Lenovo XClarity Management Hub
Guía del usuario y de instalación

Versión 2.1

Nota

Antes de usar esta información y el producto al cual está asociada, lea los avisos legales y generales en la documentación en línea de XClarity Orchestrator.

Segunda edición (Julio 2024)

Contenido

Capítulo 1. Planificación para Lenovo XClarity Management Hub

Revise las consideraciones y requisitos siguientes, que le ayudarán a planificar la instalación de Lenovo XClarity Management Hub.

Hardware y software admitidos

Asegúrese de que su entorno cumpla con los requisitos de hardware y software para Lenovo XClarity Management Hub.

Sistemas host

Requisitos de hipervisor

Se admiten los siguientes hipervisores para instalar Lenovo XClarity Management Hub.
- VMware ESXi 7.0, U1, U2 y U3
- VMware ESXi 6.7, U1, U2[1] y U3

Para VMware ESXi, el dispositivo virtual es una plantilla OVF.

Importante:

- Para VMware ESXi 6.7 U2, debe utilizar la imagen ISO VMware-ESXi-6.7.0.update02-13981272-LNV-20190630.iso o posterior.

Requisitos de hardware

En la tabla siguiente se enumeran las configuraciones *recomendadas mínimas* para XClarity Management Hub según el número especificado de dispositivos de cliente perimetral gestionados. Dependiendo del entorno, puede que se necesiten recursos adicionales para obtener un rendimiento óptimo.

Número de dispositivos de cliente perimetral gestionados	Procesadores	Memoria	Almacenamiento
0 a 100 dispositivos	6	32 GB	340 GB
100 a 200 dispositivos	8	34 GB	340 GB
200 a 400 dispositivos	10	36 GB	340 GB
400 a 600 dispositivos	12	40 GB	340 GB
600 a 800 dispositivos	14	44 GB	340 GB
800 a 1000 dispositivos	16	48 GB	340 GB

1. Esta es la cantidad mínima de almacenamiento que debe usar el dispositivo virtual del XClarity Management Hub como almacén de datos de SSD.

Requisitos de software

XClarity Management Hub requiere el siguiente software.

- **Servidor NTP**. Se necesita un servidor de protocolo de tiempo de red (NTP) para asegurarse de que las marcas de tiempo de todos los sucesos y alertas que se reciben desde los gestores de

dispositivos y dispositivos gestionados se sincronicen con XClarity Management Hub. Asegúrese de que se pueda acceder a dicho servidor mediante la red de gestión (normalmente, la interfaz Eth0).

Dispositivos gestionables

XClarity Management Hub puede gestionar, supervisar y aprovisionar un máximo de 10,000 dispositivos de cliente ThinkEdge (sin controladores de gestión de la placa base).

Encontrará una lista completa de los dispositivos del cliente ThinkEdge y opciones compatibles (como E/S, DIMM y adaptadores de almacenamiento), los niveles de firmware mínimos requeridos y las consideraciones de limitaciones en Servidores XClarity Management Hub.

Para obtener información general sobre las configuraciones del hardware y las opciones para un dispositivo específico, consulte la Página web de Lenovo Server Proven.

Navegadores web

La interfaz web XClarity Management Hub funciona con los siguientes navegadores web.
- Chrome 80.0 o posterior
- Firefox ESR 68.6.0 o posterior
- Microsoft Edge 40.0 o posterior
- Safari 13.0.4 o posterior (se ejecuta en macOS 10.13 o posterior)

Firewall y servidores proxy

Algunas funciones de servicio y soporte, como Llamar a casa y el estado de la garantía, requieren acceso a Internet. Si tiene firewalls en su red, configúrelos para habilitar el servidor XClarity Orchestrator y los gestores de recursos para realizar estas operaciones. Si Lenovo XClarity Orchestrator y los gestores de recursos no tienen acceso a Internet, configúrelos para que utilicen un servidor proxy.

Firewalls

Asegúrese de que los siguientes nombres y puertos de DNS estén abiertos en el firewall para XClarity Orchestrator y los gestores de recursos aplicables (Lenovo XClarity Management Hub 2.0, Lenovo XClarity Management Hub y Lenovo XClarity Administrator), según proceda. Cada DNS representa un sistema distribuido geográficamente con una dirección IP dinámica.

