En los servidores OpenLDAP, los usuarios suelen asignarse a grupos cuya objectClass es igual 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 del atributo. Si se usa el servidor LDAP para la autenticación y la autorización, pero este campo se deja en blanco, el usuario no tendrá acceso.

El valor del atributo devuelto por las búsquedas del servidor LDAP debe ser una cadena de bits que se introduce como 13 números 0 o 1 consecutivos, o una cadena de bits como 13 números 0 o 1 consecutivos en total. 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 más a la derecha es la posición de bit 12. Un valor de 1 en una posición de bit habilita la función asociada a esa posición de bit. Un valor de 0 en una posición de bit deshabilita la función asociada a esa posición de bit.

La cadena 0100000000000 es un ejemplo válido, que se utiliza para permitir que se coloque en cualquier 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 1. 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.

Tabla 1. Bits de permiso (continuación)

Posición de bit	Función	Explicación
3	Configuración: seguridad de redes y BMC	Un usuario puede modificar la configuración en Seguridad, Protocolos de red, Interfaz de red, Asignaciones de puertos y Puerto de serie.
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: básico	Un usuario puede modificar los parámetros de configuración en las ventanas de configuración del sistema y alertas.
9	Capacidad de borrar registros de eventos	Un usuario puede borrar los registros de eventos. **Nota:** Todos los usuarios pueden ver los registros de eventos; pero para borrar los registros de eventos se pedirá al usuario tener este nivel de permiso.
10	Configuración: avanzado (actualización de firmware, reiniciar el BMC, restaurar la configuración)	Un usuario no tiene restricciones al configurar XClarity Controller. Además, el usuario tiene acceso administrativo a XClarity Controller. El usuario puede realizar las siguientes funciones avanzadas: actualizaciones de firmware, arranque de red PXE, restauración de los valores predeterminados de fábrica del adaptador, modificación y restauración de la configuración del adaptador desde un archivo de configuración y reinicio/restablecimiento del adaptador.
11	Configuración: seguridad de UEFI	Un usuario puede configurar valores relacionados con la seguridad de UEFI, que también se pueden configurar desde la página de configuración de seguridad F1 de UEFI.
12	Reservado	Reservado para uso futuro y actualmente ignorado.

Si no se establece ninguno de los bits, se denegará el acceso al usuario

Nota: 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.

Importante: 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 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. Si se utiliza el modo **Usar el servidor LDAP únicamente para autenticación (con autorización local)**, configure **Grupos para autorización local**. El nombre de grupo, el dominio de grupo y el rol están configurados para proporcionar autorización local a grupos de usuarios. A cada grupo se le puede

asignar un rol (permisos) que es el mismo que se configuró en los roles en Usuario local. Las cuentas de usuario se asignan a diferentes grupos en el servidor LDAP. Se asignará una cuenta de usuario con el rol (permisos) del grupo al que pertenece esta cuenta de usuario después de iniciar sesión en el BMC. El dominio de grupo debe tener el mismo formato que el nombre distinguido, como: dc=miempresa, dc=com, se utilizará como objeto base para las búsquedas de grupo. Si el campo se deja en blanco, utilizará el mismo valor que el campo “DN raíz”. Se pueden agregar grupos adicionales pulsando en el icono “+” o eliminarlos pulsando en el icono “x”.

4. Seleccione el atributo utilizado para mostrar el nombre de usuario en el menú desplegable **Especificar el atributo utilizado para mostrar el nombre de usuario**.

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 XClarity Controller se comunica por una conexión Ethernet.

Nota: Los servidores AMD no admiten la función de conmutación por error Ethernet.

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 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 XClarity Controller. Se recomienda que, cuando se utiliza DHCP, los usuarios deben utilizar el nombre de host para acceder a 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 a XClarity Controller cuando caduque la concesión de DHCP, o cuando se reinicia XClarity Controller. Si un usuario necesita acceder a XClarity Controller utilizando una dirección IP que no se cambia, debe configurarse XClarity Controller para una dirección IP estática en lugar de DHCP.

Pulse **Red** en **Configuración del BMC** para modificar los valores de Ethernet de 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: Esta configuración no afecta a la interfaz LAN USB ni al puerto de gestión USB situado 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 a 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 IPv4** escriba la dirección IP que desea asignar a 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.

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.

En la **lista de direcciones MAC**, elija una de las siguientes opciones:

- **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 `00000000000` 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 **Velocidad de datos y dúplex**, seleccione **negociar automáticamente** o **personalizar** para especificar la velocidad de datos y dúplex.

En el campo **MTU (unidad de transmisión máxima)**, especifique el tamaño máximo de un paquete (en bytes) para la interfaz de red. El rango máximo de la unidad de transmisión es de 1000 a 1500. El valor predeterminado para este campo es 1500.

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.

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

Si pulsa la casilla de verificación **Usar DNS para detectar Lenovo XClarity Administrator**, se debe seleccionar XClarity Manager.

Configuración de DDNS

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

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

Pulse la casilla de verificación **Habilitar DDNS** para habilitar DDNS. Cuando se habilita el DDNS, 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 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 de XClarity Controller se seleccione.

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

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

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

Importante:

- Si deshabilita **Ethernet sobre USB**, no podrá realizar una actualización en banda del firmware de XClarity Controller o del firmware del servidor mediante la utilidad de actualización en banda de XClarity Essentials. Utilice la opción de actualización de firmware en la interfaz web de XClarity Controller o la utilidad de actualización fuera de banda de XClarity Essentials para actualizar el firmware.
- Es importante deshabilitar los tiempos de espera del proceso de vigilancia para impedir que el servidor se reinicie inesperadamente cuando la interfaz USB en banda esté deshabilitada.
- Para utilizar esta interfaz, se deben instalar los controladores del sistema operativo que admiten esta función (RNDIS para Windows, cdc_ether y usbnet para Linux). XClarity Controller proporciona un archivo INF para Windows que permite a Windows reconocer el dispositivo USB de XClarity Controller como un dispositivo RNDIS.

Seleccione el método que 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 de XClarity Controller está configurado para utilizar la modalidad de dirección local de enlace IPv6, varias funciones que utilizan esta interfaz no funcionarán porque 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
  ```
- **Configurar IPv4 para Ethernet sobre USB**: Con este método, especifica las direcciones IP y máscara de red que se asignan a XClarity Controller y al extremo del servidor de la interfaz de Ethernet sobre USB.

  Notas:

  – Debe configurar manualmente la dirección IP de la interfaz Ethernet sobre USB en el sistema operativo local después de configurar la dirección IP de XClarity Controller, la dirección IP del SO y la máscara de red.

  – La configuración de la dirección IP del SO se utiliza para que XClarity Controller conozca el extremo opuesto de la red Ethernet sobre USB (sistema operativo) para fines de comunicación, como la supervisión del estado del proceso de vigilancia o la actualización de firmware en banda.

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 de XClarity Controller.

1. Pulse **Red** en **Configuración del BMC**.
2. Marque la casilla de verificación correspondiente para habilitar el **Agente SNMPv3**, la **Captura SNMPv1**, la **Captura SNMPv2** o la **Captura SNMPv3**.

   Notas:

   - Para habilitar el **Agente SNMPv3**, se debe especificar un contacto y una ubicación del BMC.
   - Una vez habilitado el **Agente SNMPv3**, puede configurar SNMPv3 para cada cuenta de usuario de XClarity Controller.
   - Para recibir capturas, tanto las capturas SNMP como el agente SNMPv3 deben estar habilitados
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 de la comunidad 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 eventos para los que desea recibir alertas:

   - **Crítico**
   - **Atención**
   - **Sistema**

   Nota: Pulse cada categoría importante para seleccionar mejor los tipos de eventos de subcategoría en los que desea recibir la alerta.
6. Si habilita el **Agente SNMPv3**, complete la siguiente información:
   a. Pulse **Usuario/LDAP** en **Configuración del BMC**.
   b. Pulse el botón **Editar** que está junto al usuario correspondiente y, luego, seleccione **SNMP** en la lista desplegable de la opción **Interfaz accesible de usuario**.

Nota: Pulse el botón **Enviar** junto a **Enviar una captura de prueba** para verificar la configuración de SNMP.

Habilitación del acceso de red IPMI

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

Siga estos pasos para habilitar el acceso de IPMI sobre LAN.

1. Pulse **Red** en **Configuración del BMC** para ver o modificar los valores de IPMI de XClarity Controller.
2. Pulse el conmutador **IPMI sobre LAN** en **Habilitación del servicio y asignación de puertos** para habilitar el acceso de red IPMI a XClarity Controller.
3. Pulse **Usuario/LDAP** en **Configuración del BMC**.
4. Pulse el botón **Editar** que está junto al usuario correspondiente y, luego, seleccione **IPMI sobre LAN** en la lista desplegable de la opción **Interfaz accesible de usuario**.

Importante:

- Si no está usando herramientas o aplicaciones que tienen acceso a 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 XClarity Controller.

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

HTTPS (Web/Redfish)
Este elemento siempre está habilitado. En este campo especifique el número de puerto para la web sobre HTTPS. El valor predeterminado es 443.

Presencia remota
Este elemento siempre está habilitado. El número de puerto es 443.

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

Nota: Asegúrese de que **IPMI sobre LAN** esté seleccionado y aplicado en el campo **Interfaz accesible de usuario** para el usuario correspondiente en la página Usuario/LDAP.

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 XClarity Controller. El valor predeterminado es 161. Los valores válidos del número de puerto son de 1 a 65535.

Nota: Asegúrese de que **SNMP** esté seleccionado y aplicado en el campo **Interfaz accesible de usuario** para el usuario correspondiente en la página Usuario/LDAP.

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 de XClarity Controller.

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

La conexión a 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.

En algunos servidores, el puerto USB del panel frontal se puede conmutar para que esté conectado al servidor o a XClarity Controller.

Nota: Esta característica se admitirá en una actualización futura.

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 135.

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

Panel de seguridad

En este tema se proporciona una visión general del panel de seguridad.

El panel de seguridad proporciona una evaluación general de la seguridad y el estado del sistema.

- **Eventos de seguridad del BMC** informa los eventos provocados por problemas de seguridad, como la intrusión en el chasis, la corrupción detectada en el PFR, la incoherencia de hardware detectada por la protección del sistema, el puente de seguridad abierto en la placa, etc.
- **Modo de seguridad del BMC** proporciona un estado general del cumplimiento del modo de seguridad.
- **Servicios y puertos del BMC** enumera todos los servicios/puertos no seguros habilitados, pero que no cumplen con el modo de seguridad actual.
- **Certificados del BMC** enumera todos los certificados no conformes utilizados por XCC.
- **Cuentas de usuario del BMC** proporciona sugerencias generales sobre cómo hacer más segura la gestión de cuentas y contraseñas.

Nota: El panel muestra un icono de advertencia si hay riesgo en estas áreas de seguridad a través de XCC. El enlace **Detalles** bajo cada categoría también lleva al usuario a la página de configuración para resolver los problemas.

Modo de seguridad

En este tema se proporciona una visión general del modo de seguridad.

La licencia Estándar de XCC permite a los usuarios configurar sus servidores en uno de los dos modos de seguridad: modo estándar y modo de compatibilidad. Estos están disponibles en todos los servidores V4.

La licencia de actualización Lenovo XClarity Controller 3 Premier viene con un tercer modo de seguridad: el modo estricto empresarial. Este modo es el más adecuado para los requisitos de seguridad de alto nivel.

Nota: De forma predeterminada, XCC utiliza un certificado autofirmado de ECDSA y solo están disponibles los algoritmos basados en ECDSA. Para utilizar un certificado basado en RSA, genere una CSR y fírmela con una CA interna o externa. Luego, importe el certificado firmado a XCC.

Modo de seguridad estricto empresarial

- El modo de seguridad estricto empresarial es el modo más seguro.
- Todos los algoritmos criptográficos utilizados por BMC cumplen con CNSA 1.0.
- BMC funciona en el modo FIPS 140-3 validado.
- Requiere certificados de grado estricto de empresa.
- Solo se pueden habilitar los servicios que admiten la criptografía CNSA 1.0.
- Requiere la habilitación de la clave de característica bajo demanda.

Modo de seguridad estándar

- El modo estándar es el modo de seguridad predeterminado.
- Todos los algoritmos criptográficos utilizados por BMC cumplen con FIPS 140-3.
- BMC funciona en modo validado por FIPS 140-3 cuando todos los servicios habilitados utilizan criptografía compatible con FIPS 140-3.
- Requiere certificados de grado estándar.
- Los servicios que requieren criptografía que no admite criptografía compatible con FIPS 140-3 están deshabilitados de forma predeterminada.

Modo de compatibilidad

- El Modo de compatibilidad es el modo que se debe utilizar cuando los servicios y los clientes requieren una criptografía que no sea compatible con el modo estricto empresarial/estándar.
- Se admite una gama más amplia de algoritmos criptográficos.
- Cuando este modo está habilitado, BMC **NO** está funcionando en el modo validado estándar.
- Permite habilitar todos los servicios.

Suites de cifrado TLS admitidas

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

Suites de cifrado TLS	Modo de seguridad	Versión de TLS
TLS_AES_256_GCM_SHA384	• Modo de seguridad estricto empresarial • Estándar* • Compatibilidad*	TLS 1.3
TLS_CHACHA20_POLY1305_SHA256	• Compatibilidad	TLS 1.3

Suites de cifrado TLS	Modo de seguridad	Versión de TLS
TLS_AES_128_GCM_SHA256	• Estándar • Compatibilidad	TLS 1.3
TLS_AES_128_CCM_SHA256	• Estándar • Compatibilidad	TLS 1.3
TLS_AES_128_CCM_8_SHA256	• Estándar • Compatibilidad	TLS 1.3
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	• Modo de seguridad estricto empresarial • Estándar* • Compatibilidad*	TLS 1.2
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	• Modo de seguridad estricto empresarial • Compatibilidad*	TLS 1.2
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	• Modo de seguridad estricto empresarial	TLS 1.2
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	• Estándar • Compatibilidad	TLS 1.2
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	• Estándar • Compatibilidad	TLS 1.2
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	• Estándar • Compatibilidad	TLS 1.2
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305	• Compatibilidad	TLS 1.2
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305	• Compatibilidad	TLS 1.2
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	• Estándar • Compatibilidad	TLS 1.2
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	• Estándar • Compatibilidad	TLS 1.2
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	• Estándar • Compatibilidad	TLS 1.2
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	• Estándar • Compatibilidad	TLS 1.2
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	• Estándar • Compatibilidad	TLS 1.2

Suites de cifrado TLS	Modo de seguridad	Versión de TLS
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_ SHA256	• Estándar • Compatibilidad	TLS 1.2
TLS_RSA_WITH_AES_256_GCM_SHA384	• Estándar • Compatibilidad	TLS 1.2
TLS_RSA_WITH_AES_128_GCM_SHA256	• Estándar • Compatibilidad	TLS 1.2
TLS_DHE_RSA_LATH_AES_256_GCM_SHA384	• Estándar	TLS 1.2
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA3U	• Estándar	TLS 1.2
TLS_RSA_WITH_AES_256_CBC_SHA256	• Estándar	TLS 1.2
TLS_RSA_WITH_AES_128_CBC_SHA256	• Estándar	TLS 1.2

Nota: Los modos de seguridad de la tabla que presentan un asterisco (*) requieren la licencia de actualización Lenovo XClarity Controller 3 Premier.

Matriz de servicio en tres modos de seguridad

Característica/ servicio	Utiliza criptografía	Estado predeterminado de fábrica	Se admite en modo estricto	Se admite en el modo estándar	Se admite en el modo de compatibilidad
IPMI sobre KCS	No	Habilitado	Sí	Sí	Sí
IPMI sobre LAN	Sí	Deshabilitado	No	Sí	Sí
Trampas SNMPv1	No	Sin configurar	No	Sí	Sí
Trampas SNMPv3	Sí	Sin configurar	No	Sí Si está habilitado, alertará del uso de criptografía no FIPS	Sí
Agente de SNMPv3	Sí	Sin configurar	No	Sí Si está habilitado, alertará del uso de criptografía no FIPS	Sí
Alertas por correo electrónico	Sí	Sin configurar	Sí No se puede habilitar con la autenticación CRAM-MD5	Sí Si CRAM-MD5 es necesario, alertará del uso de criptografía no FIPS.	Sí
Alertas de Syslog	No	Sin configurar	No	Sí	Sí

Característica/ servicio	Utiliza cripto-grafía	Estado predeter-minado de fábrica	Se admite en modo estricto	Se admite en el modo estándar	Se admite en el modo de compatibilidad
TLS 1.2	Sí	Habilitado	Sí	Sí	Sí
TLS 1.3	Sí	Habilitado	Sí	Sí	Sí
Web sobre HTTPS	Sí	Habilitado	Sí	Sí	Sí
Redfish sobre HTTPS	Sí	Habilitado	Sí	Sí	Sí
SSDP	No	Habilitado	Sí	Sí	Sí
SSH-CLI	Sí	Habilitado	Sí	Sí	Sí
SFTP	Sí	Deshabili-tado	Sí	Sí	Sí
LDAP	No	Sin configurar	No	Sí	Sí
LDAP seguro	Sí	Sin configurar	Sí	Sí	Sí
Gestión de claves de seguridad	Sí	Sin configurar	Sí	Sí	Sí
Puerto remoto	Sí	Habilitado	Sí	Sí	Sí
Medio virtual - CIFS	Sí	Sin configurar	No	Sí	Sí
Medio virtual - NFS	No	Sin configurar	No	Sí	Sí
Medio virtual - HTTPFS	Sí	Sin configurar	Sí	Sí	Sí
RDOC - Local	Sí	Sin configurar	Sí	Sí	Sí
RDOC - CIFS	Sí	Sin configurar	No	Sí	Sí
RDOC - HTTP	No	Sin configurar	No	Sí	Sí
RDOC - HTTPS	Sí	Sin configurar	Sí	Sí	Sí
RDOC - FTP	No	Sin configurar	No	Sí	Sí
RDOC - SFTP	Sí	Sin configurar	Sí	Sí	Sí
Carga de FFDC (SFTP)	Sí	Habilitado	Sí	Sí	Sí
Carga de FFDC (TFTP)	No	Habilitado	No	Sí	Sí

Característica/ servicio	Utiliza cripto-grafía	Estado predeter-minado de fábrica	Se admite en modo estricto	Se admite en el modo estándar	Se admite en el modo de compatibilidad
Actualizar desde el repositorio – CIFS	Sí	Sin configurar	No	Sí	Sí
Actualizar desde el repositorio - NFS	No	Sin configurar	No	Sí	Sí
Actualizar desde el repositorio – HTTP	No	Sin configurar	No	Sí	Sí
Actualizar desde el repositorio – HTTPS	Sí	Sin configurar	Sí	Sí	Sí
Llamar a casa	Sí	Deshabili-tado	Sí	Sí	Sí
Contraseña de terceros	Sí	Sin configurar	No	Sí	Sí
Reenvío de puerto	N/A	Deshabili-tado	Sí	Sí	Sí

Conmutación del modo de seguridad

Utilice la información de este tema para cambiar y validar el modo de seguridad.

El modo estándar es el modo de seguridad predeterminado.

En general, si XCC detecta algún ajuste no conforme con el modo estándar, mostrará una notificación, pero no exigirá al usuario que cambie el modo. En este caso, XCC entrará en modo de seguridad Estándar con sustitución (incumplimiento).

El usuario puede abrir el menú desplegable para seleccionar un modo diferente y utilizar la función **Validar** para determinar cuántos elementos no conformes detecta XCC.

Cuando el usuario pulse **Aplicar**, XCC también validará los elementos conformes.

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.

Manejo de certificados SSL

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

El cliente WEB, Redfish y LDAP utilizan la misma configuración de certificado. La conexión SSL debe restablecerse cada vez que desee cambiar la configuración del certificado SSL. SSL se puede utilizar con un certificado autofirmado o con un certificado firmado por una autoridad de certificación de terceros. El uso de un certificado autofirmado es el método más sencillo para usar SSL, pero a costa de un pequeño riesgo de seguridad. El riesgo surge porque el cliente SSL no tiene forma de validar la identidad del servidor SSL para el primer intento de conexión entre el cliente y el servidor. Es posible que un tercero malintencionado se haga pasar por el servidor e intercepte los datos que fluyen entre XClarity Controller y el navegador. Si (en el momento de la conexión inicial entre el navegador y 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). Después de utilizar la página Gestión de certificados SSL para generar un par de claves y un certificado autofirmado, es posible que SSL esté habilitado.

Para una seguridad más completa, utilice un certificado firmado por una entidad de certificación (CA). Para obtener un certificado firmado:

- Seleccione **Generar CSR (solicitud de firma de certificado)** en el icono **Generar** que se encuentra en **Gestión de certificados SSL**.
- Rellene los campos obligatorios y seleccione **Generar**.
- Después de generar un certificado autofirmado, se mostrará en **Gestión de certificados SSL**.
- Seleccione **Descargar solicitud de firma de certificado (CSR)** en el icono **Descargar** para descargar el certificado firmado.
- Cuando se descargue el certificado firmado, seleccione el ícono **Importar certificado firmado** en **Gestión de certificados CA** para importarlo en XClarity Controller.

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

Tenga en cuenta que SSL compara el nombre de host (o nombre común) de XClarity Controller en el certificado con el nombre de host, tal como lo ve en su navegador web.

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 del BMC** para configurar la gestión de certificados SSL.

Al gestionar los certificados de 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 utilizando una herramienta de terceros como OpenSSL (http://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 del 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 **Generar clave** en **Servidor SSH**.
- Después de completar la acción, debe reiniciar 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) a XClarity Controller.

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

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

Notas:

- Después de cambiar los valores, debe reiniciar XClarity Controller para que los cambios entren en vigor.
- **Deshabilitado (habilitar bajo demanda)** deshabilitará el canal KCS la mayor parte del tiempo, pero permitirá que algunas herramientas de Lenovo intercambien información con XClarity Controller durante

la ventana de actualización de firmware del sistema. Cuando eso sucede, el canal KCS se habilita brevemente durante unos minutos y luego se deshabilita al finalizar o cuando se agota el tiempo de espera.

Importante: Si no está ejecutando herramientas o aplicaciones en el servidor que tiene acceso a 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 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 del BMC** para habilitar o deshabilitar **Evitar firmware del sistema de nivel inferior**.

Cualquier cambio que se realice surtirá efecto inmediatamente sin la necesidad de reiniciar XClarity Controller.

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).

Nota: Esta característica se admitirá en una actualización futura.

Security password manager

Utilice la información de este tema para habilitar la contraseña de terceros.

Esta función permite al usuario decidir si permite o no el uso de contraseñas de terceros.

- **Contraseña de terceros**: una vez habilitada, el BMC podrá usar un hash de contraseña proporcionado por el usuario para la autenticación.
- **Permitir recuperación de contraseña de terceros**: el usuario también puede habilitar o deshabilitar la recuperación del hash de contraseña de terceros desde BMC.

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).

Limitar inicio de sesión simultáneo por cuenta de usuario

Utilice la información de este tema para limitar las sesiones simultáneas por cuenta de usuario.

Esta función permite al usuario decidir cuántas sesiones simultáneas se permiten por cuenta de usuario.

- **Número de sesiones web simultáneas**: se puede configurar de 1 a 10 sesiones.
- **Número de sesiones simultáneas de la línea de comandos**: se puede establecer desde 1 o 2 sesiones.
- **Número de sesiones Redfish simultáneas**: se puede configurar de 1 a 16 sesiones.

Nota: Si el número total de sesiones supera el número establecido, el usuario ya no puede crear una sesión nueva.

Protección del sistema

En este tema se proporciona una visión general de la protección del sistema.

La característica de protección del sistema toma una instantánea del inventario de componentes de hardware como referencia de confianza y, a continuación, supervisa cualquier desviación de la instantánea de referencia. Cuando se produce una desviación, puede informar de un evento al usuario y, opcionalmente, también puede impedir que el servidor arranque en el sistema operativo y solicitar al usuario una respuesta.

El usuario puede tomar una instantánea en cualquier momento, incluso cuando la característica está deshabilitada. La generación de la instantánea dura aproximadamente un minuto. El usuario puede seleccionar un subconjunto de componentes de hardware para aplicar y seleccionar la acción que debe realizarse cuando se detecte una desviación.

Nota: La detección de desviaciones se ejecuta al encender el servidor (POST) o al reiniciar el sistema. Por ejemplo, mientras el SO sigue funcionando, si se extrae una unidad de disco y se vuelve a conectar después, la función de protección del sistema no registrará el evento ni realizará ninguna acción. Si la unidad de disco extraída permanece ausente hasta el siguiente reinicio, la función de protección del sistema entraría en acción.

Notas: Durante el restablecimiento de la CA seguido del primer encendido, XCC puede no notificar a la UEFI para evitar el arranque del SO si se cumplen las siguientes condiciones:

- Si la protección del sistema está habilitada con lo siguiente:
  - Hardware de **CPU** o **DIMM** seleccionado
  - La opción **Evitar el arranque del SO** seleccionada
- Si se produce un cambio en la configuración del hardware que no coincide con la instantánea de confianza.

XCC notificará una discrepancia de configuración después de la POST, y esta limitación no seguirá estando en el rearranque posterior del SO.

Habilitación de la protección del sistema

Utilice la información en este tema para habilitar la protección del sistema.

La función de protección del sistema está deshabilitada de forma predeterminada. Se habilita antes del envío según el requisito del usuario final.

La opción de restablecimiento de XCC a los valores predeterminados también deshabilita la protección del sistema y borra la configuración excepto el historial de instantáneas.

Al activar la protección del sistema, se pide al usuario que confirme la configuración, que utilice la instantánea de confianza existente o que capture el inventario como una nueva instantánea de confianza antes de activar la protección del sistema. Una vez activada:

- Si el sistema está apagado, la protección del sistema comienza a recopilar el inventario de hardware de inmediato.
- Si el sistema está encendido, la protección del sistema compara los datos del inventario de componentes con la instantánea de confianza.

Si el resultado de la comparación indica una desviación de la instantánea de confianza, XCC muestra una advertencia de **incumplimiento debido a una discrepancia de configuración del hardware**. En los detalles de la discrepancia se enumera cada componente de hardware que falta/cambiado/nuevo con atributos de ubicación/identificador/descripción, en comparación con la instantánea de confianza.

El usuario puede configurar el alcance y la acción de la protección del sistema y decidir qué acción tomar cuando el sistema a no es conforme a través del panel Alcance y acción.

Soporte de versión de TLS

Utilice la información de este tema para comprender las distintas versiones de TLS admitidas.

Se admiten las siguientes versiones de TLS:

- TLS 1.2 y superior
- TLS 1.3

Para obtener una lista completa de los conjuntos de cifrado TLS admitidos, consulte “Suites de cifrado TLS admitidas” en la página 38

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
- Restablecer la configuración del controlador de gestión a su configuración predeterminada de fábrica
- Acceder 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, luego pulse **Siguiente >**.
2. Verifique el archivo pulsando **Ver detalles**.
3. Después de verificar el contenido, pulse **Iniciar la restauración**.

Restablecimiento del 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 de XClarity Controller de nuevo después de que se realice la operación de restablecimiento.
   - Al pulsar en **Comenzar a restablecer el BMC a los valores predeterminados de fábrica**, aparecerá una ventana de confirmación y podrá marcar las casillas de verificación para conservar la siguiente configuración:
     - **Conservar configuración de usuario local**: Se realizará una copia de seguridad de la configuración actual del usuario/del rol/global. Restaura el comando CLI de contenido “users”/ ”roles”/”accesscfg”. Por ejemplo: Nombre de usuario/Nombre de rol/Período de tiempo de advertencia de caducidad de la contraseña/Reglas de complejidad de la contraseña habilitadas, etc.

  - **Conservar configuración de red**: Se realizará una copia de seguridad de la configuración actual de red. Restaura la salida de red del comando CLI “ifconfig”. Por ejemplo: nombre de host/ dirección IPv4/dirección IPv6/puerta de enlace, etc.
- Al pulsar en **Aceptar**, se perderán todos los cambios de configuración anteriores, excepto los que decida conservar.
- Si desea habilitar LDAP al restaurar la configuración del BMC, antes de ello debe importar un certificado de seguridad de confianza.
- Si está trabajando desde el sistema local BMC, perderá su conexión TCP/IP. Deberá volver a configurar la interfaz de red del BMC para restablecer la conectividad.