Nota: Las direcciones IP están sujetas a cambio. Utilice nombres DNS cuando sea posible.

Nombre DNS	Puertos	Protocolos
Descargue actualizaciones (actualizaciones del servidor de gestión, actualizaciones de firmware, UpdateXpress System Packs (controladores de dispositivos del SO) y paquetes de repositorio)		
download.lenovo.com	443	https
support.lenovo.com	443 y 80	https y http
Envíe datos de servicio a Soporte de Lenovo (Llamar a casa) – Solo XClarity Orchestrator		
soaus.lenovo.com	443	https
esupportwebapi.lenovo.com (XClarity Orchestrator v2.0 y posterior) rsgw-eservice.motorola.com (XClarity Orchestrator v1.6) supportwebapi.lenovo.com:443/luf.luf-web.prd/BLL/Logupload.ashx (XClarity Orchestrator v1.5 y anterior)	443	https
Envíe datos periódicos a Lenovo – Solo XClarity Orchestrator		

Nombre DNS	Puertos	Protocolos
esupportwebapi.lenovo.com (XClarity Orchestrator v2.0 y posterior) rsgw-eservice.motorola.com (XClarity Orchestrator v1.6) supportwebapi.lenovo.com:443/luf.luf-web.prd/BLL/uploadSnapshot.ashx (XClarity Orchestrator v1.5 and earlier)	443	https
Recupere la información de garantía		
supportapi.lenovo.com	443	https y http

Servidor proxy

Si XClarity Orchestrator o los gestores de recursos no tienen acceso directo a Internet, asegúrese de que estén configurados para usar un servidor proxy HTTP (consulte Configuración de la reden la documentación en línea de XClarity Orchestrator).

- Asegúrese de que el servidor proxy esté configurado para utilizar autenticación básica.
- Asegúrese de que el servidor proxy esté configurado como un proxy no de terminación.
- Asegúrese de que el servidor proxy esté configurado como un proxy de reenvío.
- Asegúrese de que los balanceadores de carga estén configurados para mantener las sesiones con un servidor proxy y no conmutar entre ellos.

Atención: XClarity Management Hub debe tener acceso directo a Internet. Actualmente, no se admite un servidor proxy HTTP.

Disponibilidad de puertos

Lenovo XClarity Orchestrator y los gestores de recursos requieren que determinados puertos estén abiertos para facilitar la comunicación. Si los puertos necesarios están bloqueados o se utilizan en otro proceso, puede que algunas funciones no funcionen correctamente.

XClarity Orchestrator, Lenovo XClarity Management Hub 2.0, Lenovo XClarity Management Hub y Lenovo XClarity Administrator son aplicaciones RESTful que se comunican de forma segura a través de TCP en el puerto 443.

XClarity Orchestrator

XClarity Orchestrator escucha y responde a través de los puertos que se enumeran en la tabla siguiente. Si XClarity Orchestrator y todos los recursos gestionados se rigen por un firewall y tiene pensado acceder a estos recursos a través de un navegador que está *fuera* del firewall, asegúrese de que los puertos necesarios estén abiertos.

Nota: XClarity Orchestrator puede configurarse opcionalmente para realizar conexiones de salida a servicios externos, como LDAP, SMTP o syslog. Estas conexiones pueden requerir puertos adicionales que generalmente son configurables y no están incluidos en la lista de usuarios. También es posible que estas conexiones requieran acceso a un servidor de servicio de nombre de dominio (DNS) en el puerto TCP o UDP 53 para resolver los nombres de servidor externo.

Servicio	Salida (puertos abiertos en sistemas externos)	Entrada (puertos abiertos en el dispositivo XClarity Orchestrator)
Dispositivo XClarity Orchestrator	• DNS: TCP/UDP en el puerto **53**	• HTTPS: TCP en el puerto **443**
Servidor de autenticación externo	• LDAP: TCP en el puerto **389**[1]	No aplicable

Servicio	Salida (puertos abiertos en sistemas externos)	Entrada (puertos abiertos en el dispositivo XClarity Orchestrator)
Servicios de reenvío de sucesos	• Servidor de correo electrónico (SMTP): UDP en el puerto **25**[1] • Servicio Web REST (HTTP): UPD en el puerto **80**[1] • Splunk – UDP en el puerto **8088**[11], **8089**[1] • Syslog: UDP en el puerto **514**[1]	No aplicable
Servicios de Lenovo (incluyendo Llamar a casa)	• HTTPS (Llamar a casa): TCP en el puerto **443**	No aplicable