- Después de que se realice el proceso, XClarity Controller se reiniciará.
- El restablecimiento del BMC a los valores predeterminados de fábrica no afectará a la configuración de UEFI ni al modo de acceso (único/multiusuario) de la consola remota (esto se guarda en las cookies del navegador).

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 62

Capítulo 4. Supervisión del 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.

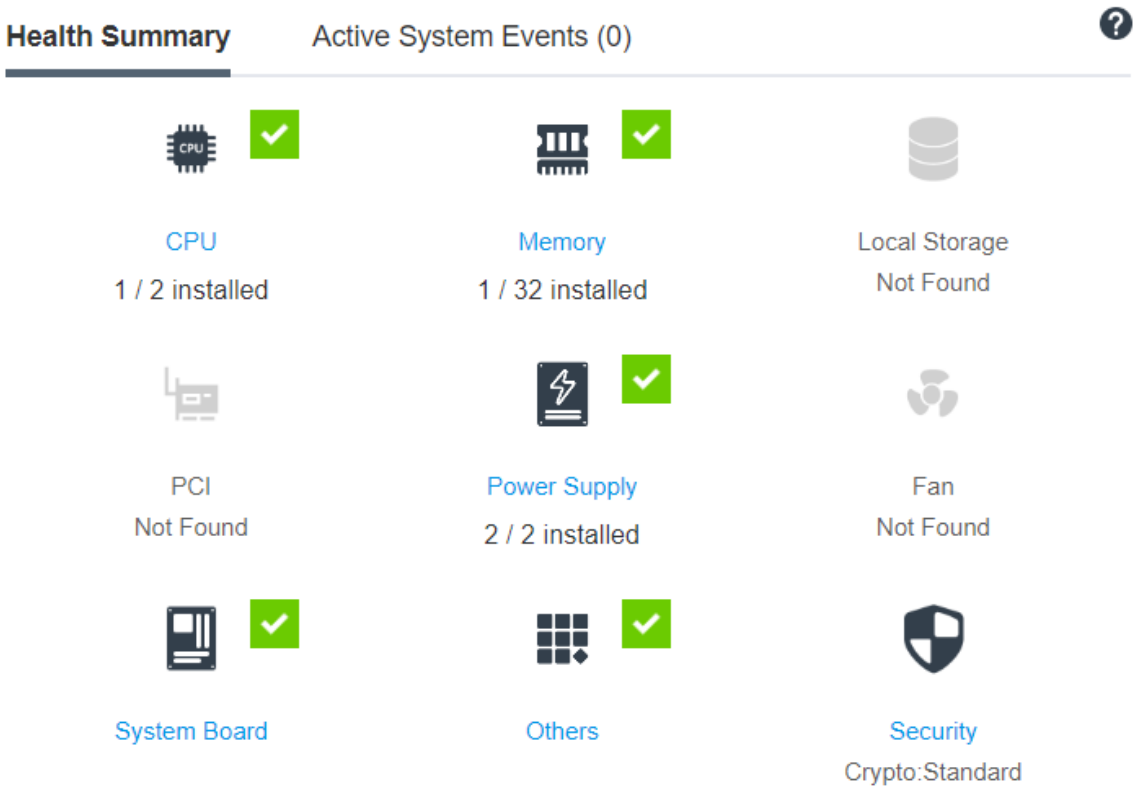
Visualización del resumen de estado/eventos activos del sistema

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

Cuando accede a la página de inicio de 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:

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

Nota: Es posible que el **almacenamiento local** muestre **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 eventos activos para ese componente.

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

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

El texto debajo del componente de hardware indica el número de componentes instalados. Si pulsa en el texto (enlace), se dirigirá a la página **Inventario**.

Nota: En los nodos compatibles con el chasis D3 V2, el enlace de **Fuente de alimentación** solo está disponible en el nodo encargado.

Visualización de la información del sistema

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

En el panel **Información del sistema y configuración** que se encuentra a la derecha de la página de inicio, se proporciona un resumen de la 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
- Gestión de puerto USB del panel frontal

  Nota: Esta característica se admitirá en una actualización futura.
- Licencia del BMC
- Dirección IP del BMC
- Nombre de host del BMC
- Encargado del chasis activo

  Nota: Este elemento solo está disponible en los nodos compatibles con el chasis D3 V2.
- Versión BMC
- Versión UEFI
- Ubicación

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

Tabla 2. 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.
Arrancando sistema operativo o en sistema operativo no admitido (el sistema puede estar en este estado si el SO no responde a los pings)	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.
El sistema se está ejecutando en la prueba de memoria	El servidor está encendido y está ejecutando herramientas de diagnóstico de memoria.

Tabla 2. Descripciones de estado del sistema (continuación)

Estado	Descripción
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 el servidor tiene una licencia que no sea la licencia empresarial del nivel Premier de XClarity Controller, puede comprar una actualización de la licencia para habilitar características 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 del 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 del 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 pulsar 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 pueden ver en la vista gráfica o en la vista de tabla, que incluye lo siguiente:

- **Temperatura**
  - Muestra la temperatura ambiente en tiempo real y las temperaturas de los componentes clave.
  - Al pasar el cursor del ratón sobre un módulo de memoria, se mostrará su temperatura actual.
- **Consumo de energía**

  - Muestra el gráfico circular del consumo de alimentación actual.
  - Al pasar el cursor del ratón sobre el gráfico circular, se mostrará su consumo de energía actual.
  - El gráfico circular de consumo de energía actual está formado por cuatro categorías: CPU, Memoria, Otros y Repuesto. “Otros” significa el consumo total de energía del sistema menos el consumo de energía de la CPU y la memoria. “Repuesto” significa la energía total asignada disponible menos el consumo total de energía del sistema.
  - La pestaña Tensión muestra las lecturas de tensión actuales y el estado de todos los sensores de tensión compatibles con el hardware.
- **Utilización del sistema**
  - Representa la instantánea de utilización actual del sistema, procesador, memoria y subsistemas de E/S.

    Nota: Esta característica se admitirá en una actualización futura.
- **Velocidad del ventilador (RPM)**
  - La sección de velocidad del ventilador muestra las velocidades del ventilador como porcentaje de la velocidad máxima.
  - El usuario puede pulsar en el icono de engranaje para acceder a las opciones de **Aumento de velocidad del ventilador**.
    - Este ajuste permite una refrigeración adicional del servidor en función de la temperatura ambiente. Puede aumentar el ventilador por encima de la velocidad normal mediante un algoritmo térmico controlado. No habrá ningún cambio si los ventiladores ya están funcionando a toda velocidad.

Visualización de los registros de eventos

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

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

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

- **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 eventos cuando hay más de un evento en la misma hora.

  Nota: Algunos números de secuencia utilizan procesos internos del BMC, de modo que es normal que puede haber espacios en los números de secuencia cuando los eventos son clasificados por número de secuencia.
- **Borrar registros**: seleccione esta acción para eliminar los registros de eventos.
- **Actualizar**: seleccione esta acción para actualizar la pantalla con cualquier entrada del registro de eventos que pueda haberse producido desde la última visualización de la página.
- **Tipo**: seleccione qué tipos de eventos se van a mostrar. Los tipos de eventos 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 eventos. Una caja negra que rodea el icono indica qué tipo de evento se mostrará.

- **Filtro de tipo de fuente**: seleccione un elemento del menú desplegable para mostrar solo el tipo de entradas de registro de eventos que desee mostrar.
- **Filtro de tiempo**: seleccione esta acción para especificar el intervalo de los eventos que desea mostrar.
- **Buscar**: para buscar tipos específicos de eventos 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 eventos es 1024. Cuando los registros de eventos 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 eventos” 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 a XClarity Controller. La cuenta se crea con un nombre de usuario y una contraseña aleatoria y solo se puede utilizar para acceder a XClarity Controller en la interfaz Ethernet sobre USB interna. La cuenta solo se puede utilizar para acceder a las interfaces de Redfish y SFTP de XClarity Controller. 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

Utilice la información de este tema para añadir y modificar las notificaciones de correo electrónico y syslog o los destinatarios de SNMP TRAP.

Nota: Esta característica se admitirá en una actualización futura.

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
- Directiva de alimentación
- Propiedades del servidor
- Chasis

  Nota: Este elemento solo está disponible en los nodos compatibles con el chasis D3 V2.

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.

Nota: 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 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 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.

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

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 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 alojamiento que contiene nodos de servidor de alta densidad, la refrigeración del chasis y la alimentación son controladas mediante el SMM en lugar de XClarity Controller. Consulte la interfaz web de SMM3 para obtener más detalles sobre el estado de alimentación de la solución.

Configuración de la redundancia de alimentación

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

Notas:

- Los servidores AMD no admiten la configuración de la función de directiva de energía.
- Cuando hay 2 unidades de fuente de alimentación instaladas, el modo de redundancia se establece en Redundante (N+N). Con esta configuración de 2 unidades de fuente de alimentación, si una de las unidades de fuente de alimentación falla, se perdió o se quitó la CA, presentará un evento de pérdida redundante en el registro de eventos XCC.
- Cuando solo se instala 1 unidad de fuente de alimentación después del envío, el modo de redundancia se configurará automáticamente en modo No redundante.

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

- **Redundante (N+N)**: hay dos o más fuentes de alimentación independientes capaces de suministrar alimentación al sistema simultáneamente. Esto significa que si una o varias fuentes de alimentación fallan, las otras pueden seguir suministrando energía al sistema sin interrupción. La redundancia N+N proporciona un alto nivel de tolerancia a fallos y garantiza que el sistema siga funcionando incluso en caso de fallos múltiples.
  - **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.
- **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 directiva de limitación de alimentación

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

Notas:

- Los servidores AMD no admiten la configuración de la función de limitación de alimentación.
- En un alojamiento que contiene nodos de servidor de alta densidad, la refrigeración del chasis y la alimentación son controladas mediante el SMM en lugar de XClarity Controller. Consulte la interfaz web de SMM3 para obtener más detalles sobre el estado de alimentación de la solución.

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 directiva de redundancia de alimentación. Para cambiar el valor, primero pulse **Restablecer**. Elija el valor preferido; a continuación pulse **Aplicar**.

La capacidad de alimentación total se calcula en función del modo de redundancia de alimentación y el número de PSU instaladas en el sistema. El ajuste manual del límite máximo de alimentación puede estar por encima de la capacidad de alimentación real.

Cuando se habilita la limitación de alimentación, el sistema puede estar regulado para mantener el límite de alimentación.

Nota: Incluso cuando la limitación de alimentación se deshabilita, el sistema puede estar regulado en ciertas condiciones de error, como fallas en la fuente de alimentación, problemas de refrigeración, etc.

La limitación de alimentación se puede habilitar con mediciones de **entrada** o de **salida**. En el menú desplegable, seleccione el tipo de medición que se utilizará para determinar la limitación de alimentación. Al cambiar entre mediciones, el número en el control deslizante cambiará en consecuencia.

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. Los cambios entrarán en vigor inmediatamente.

Configuración de la directiva 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 directiva 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.

Nota: Seleccione la casilla de verificación siguiente para establecer un retraso aleatorio de entre 1 y 15 segundos para Encender si el servidor estaba encendido antes de que se produjera la falla de alimentación.

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

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

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 de XClarity Controller.

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

Tabla 3. 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.
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 NMI (interrupción no enmascarable)	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 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 XClarity Controller
Apagar y volver a encender la alimentación de CA del servidor	Seleccione esta acción para encender y apagar el servidor.
Notas: • Si el sistema operativo está en el modo de protector de pantalla o bloqueado cuando se intenta apagar el sistema operativo, XClarity Controller no pueda iniciar un apagado normal. 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. • Si el LED de encendido del panel frontal parpadea rápidamente, es posible que XClarity Controller no pueda iniciar una secuencia de encendido normal. XClarity Controller puede encender el sistema una vez que el LED de encendido empieza a parpadear lentamente.	

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 de 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.

Descarga de registro 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 de XClarity Controller, pulse la opción **Registro de servicio** en la sección **Acción rápida** y seleccione **Registro de datos de servicio**.

De manera predeterminada, el registro de servicio contendrá los siguientes datos: información del sistema, inventario del sistema, utilización del sistema, tabla SMBIOS, lectura de sensores, registro de eventos, clave FOD, clave SLP, configuración de UEFI y configuración de XClarity Controller 3.

Pase el mouse sobre la opción Información básica y pulsar en la ventana flotante para ver algunos datos reales que se exportarán.

Si bien la información básica es obligatoria, también se puede exportar la siguiente información:

- Información de red (IP, nombre de host)
- Telemetría (datos de 24 horas)
- Registro de auditoría (contiene nombre de usuario)
- Última pantalla de error

Pulse **Exportar** para descargar el registro de datos de servicio.

El proceso de recopilar datos del servicio y soporte puede tardar unos minutos. 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>_xcc3_ServiceData_<date>-<time>.zip`

Por ejemplo: 7X2106Z01A_2345678_xcc3_ServiceData_240517-112857.zip.

Además de los datos de servicio en formato .zip, el registro de depuración también se puede descargar en un formato de archivo .tar.zst a través de **Examinar historial...**. La convención de denominación para el archivo de depuración lodf sigue este patrón: `<machine type and model>_<serial number>_xcc3_DebugLog_<date>-<time>.tar.zst`

Por ejemplo: 7X2106Z01A_2345678_xcc3_DebugLog_240517-112857.zip.

Notas:

- **Examinar historial…** también conservará los registros de servicio exportados recientemente.
- El formato de archivo .tar.zst utiliza un algoritmo de compresión diferente y se puede extraer con el paquete “zstd”. Por ejemplo:
  `tar --use-compress-program=unzstd -xvf <machine type and model>_<serial number>_xcc3_DebugLog_<date>-<time>.tar.zst`

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.

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.

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 de 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:

Habilitar el retardo de apagado

Utilice este campo para especificar el número de minutos que el subsistema BMC esperará a que el sistema operativo se apague 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 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 de XClarity Controller cuando un usuario inicia sesión.

Servicio de solución

Use la información de este tema para habilitar o deshabilitar el servicio de soluciones.

Nota: Esta característica se admitirá en una actualización futura.

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 de XClarity Controller. La fecha y hora de XClarity Controller se utiliza para marcar la hora de todos los eventos que se registran en el registro de eventos y las alertas enviadas.

En la página de inicio de XClarity Controller, pulse el icono del reloj en la esquina superior derecha para ver o cambiar la fecha y hora de XClarity Controller. XClarity Controller no tiene su propio reloj en tiempo real. Puede configurar 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 de 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 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 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 está la hora. Por lo tanto, cuando XClarity Controller se configura para sincronizar con el reloj en tiempo real del host, el usuario puede elegir cómo XClarity Controller utiliza la hora y fecha que se obtiene del reloj en tiempo real.

- Local (ejemplo: Windows): En este modo, 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. Si en su ubicación se establece un horario de verano, también puede marcar la casilla de verificación **Ajustar automáticamente el horario de verano (DST)**.
- UTC (ejemplo: Linux): En este modo, 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 en su ubicación se establece un 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**.

Nota: Cuando se produce el cambio a horario de verano, no se realizarán las acciones que se hayan programado para que 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, XClarity Controller leerá la hora como las 3:00 am.

Configuración del chasis D3 V2

Utilice la información de este tema para comprender las configuraciones del chasis D3 V2.

Pulse **Chasis** en **Configuración del servidor** para ver información sobre el chasis D3 V2.

Información del chasis

En esta sección, se muestra la información del chasis, como el UUID, el número de serie, el tipo de equipo y la versión de firmware. También se muestra la información de los nodos, como el factor de forma, el estado de energía y la dirección IP.

Notas:

- Pulse el botón **Restablecer/Reubicar** junto al nodo correspondiente para reiniciarlo o simular una reubicación física.
- Solo el nodo encargado puede restablecer o reubicar otros nodos.

Rol del encargado del chasis

En esta sección, se muestran las preferencias de selección del encargado del chasis.

Notas:

- Seleccione **Participar en el rol de encargado del chasis** para permitir que un nodo pueda participar en el proceso de selección del encargado. Si hay otro nodo designado como encargado permanente, no se realizará ningún proceso de selección, a menos que ese nodo esté ausente.
- Seleccione **Designar este nodo como encargado permanente del chasis** si desea que solo un nodo sea el encargado. En ese caso, no hay una alta disponibilidad para el rol de encargado. Si el nodo encargado permanente está ausente del chasis, se llevará a cabo el proceso de selección del encargado para elegir al próximo encargado adecuado.

Historial de mantenimiento del chasis

En el historial de mantenimiento del chasis, se conserva un registro de los nodos que se agregan al chasis o que se quitan de él, así como el cambio de rol de encargado de un nodo a otro.

Capítulo 6. 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 de 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 consola remota está disponible con las características del nivel Premier de XClarity Controller y solo está disponible a través de la interfaz web. Debe iniciar sesión en 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 la actualización del nivel Estándar de XClarity Controller al nivel Premier de XClarity Controller, consulte "Actualización de XClarity Controller" en la página 6.

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

- Visualice video de forma remota con una resolución gráfica de hasta 1920x1200 32bpp@60Hz, 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 de XClarity Controller y móntela al servidor como una unidad virtual. Se pueden cargar hasta un máximo de dos archivos con un tamaño máximo de 100 MB en la memoria de XClarity Controller.

Notas:

- Cuando la característica de consola remota se inicia en modo multiusuario, (XClarity Controller con la característica de nivel Premier configurada admite seis sesiones simultáneas), la característica 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 de 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 característica de consola remota. Para ver o cambiar el número de puerto de red utilizado por la característica de consola remota, consulte "Habilitación del servicio y asignación de puertos" en la página 35.
- La característica 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 del 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.

La funcionalidad de consola remota de XClarity Controller solo está disponible en las características de nivel Premier 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 de nivel Premier de XClarity Controller, instálela utilizando las instrucciones que aparece en “Instalación de una clave de activación” en la página 87.

Para usar la funcionalidad de consola remota, pulse la imagen con una flecha de color blanco que apunta en diagonal en la sección **Vista previa de consola remota** de la página de inicio de XClarity Controller o en la página web de **Consola remota**.

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 característica 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 JPG.

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 de XClarity Controller.

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.

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 características 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 característica de RDOC. Estos mecanismos se describen más abajo.

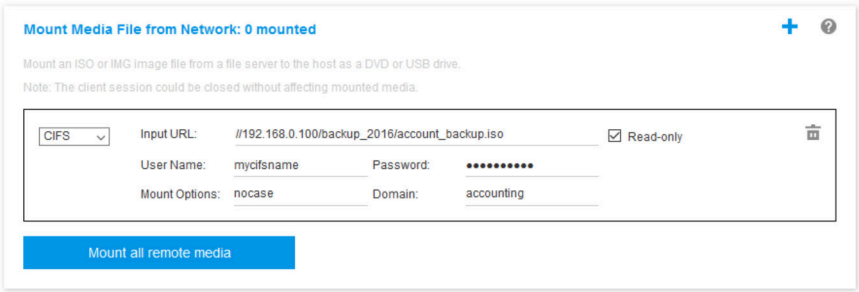
- Las medios locales son los archivos ISO e IMG que se encuentran en el sistema que está utilizando para acceder a XClarity Controller. Este mecanismo solo está disponible a través de la sesión de consola remota, no directamente desde la página web de la consola remota y solo está disponible con las características de nivel Premier de XClarity Controller. Para montar medios locales, pulse **Montar todos los medios locales** en la sección **Montar el archivo de medios local**. Se pueden montar hasta cuatro archivos concurrentemente en el servidor.
- 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. 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 XClarity Controller acceda al archivo en el sistema remoto.

      Nota: 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.

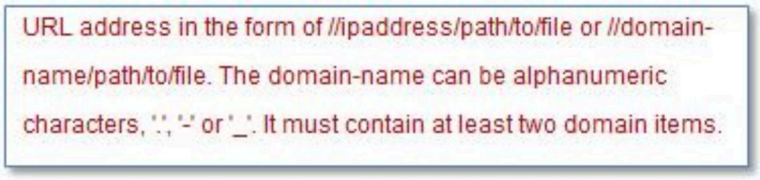
    Nota: Pueden producirse errores durante el proceso de montaje de los certificados de seguridad generados por Microsoft IIS. Si esto ocurre, consulte “Problemas de error de montaje de medios” en la página 77.

  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 de XClarity Controller y montar como medio virtual mediante la característica de RDOC de XClarity Controller. El tamaño total para ambos archivos no debe exceder 100 MB. Estos archivos se mantendrán en la memoria de XClarity Controller hasta que se eliminan, incluso si se termina la sesión de consola remota. La característica 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.

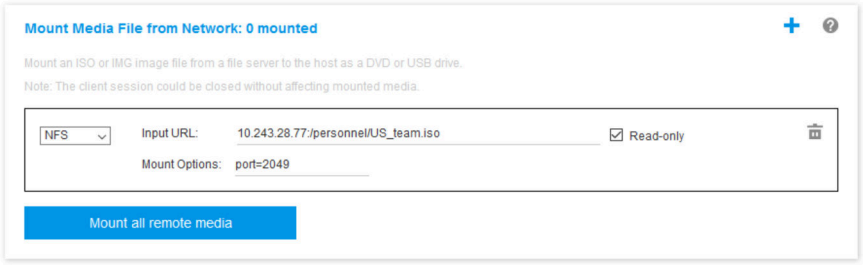


El BMC proporciona directrices cuando se especifica la URL. Si la URL que se introduce no es válida, el botón de montaje estará desactivado y se mostrará texto en rojo en el campo de la URL donde se muestra el formato esperado para la URL.

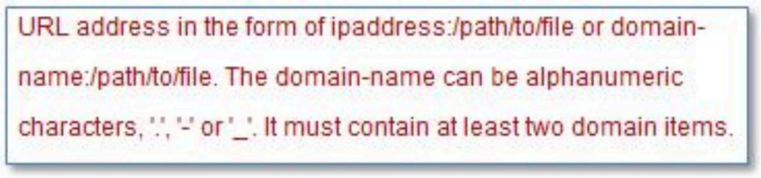


– **NFS: Sistema de archivos de red**: consulte la descripción arriba para obtener detalles. **Ejemplo**:

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 introduce 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.

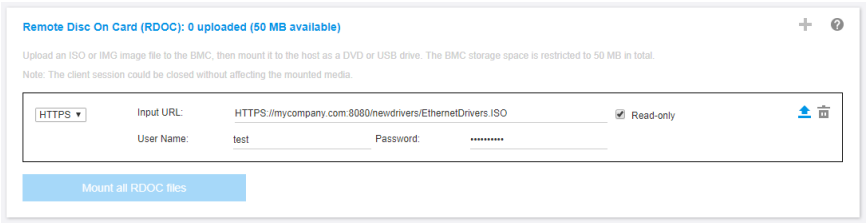


- **HTTPS - Protocolo seguro de transferencia de hipertexto**:
  - Escriba la URL que ubica el archivo en el sistema remoto.
  - Si desea que el archivo se presente al servidor como medio virtual de solo lectura, marque la casilla de verificación.
  - Especifique las credenciales necesarias para que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

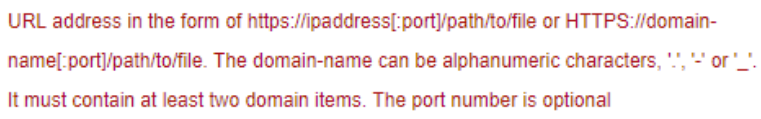
  Notas:

  - 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 77.
  - 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 introduce 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.



- **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 XClarity Controller acceda al archivo en el sistema remoto.

  Notas:

- 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 XClarity Controller se conecta a un servidor HTTPS, aparecerá una ventana emergente que muestra información del certificado de seguridad utilizado por el servidor HTTPS. 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
```

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 remota.

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

Capítulo 7. 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 de almacenamiento
- Configuración de RAID

Detalle de almacenamiento

Para utilizar la función de detalles de almacenamiento, 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.

Se activará una advertencia o un evento crítico cuando el valor de vida útil restante de la unidad SSD alcance el umbral o sea inferior. El valor de vida útil restante predeterminado para la advertencia y el evento crítico es del 8 % y el 4 %, respectivamente. Pulse el icono de engranaje que se encuentra junto a **Detalle de almacenamiento** para establecer el valor del umbral.

Para configurar las placas posteriores SAS/SATA/NVMe (AnyBay) que admiten el modo de **Pista PCIe x1**, pulse el icono de engranaje que se encuentra junto a **Placa posterior**, luego seleccione el grupo de bahías de unidad y pulse el botón **Aplicar** para guardar la configuración.

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.

Importar unidades extranjeras
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.

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 "tarjetas de discos virtuales".

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

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

Creación de un nuevo disco virtual RAID

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.

      Nota: Si no hay suficientes unidades a seleccionar y pulsa **Siguiente**, un mensaje de error aparecerá bajo el campo de nivel de RAID.

   b. Para algunos niveles de RAID, se requiere espacio. También existe una cantidad mínima de unidades que deben existir en el espacio. Para estos tipos de situaciones, especifique el número de espacio en el campo **Número de espacio**, seleccione **Miembro** o **Repuesto** en el menú desplegable que se encuentra junto a las unidades, luego marque la casilla de verificación que se encuentra junto a las unidades que se utilizarán para crear el disco virtual.
   c. 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, la creación de un disco virtual utilizará toda la capacidad 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. Pulse el icono **Quitar** para quitar un disco virtual. 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 creación** 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, como nombre de la unidad, estado de la unidad, tipo, producto, fabricante, número de serie y acciones. Puede ir a la página **Inventario** para visualizar todas las propiedades que 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.
       - **Iniciar la reconstrucción**: Reconstruye el RAID.
       - **Configurar unidad de disco como reutilizable**: Establece la unidad como reutilizable.
       - **Establecer unidad de disco como faltante**: Establece la unidad como faltante.
       - **Configurar unidad en buen estado a varias unidades de disco**: Añade la unidad al conjunto de discos de varias unidades de disco.
       - **Hacer 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.
       - **Hacer 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 de disco distintas de RAID**. Al pulsar la opción **Convertir varias unidades de disco a listas 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 8. Actualización del firmware del servidor

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

Visión general de la actualización de firmware

Información general sobre la actualización de firmware del servidor.

Al pulsar **Actualización de firmware** en el panel izquierdo, se proporciona una visión general de la información del firmware.

- **Actualizar desde repositorio:** sincroniza el firmware del servidor con el repositorio remoto CIFS/NFS para actualización por lotes. Consulte "Actualización desde el repositorio" en la página 84.
- **Firmware del sistema:** visión general del estado del firmware del sistema, la versión y la actualización del firmware del sistema.

  Nota: Pulse **Sincronización automática** para habilitar o deshabilitar **Promoción automática del BMC principal a copia de seguridad**. Cuando esta configuración está habilitada, el firmware del banco de copia de seguridad pendiente se sincronizará desde el banco principal después de que el banco primario pase la medición de la Métrica de estabilidad de la imagen (ISM).
- **Firmware del adaptador:** visión general del firmware del adaptador instalado, su estado, su versión y la actualización de firmware del adaptador.
- **Firmware de la unidad de fuente de alimentación:** visión general de la versión de firmware de la unidad de fuente de alimentación y actualización de firmware de PSU.
- **Firmware de PSoc de la placa posterior de la unidad:** visión general de la versión de firmware de la placa posterior. Y para realizar la actualización de firmware del sistema.

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

- **Activo:** el firmware está activo.
- **Inactivo:** el firmware no está activo.
- **Reinicio pendiente:** la imagen de firmware se ha actualizado y entrará en vigencia después de que se haya reiniciado el servidor del BMC.
- **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 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.
- A excepción del adaptador SATA M.2, los servidores de procesador AMD no admiten la actualización de firmware del adaptador fuera de banda.

- 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. Pulse **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 XClarity Controller para surtir efecto, se mostrará un mensaje de aviso. Para conocer más detalles sobre cómo reiniciar XClarity Controller, consulte “Acciones de alimentación” en la página 62.

Actualización desde el repositorio

Actualización del firmware del servidor desde un repositorio remoto

Visión general

Nota: Para la funcionalidad de historial de firmware CIFS/NFS/HTTPS/Incorporado se necesita una licencia XCC Premier.

XCC ha introducido la actualización de firmware en un servidor mediante el paquete de actualizaciones (Service Packs). Esta característica simplifica el proceso utilizando una única API o herramienta cliente Redfish para actualizar todo el firmware del sistema, incluidos los paquetes de firmware OOB e IB. El proceso consiste en identificar los paquetes de firmware aplicables, descargarlos y extraerlos de un servidor HTTP/HTTPS remoto o cargarlos en el almacenamiento interno del BMC a través de un navegador web, o montarlos desde un directorio compartido CIFS o NFS.

Los archivos de metadatos (formato JSON) deben colocarse en el directorio raíz del sistema de archivos compartidos en red si se utiliza el montaje CIFS o NFS, con las cargas útiles de firmware especificadas en los metadatos. El dispositivo microSD del servidor puede almacenar repositorios históricos, lo que permite a los usuarios retroceder niveles de firmware.

Si los paquetes de firmware contienen alguna carga útil que no admita la actualización de firmware fuera de banda, el BMC iniciará el servidor y lo configurará para que arranque desde la imagen del SO integrada instalada en el BMC antes de realizar la actualización.

Paquete de actualización y metadatos

El paquete de actualizaciones (Service Packs) es un archivo comprimido de un paquete de firmware. Contiene uno o varios paquetes de firmware para los componentes de un sistema. La característica Actualizar desde repositorio de XCC consume el archivo del paquete de actualizaciones. El archivo de paquete descomprimido contiene metadatos y binarios de carga útil. Los archivos de metadatos JSON proporcionan información a XCC sobre el tipo de imágenes de firmware que contiene el archivo de paquete, y los binarios de carga útil proporcionan las imágenes de firmware.