1. Este es el puerto predeterminado. Puede configurar este puerto desde la interfaz de usuario de XClarity Orchestrator.

XClarity Management Hub 2.0

Lenovo XClarity Management Hub 2.0 requiere que algunos puertos estén abiertos para facilitar la comunicación. Si los puertos necesarios están bloqueados o se utilizan en otro proceso, puede que algunas funciones del concentrador de gestión no funcionen correctamente.

Si los dispositivos se rigen por un firewall y tiene pensado gestionar estos dispositivos desde un concentrador de gestión que está fuera de ese firewall, debe asegurarse de que todos los puertos implicados en las comunicaciones entre el concentrador de gestión y el controlador de gestión de la placa base de cada dispositivo gestionado estén abiertos.

Servicio o componente	Salida (puertos abiertos a sistemas externos)	Entrada (puertos abiertos en dispositivos de destino)
XClarity Management Hub 2.0	• DNS: UDP en el puerto **53** • NTP: UDP en el puerto **123** • HTTPS: TCP en el puerto **443** • SSDP: UDP en el puerto **1900** • DHCP: UDP en el puerto **67**	• HTTPS: TCP en el puerto **443** • Implementación de SSDP: UDP en los puertos **32768**-**65535**
Servidores ThinkSystem y ThinkAgile	• HTTPS: TCP en el puerto **443** • Detección de SSDP: UDP en el puerto **1900**	• HTTPS: TCP en el puerto **443**

XClarity Management Hub

XClarity Management Hub escucha y responde a través de los puertos que se enumeran en la tabla siguiente.

Servicio o componente	Salida (puertos abiertos en sistemas externos)	Entrada (puertos abiertos en el dispositivo XClarity Management Hub)
Dispositivo XClarity Management Hub[1]	• DNS: TCP/UDP en el puerto **53**[2]	• HTTPS: TCP en el puerto **443** • MQTT: TCP en el puerto **8883**
Dispositivos del cliente ThinkEdge[3]	No aplicable	• MQTT: TCP en el puerto **8883**

1. Cuando se utiliza XClarity Management Hub para gestionar dispositivos a través de XClarity Orchestrator, algunos puertos deben estar abiertos para facilitar la comunicación. Si los puertos

necesarios están bloqueados o se utilizan en otro proceso, puede que algunas funciones de XClarity Orchestrator pueden no funcionar correctamente.

2. XClarity Management Hub puede configurarse opcionalmente para realizar conexiones de salida a servicios externos. También es posible que estas conexiones requieran acceso a un servidor de servicio de nombre de dominio (DNS) en el puerto TCP o UDP 53 para resolver los nombres de servidor externo.
3. Si los dispositivos gestionables se rigen por un firewall y tiene pensado gestionar estos dispositivos desde un XClarity Management Hub que está fuera de ese firewall, debe asegurarse de que todos los puertos implicados en las comunicaciones entre XClarity Management Hub y los dispositivos perimetrales estén abiertos.

XClarity Administrator

Cuando se utiliza Lenovo XClarity Administrator para gestionar dispositivos a través de Lenovo XClarity Orchestrator, algunos puertos deben estar abiertos para facilitar la comunicación. Si los puertos necesarios están bloqueados o se utilizan en otro proceso, puede que algunas funciones de XClarity Orchestrator no funcionen correctamente.

Para obtener información sobre los puertos que se deben abrir para XClarity Administrator, consulte Disponibilidad de puertos en la documentación en línea de XClarity Administrator.

Consideraciones de red

Puede configurar Lenovo XClarity Management Hub para que utilice una única interfaz de red (eth0) o dos interfaces de red separadas (eth0 y eth1) para la comunicación.

Lenovo XClarity Management Hub se comunica a través de las redes siguientes.

- La *red de gestión* se utiliza para las comunicaciones entre Lenovo XClarity Management Hub y dispositivos gestionados.
- La *red de datos* se utiliza para las comunicaciones entre los sistemas operativos que están instalados en los servidores y la intranet de la empresa, Internet o ambos.