Repositorio de firmware dentro de XCC

El paquete de actualizaciones puede contener varios paquetes de firmware y XCC reserva 2 GB de espacio en su memoria flash para nuevas características. Cuando se recibe un nuevo paquete, XCC limpia los datos antiguos. Algunas plataformas utilizan una tarjeta MicroSD para proporcionar almacenamiento adicional y XCC mueve el último paquete actualizado al repositorio histórico de la tarjeta SD. El repositorio del historial de firmware puede almacenar hasta tres paquetes y los usuarios pueden utilizar la característica de reversión de firmware para volver a un paquete anterior.

Notas:

- Si el paquete de actualizaciones solo incluye el paquete de firmware OOB disponible para el sistema, XCC no cambia el estado de alimentación del sistema. Para actualizar el firmware del dispositivo PCI, es necesario que el sistema esté encendido.
- Si el paquete de actualizaciones incluye el paquete de firmware IB disponible para el sistema, XCC almacena el estado de alimentación del sistema antes de la actualización y restaura el estado de alimentación una vez actualizado el paquete de actualizaciones. Durante el proceso de actualización, XCC reinicia el host en el SO integrado.
- Si el paquete de actualizaciones incluye un nivel de requisito de firmware de UEFI y la versión de UEFI instalada actualmente no cumple o está por detrás de ese nivel, XCC apaga el sistema para realizar primero una actualización del firmware de UEFI.
- Si el paquete de actualizaciones incluye un nivel de requisito de firmware de XCC y la versión actual de XCC instalada no cumple o está por detrás de ese nivel, XCC se reinicia primero después de actualizarse.

Actualización con WebGUI

Con **Actualizar desde repositorio**, el usuario puede configurar XCC para sincronizar el firmware de servidor con un almacenamiento interno. El repositorio de firmware debe contener paquetes que incluyan archivos binarios y de metadatos, o un JSON de metadatos de paquete de actualizaciones y los archivos binarios correspondientes. XCC analiza los archivos JSON de metadatos para seleccionar los paquetes de firmware que admiten la actualización OOB para este hardware de sistema específico y luego inicia una actualización por lotes.

Para actualizar desde el repositorio, realice los pasos siguientes:

1. Cuando utilice el almacenamiento interno, pulse **Importar paquetes de firmware** y examine el paquete de firmware (formato .tgz o zip).
2. Pulse **Actualizar sistema** para comenzar la actualización de lote.
3. Pulse **Ver detalles** para ver el estado de actualización.
   - **Marca de verificación verde** : la actualización del firmware ha finalizado correctamente.
   - **Marca de X roja** : se ha producido un error en la actualización del firmware.
   - **Actualización:** el firmware está llevando a cabo el proceso de actualización.
   - **Cancelar:** la actualización del firmware se ha cancelado.
   - **En espera:** la actualización del firmware está en espera de desplegarse.

Nota: Al pulsar **Detener actualización** se cancelarán las actualizaciones en la cola una vez completada la actualización del paquete de instalación actual.

4. Cuando utilice CIFS o NFS, pulse **Desmontar** para desconectarse del repositorio remoto.
5. Si la actualización necesita reiniciar XClarity Controller para surtir efecto, se mostrará un mensaje de aviso. Para conocer más detalles sobre cómo reiniciar XClarity Controller, consulte “Acciones de alimentación” en la página 62.

Nota: Si el sistema tiene instalada una tarjeta MicroSD, puede ver el historial de actualizaciones del paquete de actualizaciones y seleccionar el índice del paquete de actualizaciones para realizar la reversión del firmware. El proceso es similar a la actualización desde el repositorio, excepto que el paquete de actualizaciones histórico se coloca dentro de la MicroSD.

Capítulo 9. 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 de XClarity Controller disponibles para el servidor. El nivel del firmware instalado en el servidor varía según el tipo de hardware.

Puede actualizar la funcionalidad de 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 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 87, “Eliminación de una clave de activación” en la página 87 o “Exportación de una clave de activación” en la página 88 para obtener información acerca del manejo de una clave de activación mediante la interfaz web de XClarity Controller. Consulte “Comando keycfg” en la página 117 para obtener información acerca del manejo de una clave de activación mediante CLI de XClarity Controller.

Para registrar un ID en la administración de 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

Instalación de una clave de activación

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

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

Paso 1. Pulse **Licencia** en **Configuración del 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 pulse **Abrir** para añadir el archivo. Para terminar de añadir la clave, pulse **Importar** en la ventana Añadir clave de activación.

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

Eliminación de una clave de activación

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

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

Paso 1. Pulse **Licencia** en **Configuración del 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 la eliminación del archivo de clave. La clave de activación seleccionada se eliminará del servidor y ya no aparecerá en la página Administración de licencias.

Exportación de una clave de activación

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

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

Paso 1. Pulse **Licencia** en **Configuración del 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 solicitud de exportación de la clave de activación.

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

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 de XClarity Controller.

Utilice la interfaz de línea de comandos (CLI) de XClarity Controller para acceder a 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 de XClarity Controller (consulte “Configuración de redirección serie a SSH” en la página 89 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.

> **Nota:** 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 XClarity Controller como servidor terminal en serie.

La redirección serie a SSH le permite a un administrador del sistema utilizar 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 del 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> ?
```

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 usbeth” en la página 137
- “Comando users” en la página 137
- “Comando volts” en la página 101
- “Comando vpd” en la página 101

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 eventos del IMM.

Utilice el comando **clearlog** para borrar el registro de eventos del IMM. Debe tener autorización para borrar los registros de eventos para utilizar este comando.

Nota: Este comando está diseñado solo para el uso del personal de soporte.

Sintaxis:
```
clearlog [-options]
```

Tabla 4. Opciones de clearlog

Opción	Descripción	Valores
-t	Tipo de evento, elija el tipo de evento a borrar. Si no se especifica, se seleccionarán todos los tipos de eventos.	all, platform, audit • all: todos los tipos de eventos, lo que incluye los eventos de plataforma y eventos de auditoría. • platform: tipo de evento de plataforma. • audit: tipo de evento de auditoría.

Example:
```
system> clearlog
All event log cleared successfully
system>
system> clearlog -t all
All event log cleared successfully
system>
system> clearlog -t platform
Platform event log cleared successfully
system>
system> clearlog -t audit
Audit event log cleared successfully
system>
```

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 mhlog

Utilice este comando para visualizar las entradas de registro de actividad del historial de mantenimiento

Sintaxis:

```
mhlog [-options]
```

Tabla 5. Opciones de mhlog

Opción	Descripción	Valores
-c	Mostrar entradas de recuento	Entre 1 y 250
-i	Mostrar entradas empezando en el índice	Entre 1 y 250
-f	Nombre de archivo remoto del archivo de registro	Nombre de archivo válido para el nombre de archivo del archivo de registro
-ip	Dirección del servidor tftp/sftp	Dirección IP válida para el servidor TFTP/SFTP
-pn	Número de puerto del servidor tftp/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

Ejemplo:

```
system> mhlog
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: D1DG94C0075) is added.                          05/08/2020,06:43:28
system>
```

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.

Sintaxis:

```
led [-options]
```

Tabla 6. Opciones de led

Opción	Descripción	Valores
-l	Obtener el estado de todos los LED del sistema y los subcomponente del sistema	
-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)

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 eventos del IMM.

Utilice el comando **readlog** para visualizar las entradas de registro de eventos del IMM. Se muestran cinco registros de eventos al mismo tiempo. Las entradas se visualizan de más reciente a más antigua.

Notas:

- R - no válido
- I - información
- W - advertencia
- E - crítico

Sintaxis:
```
readlog [-options]
```

Tabla 7. Opciones de readlog

Opción	Descripción	Valores
-a	Muestra todas las entradas del registro de eventos, empezando por la más reciente.	
-f	Restablece el contador y muestra las 5 primeras entradas en el registro de eventos, empezando por la más reciente.	
-date	Muestra las entradas del registro de eventos para la fecha especificada	Utilice el formato siguiente: mm/dd/aaaa
-sev	Muestra las entradas del registro de eventos para el nivel de gravedad especificado.	R, I, W, E
-i	Establece la dirección IP IPv4 o IPv6 del servidor TFTP o SFTP donde se guarda el registro de eventos. Las opciones de comando **-i** y **-l** se utilizan juntas para especificar la ubicación.	Dirección IP válida

Tabla 7. Opciones de readlog (continuación)

Opción	Descripción	Valores
-l	Establece el nombre del archivo de registro de eventos. Las opciones de comando **-i** y **-l** se utilizan juntas para especificar la ubicación.	Nombre de archivo válido
-pn	Muestra o establece el número de puerto del servidor TFTP o SFTP.	Número de puerto válido (predeterminado 69/22)
-u	Especifica el nombre de usuario del servidor SFTP.	Nombre de usuario válido
-pw	Especifica la contraseña del servidor SFTP.	Contraseña válida
-di	Capacidad de registro de auditoría ampliada	none, ipmi

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 servicelog

Se utiliza este comando para generar un nuevo archivo de datos de servicio.

Nota: Este comando solía ser el comando **ffdc**.

Utilice el comando **servicelog** para generar y transferir datos de servicio a Soporte.

La siguiente lista consta de comandos que se utilizarán con el comando **servicelog**:

En la tabla siguiente se muestran los argumentos para las opciones.

Sintaxis:
```
servicelog [subset_command] [-options]
```

Tabla 8. Comandos de subconjunto servicelog

Opción	Descripción
generar	Crear un nuevo archivo de datos de servicio
estado	Comprobar el estado del archivo de datos de servicio

Tabla 8. Comandos de subconjunto servicelog (continuación)

Opción	Descripción
copiar	Copiar datos de servicio existentes
suprimir	Eliminar datos de servicio existentes

Tabla 9. opciones de servicelog

Opción	Descripción	Valores
-t	Tipo de registro de servicio	1, 2, 3 • **1**: Registro de depuración (FFDC, predeterminado) • **2**: Registro de datos de servicio • **3**: Registro de depuración acoplado al registro de datos de servicio, que solo es válido cuando se copian archivos de registro
Opciones adicionales para generar comandos		
-c	Selección de categoría de datos de volcado. La categoría de datos no estará contenida si no se especifica con esta opción.	• Para el tipo 1 (ffdc): archivo de núcleo • Para el tipo 2 (registro de datos de servicio): red, auditoría, telemetría, osscreen
Opciones adicionales para los comandos generate y copy		
-f	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	Dirección 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
-timeout	Minutos para permitir la copia en primer plano.	Entre 1 y 5 (predeterminado 1)

Ejemplo:

```
system> servicelog generate
Generating ffdc...
system> servicelog status
Type 1 ffdc: in progress
system> servicelog copy -t 1 -ip 192.168.70.230 -u User2 -pw Passw0rd -f /tmp/
Waiting for ffdc.....
Copying ffdc...
ok
system> servicelog status
Type 1 ffdc: completed
8737AC1_DSY0123_xcc_120317-153327.tgz


system> servicelog generate
```

```
Generating ffdc...
system> servicelog status
Type 1 ffdc: in progress
system> servicelog status
Type 1 ffdc: in progress
system> servicelog copy -ip 192.168.70.230
Copying ffdc...
ok
system> servicelog status
Type 1 ffdc: completed
8737AC1_DSY0123_xcc_120926-105320.tgz
system>
```

Comando syshealth

Este comando proporciona un resumen del estado o los eventos activos.

Utilice el comando **syshealth** para visualizar un resumen de estado o de eventos 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 [arguments]
```

Tabla 10. Argumentos de syshealth

Argumentos	Descripción
resumen	Muestra el resumen de estado del sistema.
eventos activos	Muestra los eventos activos.
refrigeración	Muestra el estado de salud de los dispositivos de refrigeración.
alimentación	Muestra el estado de los módulos de alimentación.
almacenamiento	Muestra el estado del almacenamiento local.
procesadores	Muestra el estado de los procesadores.
memoria	Muestra el estado de la memoria.

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.

Sintaxis:
```
temps
```

Ejemplo:

```
system> temps
Temperatures are displayed in degrees Fahrenheit/Celsius
              WR          W     T             SS             HS
-------------------------------------------------------------------------
Ambient Temp  109.40/43   N/A   78.80/26.00  109.40/43.00  122.00/50.00
Exhaust Temp  N/A         N/A   32.00/0 .00  116.60/47.00  N/A
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.

Sintaxis:

```
volts
```

Ejemplo:

```
system> volts
              HSL  SSL   WL    WRL   V     WRH   WH   SSH   HSH
-------------------------------------------------------------
CMOS Battery  N/A  2.25  2.39  0.03  3.12  0.03  N/A  N/A   N/A
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 vitales) asociados con el hardware y el software del servidor.

Utilice el comando **vpd** para visualizar los datos de producto vitales 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 [arguments]
```

Tabla 11. Argumentos de vpd

Argumentos	Descripción
vpd sys	Muestra los datos de producto vitales para el sistema.
vpd bmc	Muestra los datos de producto vitales para el controlador de gestión.
vpd uefi	Muestra los datos de producto vitales para la BIOS del sistema.
vpd lxpm	Muestra los datos de producto vitales para la LXPM del sistema.
vpd fw	Muestra los datos de producto vitales para el firmware del sistema.
vpd comp	Muestra los datos de producto vitales para los componentes del sistema.
vpd pcie	Muestra los datos de producto vitales para los dispositivos PCIe.

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.

Sintaxis:
```
power on [-options]
power off [-options]
power cycle [-options]
power uefi
power state
```

Tabla 12. Comandos de power

Comando	Descripción
encender	Utilice este comando para encender la alimentación del servidor.
apagar	Utilice este comando para apagar la alimentación del servidor.
apagar y encender la alimentación	Use este comando para apagar la alimentación del servidor y luego encenderla.
UEFI de alimentación	Utilice este comando para arrancar en F1 Configuración de UEFI.
estado de energía	Utilice este comando para visualizar el estado de alimentación del servidor y el estado actual del servidor.

Tabla 13. Opciones de power

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.	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**.	

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 1:30
```

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.

Sintaxis:
```
reset [-options]
```

Tabla 14. Opciones de reset

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.	

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 directivas para la pérdida de redundancia de alimentación.

Sintaxis:
```
fuelg [-options]
```

Tabla 15. Opciones de fuelg

Opción	Descripción	Valores
-pme	Habilita o deshabilita la gestión de alimentación y limitación de alimentación en el servidor.	on, off
-pcapmode	Establece el modo de limitación de alimentación del servidor.	output, input
-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, perf
-period	Valor numérico para mostrar el historial.	1, 6, 12, 24 horas
-pm	Establece el modo de directiva de pérdida de alimentación redundante.	• **bt**: básico con regulación • **rt**: redundante con regulación (predeterminada)
-zm	Habilitar o deshabilitar el modo de salida cero. Esta configuración solo se puede establecer cuando el modo de la directiva está establecido en redundante con regulación.	on, off

Tabla 15. Opciones de fuelg (continuación)

Opción	Descripción	Valores
-perf	Visualiza el uso actual de cálculo, incluyendo el sistema, el procesador, el módulo de memoria y E/S.	
-pc	Mostrar consumo de alimentación actual	• **output**: muestra el consumo de alimentación de salida actual del sistema, el procesador, el módulo de memoria y otros componentes. • **input**: muestra el consumo de alimentación de entrada actual, incluido el consumo de alimentación del sistema. **Nota:** En el caso de los servidores AMD, el consumo de alimentación de salida actual no mostrará algunos de los componentes.

Comando pxeboot

Este comando muestra y establece la condición del entorno de ejecución de prearranque.

Sintaxis:
```
pxeboot [-options]
```

Tabla 16. Opciones de pxeboot

Opción	Descripción	Valores
-en	Establece la condición del entorno de ejecución de prearranque para el siguiente reinicio del sistema.	enabled, disabled

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.

Sintaxis:
```
accseccfg [-options]
```

Tabla 17. Opciones de accseccfg

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.	on, off
-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
-chgnew	Cambie la contraseña de usuario nuevo en el primer inicio de sesión.	on, off
-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

Ejemplo:

```
system> accseccfg
  -am: local
  -lp: 60
  -pe: none
  -pew: 0
  -pc: on
  -pl: 10
  -ci: 0
  -lf: 5
  -chgnew: on
  -rc: 5
  -wt: 20
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.

Sintaxis:
```
asu [subset_command]
```

Tabla 18. Comandos de subconjunto de asu

Comando	Descripción	Valor
ayuda	Utilice este comando para visualizar la información de ayuda para una o varias configuraciones.	**setting_name**
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_name=valor**
show	Utilice este comando para visualizar el valor actual para una o varias configuraciones.	**setting_name**
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.	**setting_name**
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.	
Notas: • En la sintaxis de comandos, **setting_name** es el nombre de la configuración que desea ver o cambiar y **valor** es el valor que está colocando en la configuración. • **setting_name** puede ser más que un nombre, excepto cuando usa el comando **set**. • **setting_name** puede contener comodines, como por ejemplo un asterisco (*) o un símbolo de interrogación (?). • **setting_name** puede ser un grupo, el nombre de una configuración o **all**.		

Ejemplos:

- Para visualizar todas las opciones del comando asu escriba `asu help`.
- Para visualizar la ayuda de un comando escriba `asu help setting_name`.

- Para cambiar un valor escriba `asu set setting_name=value`.
- Para visualizar el valor actual escriba `asu show setting_name`.
- Para ver todos los posibles valores de una configuración escriba `asu showvalues setting_name`. 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>
```
- Para mostrar los grupos de configuración disponibles, ingrese `asu showgroups`.

En la tabla siguiente se muestran los argumentos para las opciones.

Tabla 19. 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**.	
-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 20. 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.

Sintaxis:

```
backup [-options]
```

Tabla 21. Opciones de backup

Opción	Descripción	Valores
-f	Nombre de archivo del archivo de copia de seguridad	Nombre de archivo válido
-pp	Contraseña o frase delimitada por comillas que se utiliza para cifrar las contraseñas dentro del 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 21. Opciones de 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

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 [ethernet_number]
```

Ejemplo:
```
dhcpinfo eth1
```

La tabla siguiente describe la salida del ejemplo.

Tabla 22. Salida de dhcpinfo

Campo	Descripción
-server	Servidor DHCP que asignó la configuración
-n	Nombre de host asignado
-i	Dirección IPv4 asignada
-i6	Dirección IPv6 asignada
-g	Puerta de enlace asignada
-s	Máscara de subred asignada
-d	Nombre de dominio IPv4 asignado
-d6	Nombre de dominio IPv6 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

Tabla 22. Salida de dhcpinfo (continuación)

Campo	Descripción
-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.

Sintaxis:
```
dns [-options]
```

Tabla 23. Opciones de DNS

Opción	Descripción	Valores
-state	Estado de DNS	on, off
-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.
-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.
-ddns	Estado de DDNS	enabled, disabled
-dnsrc	Nombre de dominio DDNS preferido	dhcp, manual
-ddn	DDN manualmente especificado	
-ddncur	DDN actual (solo lectura)	
-p	Servidores DNS preferidos (ipv4, ipv6)	ipv4, ipv6
-dscvry	detección de direcciones LXCA	enabled, disabled
-dsclist	Lista LXCA de SRV de DNS	
-dscxm	Configuración de XClarity Manager	

El siguiente ejemplo muestra una configuración del IMM donde DNS está deshabilitado:
```
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>
```

Comando encaps

Utilice este comando para permitir que el BMC salga del modo de encapsulación.

Sintaxis:
```
encaps [arguments]
```

Tabla 24. Argumentos de encaps

Argumentos	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.

Sintaxis:
```
ethtousb [-options]
```

Tabla 25. Comando ethtousb

Opción	Descripción	Valores
-en	Estado de Ethernet sobre USB.	enabled, disabled **Nota:** Habilite la interfaz Ethernet sobre USB a través de **<usbeth>** para que la asignación de puertos sea efectiva.
-m**[x] port1:port2**	Configura la asignación de puertos para el índice **x**.	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 **map_ index**	Extrae la asignación de puertos para el índice especificado.	El número de índice de puerto, **map_index**, se especifica como un número entero de 1 a 10 en la opción de comando. **Nota:** Los índices de mapa de puerto se visualizan mediante el comando **ethtousb** sin opciones.

Ejemplo:
```
system> ethtousb -en enabled -m1 100:200 -m2 101:201
system> ethtousb
        ethtousb : On
        ===============
         1:   100:  200
         2:   101:  201
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.

Sintaxis:
```
firewall [-options]
```

Tabla 26. Opciones de firewall

Opción	Descripción	Valores
La siguiente opción es para la lista blanca de direcciones IP		
-wips	Mostrar/configurar las direcciones IP de la lista blanca.	<Direcciones IP válidas>, clr • **Direcciones IP válidas**: Permite de 1 a 3 direcciones IP (separadas por comas, CIDR o rango) **Nota:** Las direcciones IPv4 e IPv6 pueden utilizar el formato CIDR para bloquear un rango de direcciones. • **-clr**: Borrar la lista blanca
Las siguientes opciones son para Lista de bloqueo y Restricción de tiempo		
-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.
-bbt	Bloquear hora de inicio, debe ser posterior a la hora actual	Hora con formato <AAAA-MM-DD HH:MM>
-bet	Bloquear hora de término, debe ser posterior a la hora de inicio	Hora con formato <AAAA-MM-DD 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

Tabla 26. Opciones de firewall (continuación)

Opción	Descripción	Valores
-iplf	Número máximo de errores de inicio de sesión antes de que la dirección IP se bloquee.	Valor numérico entre 0 y 32, 0 = no se bloquea nunca **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>**
-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

En la lista siguiente se presentan ejemplos de la sintaxis del comando **firewall**:

- Para mostrar el valor de todas las opciones y la lista de bloqueo de direcciones IP, ingrese `firewall`.
- Para bloquear el acceso desde varias IP, ingrese `firewall -bips 192.168.1.1,192.168.1.0/24,192.168.1.1-192.168.1.5`.
- Para bloquear todos los accesos durante 01:00-02:00,05:05-10:30,14:15-20:00 cada día, ingrese `firewall -bti 01:00-02:00,05:05-10:30,14:15-20:00`.
- Para borrar todas las reglas de Lista de bloqueo y Restricción de tiempo, ingrese `firewall –clr all`.
- Para establecer el período de bloqueo de la dirección IP en 60 minutos, ingrese `firewall -iplp 60`.
- Para establecer el número máximo de errores de inicio de sesión en 5 veces, ingrese `firewall -iplf 5`.
- Para eliminar 192.168.100.1 de la lista de bloqueo de direcciones IP, ingrese `firewall -ipbl -del 192.168.100.1`.
- Para eliminar 3fcc:1234::2 de la lista de bloqueo de direcciones IP, ingrese `firewall –ipbl -del 3fcc:1234::2`.
- Para eliminar todas las direcciones IP de bloqueo, ingrese `firewall –ipbl –clrall`.
- Para mostrar todas las direcciones IP de bloqueo, ingrese `firewall –ipbl –show`.

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.

Sintaxis:
```
hashpw [-options]
```

Tabla 27. Opciones de hashpw

Opción	Descripción	Valores
-sw	Estado del conmutador de contraseña de terceros	enabled, disabled
-re	Estado de lectura de contraseña de terceros **Nota:** La lectura puede configurarse si el conmutador está habilitado.	enabled, disabled

Ejemplo:

```
system> hashpw -sw enabled -re enabled
system> users -5 -n guest5 -shp ef92b778bafe771e89245b89ecbc08a44a4e166c06659911881f383d4473e94f - r Administrator
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.

Utilice el comando **ifconfig** para mostrar 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.

Sintaxis:
```
ifconfig [ethernet_number] [-options]
```

Ejemplo:
```
dhcpinfo eth1 -b
```

Tabla 28. Opciones de ifconfig

Opción	Descripción	Valores
-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)
-ghn	Obtener nombre de host de DHCP	disabled, enabled
-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.
-auto	Configuración de autonegociación, que determina si la velocidad de datos y la configuración de red dúplex son configurables	true, false
-vlan	Habilitar o deshabilitar etiquetado VLAN	enabled, disabled
-vlanid	Id. de VLAN	Números entre 1 y 4094.
-r	Velocidad de datos	10, 100, 1000
-d	Modo dúplex	full, half
-m	MTU	Números entre 60 y 1500.

Tabla 28. Opciones de ifconfig (continuación)

Opción	Descripción	Valores
-l	LAA	Formato de dirección MAC. No se permiten direcciones multidifusión (el primer byte debe ser par).
-b	Dirección MAC grabada (solo lectura)	
-dn	Nombre de dominio (solo lectura)	
-ipv6	Estado de IPv6	disabled, enabled
-ipv6static	Estado IPv6 estático	disabled, enabled
-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	Modo DHCP IPv6	enabled, disabled
-sa6	Modo IPv6 sin estado	enabled, disabled
-lla	Dirección de enlace local (solo lectura)	
-ncsi	Selección del puerto NIC NCSI	nic[x]:port[y] **Nota:** Utilice la coma como delimitador si hay dos o más configuraciones.
-nic	Cambiar el modo NIC[1]	shared, dedicated, shared:nic[x][2]
-failover[2]	Modo de conmutación por error	none, shared, shared:nic[x]
-nssync[3]	Sincronización de configuración de red	enabled, disabled
-address_table	Tabla de direcciones IPv6 generadas automáticamente y sus longitudes de prefijo (solo lectura) **Nota:** La opción es visible solo si están habilitado IPv6 y autoconfiguración sin estado.	

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:nic[X] 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.

Ejemplo:

```
system> ifconfig eth0 -c static -i 192.168.70.133
These configuration changes will become active after the next reset of the IMM.
system>
```

Comando keycfg

Utilice este comando para visualizar, añadir o eliminar claves de activación.

Las claves de activación controlan el acceso a funcionalidades opcionales del IMM.

Notas:

- 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.

Sintaxis:

```
keycfg [-options]
```

Tabla 29. Opciones de keycfg

Opción	Descripción	Valores
-add	Añadir clave de activación	ip, pn, u, pw, f • **-ip**: dirección IP del servidor TFTP/SFTP con la clave de activación para añadir • **-pn**: número de puerto del servidor de TFTP/SFTP con la clave de activación a añadir (predeterminado 69/22) • **-u**: nombre de usuario del servidor de SFTP con la clave de activación a añadir • **-pw**: contraseña del servidor de SFTP con la clave de activación a añadir • **-f**: nombre de archivo para la clave de activación que se va a añadir
-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

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.

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.

Sintaxis:
```
ldap [-options]
```

Tabla 30. Opciones de ldap

Opción	Descripción	Valores
-aom	Modo de solo autenticación para los usuarios de Active Directory	enabled, disabled
-a	Método de autenticación del usuario	• **loc**: solo local • **ldap**: solo LDAP • **locld**: primero local y luego LDAP • **ldloc**: primero LDAP y luego local
-b	Método de vinculación	• **anon**: anónimo • **client**: vinculación con ClientDN y contraseña • **login**: 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**
-fn	Nombre del bosque	Para los entornos de Active Directory. Cadena hasta de 127 caracteres.
-f	Filtro del grupo	Cadena de hasta 127 caracteres para **group_filter**
-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.
-r	Nombre distinguido (DN) de entrada raíz	Cadena de hasta 127 caracteres para **root_dn**.
-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**

Tabla 30. Opciones de ldap (continuación)

Opción	Descripción	Valores
-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**
-u	Atributo de búsqueda del nombre de inicio de sesión del usuario	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	

Ejemplo:
```
system> ldap
   -aom enable
   -a   locld
   -b   client
   -c   cn=admin,dc=lenovo,dc=com
   -d
   -fn
   -f   example.com
   -g   cn
   -l   XCC3RBSPermissions
   -r
   -s1ip 10.241.99.94
   -s2ip
   -s3ip
   -s4ip
   -s1pn 389
   -s2pn 389
   -s3pn 389
   -s4pn 389
   -u uid
   -v off
system>
```

Comando ntp

Use este comando para ver y configurar el protocolo de tiempo de red (NTP).

Sintaxis:
```
ntp [-options]
```

Tabla 31. Comando ntp

Opción	Descripción	Valores
-en	Habilita o deshabilita el protocolo de tiempo de red.	enabled, disabled
-i**[x]**	Nombre o dirección IP del servidor del protocolo de tiempo de red para el índice **x**.	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. **Nota:** -i es lo mismo que i1.
-f	La frecuencia (en minutos) que el reloj del 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.

Ejemplo:
```
system> ntp
-en: disabled
-f: 3 minutes
-i: not set
```

Comando portcontrol

Utilice este comando para encender o apagar el puerto de servicio de red.

Sintaxis:
```
portcontrol [-options]
```

Tabla 32. Opciones de portcontrol

Opción	Descripción	Valores
-ipmi	Habilita o deshabilita el acceso IPMI mediante LAN	on, off
-ipmi-kcs	Habilitar bajo demanda, habilitar o deshabilitar el acceso ipmi desde el servidor	auto, on, off
-rest	Habilita o deshabilita la detección REST	on, off
-snmp	Habilita o deshabilita la detección SNMP	on, off
-ssdp	Habilita o deshabilita la detección SSDP	on, off
-cli	Habilita o deshabilita la detección CLI	on, off
-web	Habilita o deshabilita la detección WEB	on, off
-all	Habilitar o deshabilitar todas las interfaces y protocolos de detección	on, off

Ejemplo:

```
system> portcontrol
ipmi : on
ipmi-kcs : on
rest : on
snmp : off
ssdp : on
cli : on
web : on
system>
```

Comando ports

Use este comando para mostrar y configurar los puertos del IMM.

Sintaxis:

```
ports [-options]
```

Tabla 33. Opciones de ports

Opción	Descripción	Valores
-open	Mostrar puertos abiertos (solo lectura)	
-reset	Restablecer los puertos a la configuración predeterminada (solo lectura)	
-http	Número de puerto HTTP	Número de puerto predeterminado: 80
-https	Número de puerto HTTPS	Número de puerto predeterminado: 443
-ssh	Número de puerto CLI heredado de SSH	Número de puerto predeterminado: 22
-snmpa	Número de puerto de agente SNMP	Número de puerto predeterminado: 161
-snmpt	Número de puerto de SNMP traps	Número de puerto predeterminado: 162
-rp	Número de puerto de presencia remota	Número de puerto predeterminado: 3900

Ejemplo:

```
system> ports
  -http 80
  -https 443
  -rp 3900
  -snmpa 161
  -snmpt 162
  -ssh 22
system>
```

Comando rdmount

Utilice este comando para montar imágenes de disco remoto o recursos compartidos de red

Notas:

- Se pueden cargar hasta dos archivos en la memoria de XClarity Controller y montar como medio virtual mediante la característica de RDOC de 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.

Sintaxis:
```
rdmount [-options]
```

Tabla 34. Opciones de rdmount

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.

Sintaxis:
```
restore [-options]
```

Tabla 35. Opciones de restore

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 35. Opciones de restore (continuación)

Opción	Descripción	Valores
-u	Nombre de usuario para el servidor SFTP	Nombre de usuario válido
-pw	Contraseña para el servidor SFTP	Contraseña válida

Ejemplo:
```
system> restore f xcc-back.cli pp xxxxxx ip 192.168.70.200
ok
system>
```

Comando roles

Use este comando para mostrar o configurar los roles.

Sintaxis:
```
roles role_account[3-31] [-options]
```

Tabla 36. Opciones de roles

Opción	Descripción	Valores
-n	Nombre de rol	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 eventos • **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	

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 rtd

Utilice este comando para restaurar todos los valores del BMC al valor predeterminado de fábrica.

Nota: Este comando solía ser en comando **restoredefaults** y **clearcfg**.

Sintaxis:
```
rtd [-options]
```

Tabla 37. Opciones de rtd

Opción	Descripción
-all	Restablezca todos los valores del BMC a los valores predeterminados de fábrica.
-eu	Restablezca todos los valores del BMC a los valores predeterminados de fábrica, excepto la configuración de usuario
-en	Restablezca todos los valores del BMC a los valores predeterminados de fábrica, excepto la configuración de red.
-eun	Restablezca todos los valores del BMC a los valores predeterminados de fábrica, excepto la configuración de usuario y red.

Ejemplo:
```
system> rtd -all

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 seccfg

Utilice este comando para realizar la reversión de firmware.

Sintaxis:
```
seccfg [-options]
```

Tabla 38. Opciones de seccfg

Opción	Descripción	Valor
-fwrb	Permite la reversión del firmware a versiones previas.	enabled, disabled
-aubp	Habilita o deshabilita la función de promoción automática de copia de seguridad a principal.	enabled, disabled

Comando securityinfo

Este comando se utiliza para mostrar información relacionada con la seguridad.

Sintaxis:
```
securityinfo [-options]
```

Tabla 39. Opciones de securityinfo

Opción	Descripción
-event	Mostrar eventos de seguridad.
-cryptomode	Mostrar el estado del modo criptográfico de seguridad.
-service	Mostrar el estado de seguridad de los servicios y puertos.
-cert	Mostrar el estado de seguridad del certificado.
-account	Mostrar el estado de seguridad de las cuentas de usuario.

Comando securitymode

Se utiliza este comando para generar un nuevo archivo de datos de servicio.

Sintaxis:
```
securitymode [-options]
```

Tabla 40. Opciones de securitymode

Opción	Descripción	Valores
-mode	Selecciona el modo de seguridad. • CNSA - Estricto empresarial • FIPS - Estándar • COMPAT - Compatibilidad	CNSA, FIPS, COMPAT • **CNSA**: Solo se permiten los servicios que admiten criptografía de nivel estricto empresarial; requiere la habilitación de la clave de característica bajo demanda. • **FIPS**: Los servicios que requieren criptografía que no admiten la criptografía de nivel estándar están deshabilitados de manera predeterminada. • **COMPAT:** Cuando este modo está habilitado, XCC NO está funcionando en el modo validado estándar; permite habilitar todos los servicios.
-h	Enumere el uso y las opciones.	

Comando set

Utilice este comando para cambiar algunos valores del IMM.

- Algunas configuraciones del 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 41. 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.

Tabla 41. Comando set (continuación)

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 snmp

Use este comando para mostrar y configurar la información de interfaz de SNMP.

Sintaxis:
```
snmp [-options]
```

Tabla 42. Opciones de SNMP

Opción	Descripción	Valores
-a3	Agente de SNMPv3	on, off **Notas:** Para habilitar el agente SNMPv3, se debe cumplir con el siguiente criterio: • El contacto del IMM se especifica con la opción de comando -cn. • La ubicación del IMM se especifica con la opción de comando -l.
-t	Trampas SNMPv3	on, off
-tn	Nombre de usuario de capturas SNMPv3	Nombre de usuario válido
-tauth	Protocolo de autenticación de capturas SNMPv3	none, HMAC-SHA
-tapw	Contraseña de autenticación de capturas SNMPv3	Contraseña válida
-tpriv	Protocolo de privacidad de capturas SNMPv3	none, CBC-DES, AES
-tppw	Contraseña de privacidad de capturas SNMPv3	Contraseña válida
-tix	Dirección IP o nombre de host de la comunidad **x**	Dirección IP o nombre de host válidos (limitado a 63 caracteres, **x** puede variar de 1 a 3). **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 la comunidad al no especificar ningún argumento.

Tabla 42. Opciones de SNMP (continuación)

Opción	Descripción	Valores
-l	Ubicación del 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 del 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 “”.
-t1	Trampas SNMPv1	on, off
-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 “”.
-ci	Dirección IP/nombre de host de la comunidad 1	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 la comunidad al no especificar ningún argumento.
-c1iy	Dirección IP/nombre de host de la comunidad **y**	Dirección IP o nombre de host válidos (limitado a 63 caracteres, **y** puede variar 2 o 3). **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 la comunidad al no especificar ningún argumento.
-t2	Capturas SNMPv2	on, off
-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 “”.

Tabla 42. Opciones de SNMP (continuación)

Opción	Descripción	Valores
-cti	Dirección IP/nombre de host de la comunidad de capturas SNMPv2 1	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)
-send	Enviar información de una captura de prueba	

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.

Sintaxis:

```
snmpalerts [-options]
```

Tabla 43. Opciones de snmpalerts

Opción	Descripción	Valores
-status	Estado de alerta SNMP	on, off
-crt	Establece eventos críticos que envían alertas	all, none, custom:te|vo|po|di|fa|cp|me|in|re|ot|pc 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 eventos críticos • pc: Eventos críticos de PCIe

Tabla 43. Opciones de snmpalerts (continuación)

Opción	Descripción	Valores
-wrn	Establece eventos de advertencia que envían alertas	all, none, custom:rp|te|vo|po|fa|cp|me|ot|pw 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: evento no crítico del ventilador • cp: microprocesador en estado degradado • me: advertencia de memoria • ot: todos los otros eventos de advertencia • pw: eventos de advertencia de PCIe
-sys	Establece eventos de rutina que envían alertas	all, none, custom:lo|tio|ot|po|bf|til|pf|el|ne|nl|dh|oa 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 eventos 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 eventos 75 % lleno • ne: cambio de red • nl: vínculo de NIC del host descendente/ascendente • dh: conexión dinámica de la unidad • oa: todos los demás eventos de auditoría

Comando sshcfg

Use este comando para mostrar y configurar los parámetros de SSH.

Sintaxis:
```
sshcfg [-options]
```

Tabla 44. Opciones de sshcfg

Opción	Descripción	Valores
-cstatus	Estado de SSH CLI	enabled, disabled
-hk	Clave de servidor	gen, all • **gen**: Generar la clave privada del servidor SSH • **all**: Muestra la clave pública del servidor

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 sslcfg

Utilice este comando para visualizar y configurar el SSL para el IMM y gestionar los certificados.

El comando **sslcfg** se usa para generar una nueva clave de cifrado y el certificado autofirmado o solicitud de firma de certificado (CSR).

Sintaxis:

```
sslcfg [-options]
```

Tabla 45. Opciones de sslcfg

Opción	Descripción	Valores
-server	Estado de web sobre HTTPS	enabled, disabled **Notas:** • Web sobre HTTPS solo se puede habilitar si existe un certificado. • Utilice **-rm** para deshabilitar por completo el certificado.
-client	Estado de LDAP seguro	enabled, disabled **Nota:** El cliente SSL puede habilitarse solo si hay un servidor o certificado de cliente válido establecido.
-cert	Generar certificado autofirmado	server, client, 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.
-csr	Generar una CSR	server, client, 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.
-form	Formato de la CSR o certificado que se exportará.	der, pem (predeterminado pem)

Tabla 45. Opciones de sslcfg (continuación)

Opción	Descripción	Valores
-algo	Algoritmo de CSR	p256, p384, rsa2048, rsa3072, rsa4096 **Nota:** Se establecerá un valor predeterminado (p256) si no hay una opción -algo.
-rm	Quitar el certificado	server, storekey **Nota:** Un certificado autofirmado predeterminado (servidor) se generaría automáticamente después de eliminar el actual.
-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	Exporta el archivo especificado al host remoto	Esta opción no toma ningún argumento, pero se debe utilizar con **-cert** o **-csr**; así como con las opciones de comando **-i** y **-l**.
-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	import, download, remove **Nota:** El número de certificado de confianza, **x**, se especifica como entero entre 1 y 4 en la opción de comando.
Opciones necesarias para generar un certificado autofirmado o CSR **Nota:** Requerido al generar un certificado autofirmado o una CSR.		
-c	País	Código de país (2 letras)
-sp	Estado o provincia	Cadena entre comillas (máximo de 60 caracteres)
-cl	Ciudad o localidad	Cadena entre comillas (máximo de 50 caracteres)
-on	Nombre de la organización	Cadena entre comillas (máximo de 60 caracteres)
-hn	Nombre de host del BMC	Cadena (máximo de 60 caracteres)
Opciones opcionales para generar un certificado autofirmado o CSR **Nota:** Opcional al generar un certificado autofirmado o una CSR.		
-cp	Persona de contacto	Cadena entre comillas (máximo de 60 caracteres)
-ea	Dirección de correo electrónico de la persona de contacto	Dirección de correo electrónico válida (máximo de 60 caracteres)
-ou	Unidad organizativa	Cadena entre comillas (máximo de 60 caracteres)
-s	Apellido	Cadena entre comillas (máximo de 60 caracteres)
-gn	Nombre	Cadena entre comillas (máximo de 60 caracteres)

Tabla 45. Opciones de sslcfg (continuación)

Opción	Descripción	Valores
-in	Iniciales	Cadena entre comillas (máximo de 20 caracteres)
-dq	Calificador de nombre de dominio	Cadena entre comillas (máximo de 60 caracteres)
Opciones opcionales para generar una CSR **Nota:** Opcional a generar una CSR.		
-cpwd	Contraseña de desafío	Cadena (mínimo de 6 caracteres y máximo de 30 caracteres)
-un	Nombre no estructurado	Cadena entre comillas (máximo de 60 caracteres)

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 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 LNV -hn XCC-5cf3fc -cp Contact -ea "" -ou""
  ok
  ```

- 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 LNV -hn XCC-5cf3fc -cp Contact -ea "" -ou "
  ok
  ```

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 syslock

Use este comando para mostrar y configurar los valores de bloqueo del sistema.

Sintaxis:

```
syslock [-options]
```

Tabla 46. Opciones de syslock

Opción	Descripción	Valores
-en	Habilite o deshabilite la función de bloqueo de configuración del sistema. **Nota:** Habilitar con la opción **-e** puede promover el inventario actual como una instantánea de confianza.	enabled, disabled
-e	Habilite los valores de bloqueo de configuración con o sin aplicar el inventario actual en una instantánea de confianza. **Nota:** Se establecerá un valor predeterminado si no hay una opción **-e**.	enabled, disabled
-l **[x]**	Enumere el inventario de una instantánea específica en el índice **x**.	El número de índice, x, se especifica como un número entero en la opción de comando.
-m	Tome una instantánea manual.	
-d	Descripción de la instantánea manual.	Cadena de hasta 32 caracteres.
-c	Enumere la diferencia de inventario con respecto a la instantánea de confianza.	
-po	Establezca la directiva de bloqueo. **Nota:** La acción impedirá el arranque del servidor si la protección del sistema se encuentra en un estado no conforme.	none, osboot, pperm
-cpu	Establezca el bloqueo de la cpu.	on, off
-dimm	Establezca el bloqueo de dimm.	on, off
-pci	Establecer el bloqueo de pci.	on, off
-drive	Establezca el bloqueo de la unidad.	on, off
-riser	Establezca el bloqueo de la expansión.	on, off
-bp	Establezca el bloqueo de bp.	on, off

Comando thermal

Utilice este comando para visualizar y configurar la directiva de modo térmico del sistema host.

Ejecutar el comando **thermal** sin opciones muestra la directiva de modo térmico. En la tabla siguiente se muestran los argumentos para las opciones.

Sintaxis:
```
thermal [-options]
```

Tabla 47. Opciones de thermal

Opción	Descripción	Valores
-mode	Muestra la directiva del modo térmico y configura la tabla térmica de los sistemas host (solo lectura)	• Informática general - Eficiencia energética • Informática general - Frecuencia máxima • Informática general - Rendimiento máximo • Virtualización - Eficiencia energética • Virtualización - Rendimiento máximo • Base de datos - Procesamiento de transacciones • Baja latencia • Informática de alto rendimiento • Personalizado • Desconocido
-table **table_number**	**table_number** especifica qué tabla térmica alternativa se va a utilizar.	1 = Bajo: ligero aumento de la velocidad del ventilador 2 = Medio: aumento moderado de la velocidad del ventilador 3 = Alto: gran aumento de la velocidad del ventilador 0 = Normal: sin aumento de la velocidad del ventilador

Ejemplo:
```
system> thermal
-mode normal
-table 80860126 1 10DE0DFA 3
system>
```

Comando tls

Utilice este comando para establecer el nivel mínimo de TLS.