Interfaz única (eth0)

Cuando se utiliza una única interfaz de red (eth0), las comunicaciones de gestión, las comunicaciones de datos y el despliegue de sistemas operativos se producen en la misma red.

Al configurar Lenovo XClarity Management Hub, debe definir la interfaz de red eth0 teniendo en cuenta las siguientes consideraciones.

- La interfaz de red debe estar configurada para que admita la detección y gestión de dispositivos (incluidas las actualizaciones de firmware). Lenovo XClarity Management Hub debe poder comunicarse con todos los dispositivos que gestionará desde la red de gestión.Lenovo XClarity Management Hub debe poder comunicarse con todos los dispositivos que gestionará desde la red.
- Para desplegar imágenes de SO, la interfaz eth0 debe tener la conectividad de red IP hacia la interfaz de red del servidor que se usa para acceder al sistema operativo del host.
- **Importante:** Implementar una red de datos y gestión compartida puede provocar interrupciones en el tráfico; por ejemplo, puede que se descarten paquetes o que se produzcan problemas de conectividad de red de gestión, según su configuración de red (por ejemplo, si el tráfico de los servidores tiene una prioridad alta y el tráfico de los controladores de gestión tiene una prioridad baja). La red de gestión utiliza el tráfico UDP, además de TCP. El tráfico UDP puede tener una prioridad más baja cuando el tráfico de red es alto.

Dos interfaces separadas (eth0 y eth1)

Al utilizar dos interfaces de red (eth0 y eth1), puede configurar las redes como redes separadas físicamente o separadas virtualmente.

Revise las consideraciones siguientes al definir las interfaces de red eth0 y eth1.

- La interfaz de red eth0 debe estar conectada a la red de gestión y debe estar configurada para que admita la detección y gestión de dispositivos. Lenovo XClarity Management Hub debe poder comunicarse con todos los dispositivos que gestionará desde la red de gestión.
- La interfaz de red eth1 se puede configurar para que se comunique con una red de datos interna, con una red de datos pública o ambas.
- Para desplegar imágenes del sistema operativo, la interfaz de red eth1 debe tener conectividad de red IP hacia la interfaz de red del servidor que se utiliza para acceder al sistema operativo del host.
- Las funciones se pueden realizar en cualquiera de las redes.
- Para redes separadas virtualmente, los paquetes de la red de gestión y de la red de datos se envían mediante la misma conexión física. Use el etiquetado VLAN en todos los paquetes de datos de la red de gestión para mantener separado el tráfico entre las dos redes.

Consideraciones sobre la dirección IP

Revise las siguientes consideraciones sobre la dirección IP antes de configurar la red.

- Cambiar la dirección IP del dispositivo virtual una vez que XClarity Management Hub está en funcionamiento causará problemas de conectividad con XClarity Orchestrator y con todos los dispositivos gestionados. Si necesita cambiar la dirección IP, desconecte XClarity Management Hub de XClarity Orchestrator y anule la gestión de todos los dispositivos gestionados antes de cambiar la dirección IP y, a continuación, vuelva a gestionar los dispositivos y vuelva a conectar XClarity Management Hub a XClarity Orchestrator una vez completado el cambio de dirección IP.
- configure los componentes de los dispositivos de forma que minimicen los cambios de dirección IP. Plantéese la posibilidad de utilizar direcciones IP estáticas en lugar del protocolo de configuración dinámica de host (DHCP). Si se utiliza DHCP, asegúrese de que los cambios de dirección IP se minimicen, como basar la dirección DHCP en una dirección MAC o configurar DHCP para que la concesión no caduque.Si cambia la dirección IP de un dispositivo gestionado (que no sea un dispositivo del cliente ThinkEdge), debe anular la gestión del dispositivo y, a continuación, volver a gestionarlo.
- La traducción de dirección de red (NAT), que reasigna el espacio de una dirección IP en otro, no se admite.
- Las interfaces de red se deben configurar con una dirección IPv4 para gestionar los dispositivos siguientes. No se admiten las direcciones IPv6.
  - Servidores ThinkServer
  - Dispositivos Lenovo Storage
- No se admite la gestión de dispositivos de RackSwitch mediante IPv6 enlace local a través de un puerto de datos o de gestión.