Sintaxis:
```
tls [-options]
```

Tabla 48. Opciones de tls

Opción	Descripción	Valores
-min	Seleccione el nivel mínimo de TLS	1.2, 1.3 **Nota:** Cuando la modalidad de criptografía está definida en modo de conformidad de NIST-800-131A, la versión de TLS debe establecerse en 1.2.
-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.		

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.

Sintaxis:
```
trespass [-options]
```

Tabla 49. Opciones de trespass

Opción	Descripción
-s	Configurar mensajes de advertencia de intrusión
-h	Enumera el uso y las opciones

Ejemplo:
```
system> trespass -s testingmessage
ok
system> trespass
testingmessage
system>
system> trespass -s "testing message"
ok
system> trespass
testing message
system>
```

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.

Sintaxis:
```
uefipw [-options]
```

Tabla 50. Opciones de uefipw

Opción	Descripción
-cp	Contraseña actual (limitada a 20 caracteres)
-p	Nueva contraseña (limitada a 20 caracteres)

Comando usbeth

Use este comando para habilitar o deshabilitar la interfaz en banda de LAN sobre USB.

Notas:

- 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.
- 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.

Sintaxis:
```
usbeth [-options]
```

Tabla 51. Opciones de usbeth

Opción	Descripción	Valores
-en	Habilite o deshabilite la interfaz en banda (Ethernet sobre USB).	enabled, disabled
-am	Seleccione el modo de dirección IPv4 o IPv6 LLA.	ipv4, ipv6lla
Nota: Las opciones -ip, -sn y -ipos solo son válidas cuando se selecciona el modo -am ipv4		
-ip	Dirección IP de la interfaz Ethernet sobre USB para BMC.	Dirección IP válida
-sn	Máscara de subred de interfaz Ethernet sobre USB para BMC.	Dirección IP válida
-ipos	Dirección IP de la interfaz Ethernet sobre USB para el SO.	Dirección IP válida

Ejemplo:
```
system> usbeth
-en : disabled
system> usbeth -en enabled
ok
system> usbeth
-en : disabled
system>
```

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.

Sintaxis:
```
users [-user_index] [-options]
```

Tabla 52. Opciones de users

Opción	Descripción	Valores
-user_index	Número de índice de cuenta de usuario.	Donde **user_index** es 1 a 12 (inclusive) o **all** para todos los usuarios.
-l	Mostrar los días de caducidad de la contraseña	
-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 255 caracteres. Null crea una cuenta sin contraseña que el usuario debe establecer durante el primer inicio de sesión.
-shp	Establecer contraseña hash	Total 64 caracteres
-ssalt	Establecer salt	Limitado a 64 caracteres
-ghp	Obtener hashpassword	
-gsalt	Obtener salt	
-ep	Contraseña de cifrado (para copia de seguridad/ restauración)	Contraseña válida
-esalt	salt para contraseñas cifradas	Solo para copia de seguridad o restauración
-r	Nombre de rol	Administrador, Operador, ReadOnly. Como se indica en el comando “Comando roles” en la página 123.
-clear	Borra la cuenta de usuario especificada	Se debe especificar el número de índice de la cuenta de usuario a borrar, siguiendo la forma: `users -clear -user_index` **Nota:** 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.
-curr	Muestra los usuarios actualmente conectados	
-ai	Interfaz accesible para el usuario	web, ssh, redfish, ipmi, snmp, all **Nota:** Se establecerá un valor predeterminado (web|ssh|redfish) si no hay una opción -ai.
-sauth	Protocolo de autenticación SNMPv3	None, HMAC_MD5, HMAC_SHA96, HMAC128_SHA224, HMAC192_ SHA256, HMAC256_SHA384, HMAC384_SHA512
-spriv	Protocolo de privacidad SNMPv3	Ninguno, CBC_DES, CFB128_AES128, AES192, AES256, AES192C, AES256C
-spw	Contraseña de privacidad SNMPv3	Contraseña válida
-sepw	Contraseña de privacidad SNMPv3 (cifrada)	Contraseña válida

Tabla 52. Opciones de users (continuación)

Opción	Descripción	Valores
-sacc	Tipo de acceso de SNMPv3	get
-strap1	Nombre de host de capturas SNMPv3 1	Nombre de host válido
-strap2	Nombre de host de capturas SNMPv3 2	Nombre de host válido
-strap3	Nombre de host de capturas SNMPv3 3	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.
Las siguientes opciones se utilizan junto con -pk		
-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`.
-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` para todas las claves asignadas al usuario. **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 -remove -1`.
-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=="`

Tabla 52. Opciones de users (continuación)

Opción	Descripción	Valores
-upld	Cargue una clave pública SSH en formato OpenSSH o RFC4716 **(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`.
-dnld	Descargue la clave pública SSH especificada en un servidor TFTP/SFTP **(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`.
-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`.

Tabla 52. Opciones de users (continuación)

Opción	Descripción	Valores
-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."`.

Ejemplo:

```
system> users
 Login ID     Name      Advanced Attribute     Role            Password Expires
 --------     ----      ------------------     ------          ----------------
    1         USERID                Native     Administrator          89 day(s)
system> users -2 -n sptest -p PasswOrd12 -r Administrator
The user is required to change the password when the user logs in to the management server for the first time
ok
system> users
 Login ID     Name      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 -r  Admini
system> users -5 ghp
292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee
system> users -5 gsalt
abc
system>
```

Comandos de control del IMM

Este tema proporciona una lista alfabética de los comandos CLI de control del IMM.

Actualmente, hay 7 comandos de control del IMM:

Comando batch

Utilice este comando para ejecutar uno o varios comandos CLI en un archivo.

Notas:

- 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.

Sintaxis:

```
batch [-options]
```

Tabla 53. Opciones de batch

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

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 clock

Use este comando para mostrar la fecha y hora actual. Puede establecer el ajuste de UTC y los valores de horario de verano.

Sintaxis:
```
clock [-options]
```

Tabla 54. Opciones de clock

Opción	Descripción	Valores
-u	Ajuste de 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).
-dst	Horario de verano	on, off, caso especial
-host	Formato de la hora obtenida del host (por defecto: utc)	local, utc **Nota:** Los sistemas Windows usan local, Linux usa utc

Notas:

- 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.

Ejemplo:
```
system> clock
12/12/2011 13:15:23 GMT-5:00 dst on
```

Comando info

Use este comando para mostrar y configurar información sobre el BMC.

Sintaxis:
```
info [-options]
```

Tabla 55. Opciones de info

Opción	Descripción	Valores
-name	Nombre del BMC	Cadena
-contact	Nombre de la persona de contacto del BMC	Cadena
-location	Ubicación del BMC	Cadena
-postal	Dirección postal completa del BMC	Cadena
-room	Identificador de sala del BMC	Cadena
-rack	Identificador de bastidor del BMC	Cadena
-rup	Posición del BMC en el bastidor	Cadena

Ejemplo:
```
system> info
  -name: BMCName
  -location: location
  -contact: contact
  -rack: rack
  -room: room
  -postal: postal
  -rup: 1
system>
```

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.

Sintaxis:
```
spreset
```

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.

Sintaxis:
```
storage [-options]
```

Tabla 56. Opciones de storage

Opción	Descripción	Valores
-list	Enumera los destinos de almacenamiento gestionados por el IMM.	**controllers|pools|volumes|drives** • 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 **destinos de almacenamiento** -target **target_id**	Enumera los **destinos** de almacenamiento gestionados por el IMM de acuerdo con el **target_id**.	**pools|volumes|drives** y **ctrl[x]|pool[x]** Donde **destinos de almacenamiento** y **target_id** son: • **pools** y **ctrl[x]**: enumera los grupos de almacenamiento asociados con el controlador RAID, según el target_id[1] • **volumes** y **ctrl[x]|pool[x]**: enumera los volúmenes de almacenamiento asociados con el controlador RAID, según el target_id[1] • **drives** y **ctrl[x]|pool[x]**: enumera las unidades de almacenamiento asociadas con el controlador RAID, según el target_id[1]
-list devices	Muestra el estado de todos los discos 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]**[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]**[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]**[2]
-showinfo **nvme**	Muestra la información de firmware del disco NVMe.	

Tabla 56. Opciones de storage (continuación)

Opción	Descripción	Valores
-wthre show	Muestra el umbral de desgaste de SSD crítico y de advertencia.	Valor del umbral (de 1 a 99)
-wthre -ct **valor del umbral**	Establezca el umbral crítico de desgaste de SSD.	Valor del umbral (de 1 a 99)
-wthre -wt **valor del umbral**	Establezca el umbral de advertencia de desgaste de SSD.	Valor del umbral (de 1 a 99) **Nota:** El valor de advertencia debe ser mayor que el crítico.
-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 ctrl -bootdevice -vd **volumen** -target **target_id**	Establezca el dispositivo de arranque por volumen.	Donde **target_id** es **ctrl[x]** y **volumen** es un valor en la primera columna de la salida “list volumes”.
-config ctrl -bootdevice -pd **unidad** -target **target_id**	Establezca el dispositivo de arranque por unidad.	Donde **target_id** es **ctrl[x]** y **unidad** es un valor en la primera columna de la salida “list drives”.
-config ctrl -bootdevice -index **index** -target **target_id**	Establezca el dispositivo de arranque por índice.	Donde **target_id** es **ctrl[x]** y **index** es un valor en “[]” que es el resultado de la opción “display”.
-config ctrl -bootdevice -display -target **target_id**	Mostrar dispositivo iniciable.	
-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]

Tabla 56. Opciones de storage (continuación)

Opción	Descripción	Valores
-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 (varias unidades de disco) a una unidad en buen estado sin configurar.	Donde **target_id** es **disk[x]**[5]
-config drv -mkjbod -target **target_id**[3]	Configura la unidad no configurada como varias unidades de disco.	Donde **target_id** es **disk[x]**[5]
-config drv -rebuild -target **target_id**[3]	Inicie la reconstrucción de la unidad.	Donde **target_id** es **disk[x]**[5]
-config drv -addhsp -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 -dedicated pools -target **target_id**[3]	Asigne la unidad como repuesto dinámico dedicado a los grupos de almacenamiento seleccionados.	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]
-config vol -remove -target**target_id**[3]	Quita un volumen.	Donde **target_id** es **vol[x]**[5]

Tabla 56. Opciones de storage (continuación)

Opción	Descripción	Valores
-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|3>**] es la directiva de escritura de memoria caché: – Escriba **0** para la directiva Escritura directa – Escriba **1** para la directiva de escritura protegida – Escriba **2** para la directiva de escritura no protegida – Escriba **3** para sin directiva • [-r **<0|1>**] es la directiva de lectura de la memoria caché: – Escriba **0** para la directiva Sin lectura anticipada – Escriba **1** para la directiva Lectura anticipada • [-i **<0|1>**] es la directiva de E/S de la memoria caché: – Escriba **0** para la directiva E/S directa – Escriba **1** para la directiva E/S en memoria caché • [-a **<0|2|3>**] es la directiva de acceso: – Escriba **0** para la directiva Lectura de escritura – Escriba **2** para la directiva Solo lectura – Escriba **3** para la directiva Bloqueada • [-d **<0|1|2>**] es la directiva de memoria caché del disco: – Escriba **0** si la directiva no tiene cambios – Escriba **1** para habilitar la directiva[6] – Escriba **2** para deshabilitar la directiva • [-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]
-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>**] 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

Tabla 56. Opciones de storage (continuación)

Opción	Descripción	Valores
		• [-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|3>**] es la directiva de escritura de memoria caché: – Escriba **0** para la directiva Escritura directa – Escriba **1** para la directiva de escritura protegida – Escriba **2** para la directiva de escritura no protegida – Escriba **3** para sin directiva • [-r **<0|1>**] es la directiva de lectura de la memoria caché: – Escriba **0** para la directiva Sin lectura anticipada – Escriba **1** para la directiva Lectura anticipada
-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 directiva de E/S de la memoria caché: – Escriba **0** para la directiva E/S directa – Escriba **1** para la directiva E/S en memoria caché • [-a **<0|2|3>**] es la directiva de acceso: – Escriba **0** para la directiva Lectura de escritura – Escriba **2** para la directiva Solo lectura – Escriba **3** para la directiva Bloqueada • [-d **<0|1|2>**] es la directiva de memoria caché del disco: – Escriba **0** si la directiva se mantiene igual – Escriba **1** para habilitar la directiva[6] – Escriba **2** para deshabilitar la directiva • [-f **<0|1|2>**] es el tipo de inicialización: – 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, 512B, 4K, 128K, 1M, etc. • -target **target_id** es: – **ctrl[x]** (nuevo grupo de almacenamiento)[5] – **pool[x]** (grupo de almacenamiento existente)[5]

Tabla 56. Opciones de storage (continuación)

Opción	Descripción	Valores
-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>**] 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]
-fgi **vol[idx]**	Inicialización rápida de los volúmenes especificados	Donde **vol[idx]** es **vol[id1],vol[id2]:..**
-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.

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 pools
pool[0-0]    Storage Pool 0
pool[0-1]    Storage Pool 1
system>
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.: 1234567890
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]    Storage Pool 0
pool[0-1]    Storage 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 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.

Sintaxis:
```
adapter [-options]
```

Tabla 57. Opciones de adapter

Opción	Descripción	Valores
-list	Enumera todos los adaptadores PCIe en el servidor.	
-show **target_id**	Muestra información detallada del adaptador PCIe de destino.	**target_id [info|firmware|ports]** 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

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.
```

Nota: Si elimina, sustituye o configura adaptadores, debe reiniciar el servidor (al menos una vez) para ver la información actualizada del adaptador.

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>
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
system>
```

Comandos de soporte

Este tema proporciona una lista alfabética de los comandos de soporte.

Existe solo un comando de soporte: “Comando dbgshbmc” en la página 154.

Comando dbgshbmc

Utilice este comando para desbloquear el acceso de red a la depuración segura de carcasa.

Nota: Este comando solía ser el comando **dbgshimm**.

Importante: Este comando está diseñado solo para el uso del personal de soporte.

En la tabla siguiente se muestran los argumentos para las opciones.

Sintaxis:
```
dbgshbmc [subset_command]
```

Tabla 58. Comandos de subconjunto dbgshbmc

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 de 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 a 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 157.

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 157.

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

Obtención/definición de 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 de alojamiento Flex y ThinkSystem D2 (nodo de cálculo ThinkSystem SD530), la configuración de negociación automática no se puede cambiar porque podría interrumpir 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	Obtención/definición de 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	Obtención/definición de 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 = 0x2E</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 Null.</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>

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/xcc3/nn1ia_c_servicesandsupport.html.
  - Para obtener más información sobre el uso de la CLI para recopilar datos del servicio, consulte https://pubs.lenovo.com/xcc3/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 59. 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

CH

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

X