Consideraciones de alta disponibilidad

Si desea configurar la alta disponibilidad para Lenovo XClarity Orchestrator, use las funciones de alta disponibilidad que forman parte del sistema operativo del host.

Microsoft Hyper-V

Utilice la función de alta disponibilidad que se proporciona con el entorno Hyper-V.

VMware ESXi

En un entorno VMware High Availability, se configuran varios hosts como un clúster. El almacenamiento compartido se usa para crear la imagen de disco de una máquina virtual (MV) a disposición de los hosts

del clúster. La MV se ejecuta en un solo host a la vez. Cuando se produce algún problema con la máquina virtual, se inicia otra instancia de la misma en un host de copia de seguridad.

VMware High Availability requiere los componentes siguientes.

- Dos hosts como mínimo en los que está instalado ESXi. Estos hosts pasan a formar parte del clúster de VMware.
- Un tercer host en el que se instala VMware vCenter.

  Consejo: Asegúrese de instalar una versión de VMware vCenter que sea compatible con las versiones de ESXi instaladas en los hosts que se usarán en el clúster.

  VMware vCenter se puede instalar en uno de los hosts que se usan en el clúster. Sin embargo, si ese host se apaga o no es utilizable, también perderá el acceso a la interfaz de VMware vCenter.
- Almacenamiento compartido (almacenes de datos) a los que pueden tener acceso todos los hosts de un clúster. Puede emplear cualquier tipo de almacenamiento compartido compatible con VMware. VMware usa el almacén de datos para determinar si una MV realizará la conmutación por error a otro host distinto (latidos).

Capítulo 2. Configuración de XClarity Management Hub para dispositivos de cliente perimetral

Cuando se accede al Lenovo XClarity Management Hub por primera vez, hay varios pasos que debe completar para realizar la configuración inicial del XClarity Management Hub.

Procedimiento

Siga estos pasos para realizar la configuración inicial del XClarity Management Hub.

Paso 1. Inicie sesión en la interfaz web del XClarity Management Hub.

Paso 2. Lea y acepte el acuerdo de licencia.

Paso 3. Crear cuentas de usuarios adicionales.

Paso 4. Configure el acceso de red, incluidas las direcciones IP para las redes de gestión y de datos.

Paso 5. Configure la fecha y hora.

Paso 6. Registre el XClarity Management Hub con el servidor de organización.

Inicio de sesión en XClarity Management Hub para dispositivos de cliente perimetral

Puede iniciar la interfaz web de XClarity Management Hub desde cualquier equipo que tenga conectividad de red a la máquina virtual de XClarity Management Hub.

Antes de empezar

Asegúrese de utilizar uno de los siguientes navegadores web compatibles.
- Chrome 80.0 o posterior
- Firefox ESR 68.6.0 o posterior
- Microsoft Edge 40.0 o posterior
- Safari 13.0.4 o posterior (se ejecuta en macOS 10.13 o posterior)

El acceso a la interfaz web se realiza a través de una conexión segura. Asegúrese de que utiliza **https**.

Si está configurando XClarity Management Hub de forma remota, recuerde que debe tener conectividad a la misma red de capa 2. Se debe acceder desde una dirección no enrutada hasta que se haya completado la configuración inicial. Por consiguiente, considere la posibilidad de acceder a XClarity Management Hub desde otra MV que tenga conectividad a XClarity Management Hub. Por ejemplo, puede acceder a XClarity Management Hub desde otra MV del host donde esté instado XClarity Management Hub.

XClarity Management Hub cierra automáticamente las sesiones de los usuarios tras 60 minutos, independientemente de la actividad.

Procedimiento

Lleve a cabo los pasos siguientes para iniciar sesión en la interfaz web de XClarity Management Hub.

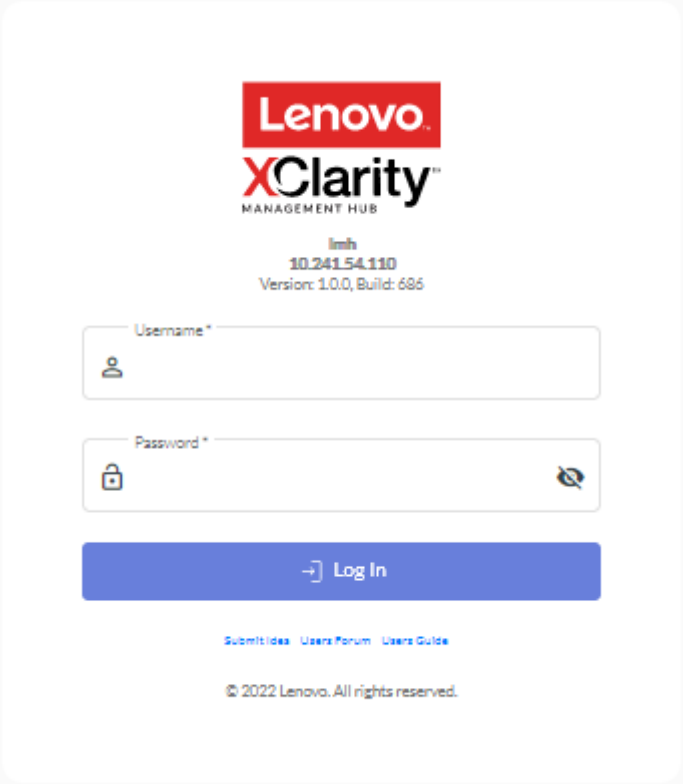
Paso 1. Dirija su navegador a la dirección IP de XClarity Management Hub.
`https://<IPv4_address>`

Por ejemplo:
`https://192.0.2.10`

La dirección IP que utilice dependerá de cómo esté configurado su entorno.

- Si especificó una dirección IPv4 en eth0_config, úsela para acceder al XClarity Management Hub.
- Si hay configurado un servidor DHCP en el mismo dominio de difusión que XClarity Management Hub, utilice la dirección IPv4 que se muestra en la consola de la máquina virtual del XClarity Management Hub para acceder al XClarity Management Hub.
- Si dispone de redes eth0 y eth1 en subredes independientes y utiliza DHCP en las dos subredes, utilice la dirección IP *eth1* cuando acceda a la interfaz web para realizar la configuración inicial. Cuando XClarity Management Hub se inicia por primera vez, tanto eth0 como eth1 obtienen una dirección IP asignada por DHCP, mientras que la puerta de enlace predeterminada de XClarity Management Hub se establece en la puerta de enlace asignada por DHCP para *eth1*.

Se muestra la primera página de inicio de sesión de XClarity Management Hub:



Paso 2. Seleccione el idioma deseado en la lista desplegable **Idioma**.

Nota: Es posible que los valores de configuración proporcionados por los dispositivos gestionados solo estén disponibles en inglés.

Paso 3. Introduzca sus credenciales de usuario y haga clic en **Iniciar sesión**.

Si es la primera vez que inicia sesión en el XClarity Management Hub, introduzca las credenciales predeterminadas **USERID** y **PASSW0RD** (donde 0 es cero).

Paso 4. Lea y acepte el acuerdo de licencia.

Paso 5. Si inició sesión por primera vez utilizando las credenciales predeterminadas, se le pedirá que cambie la contraseña. De manera predeterminada, las contraseñas deben contener de **8** a **256** caracteres y deben cumplir los siguientes criterios.

Importante: Se recomienda que utilice contraseñas seguras de 16 o más caracteres.
- (1) Deben contener al menos un carácter alfabético en mayúscula
- (2) Deben contener al menos un carácter alfabético en minúscula
- (3) Debe contener al menos un número
- (4) Debe contener al menos un carácter especial
- (5) No debe ser igual al nombre de usuario

Paso 6. Si inició sesión por primera vez, se le pedirá que elija si desea utilizar el certificado autofirmado actual o utilizar un certificado firmado externamente por la CA. Si elige utilizar un certificado firmado externamente, se muestra la página Certificado de servidor.

Atención: El certificado autofirmado no es seguro. Se le recomienda que genere e instale su propio certificado firmado externamente.

Para obtener información sobre cómo utilizar un certificado firmado externamente, consulte Instalación de un certificado de servidor firmado externamente y de confianza para dispositivos de cliente perimetral de XClarity Management Hub.

Después de finalizar

Puede realizar las siguientes acciones desde el menú de **Cuenta del usuario** ( ) en la esquina superior derecha de la interfaz web de XClarity Management Hub.

- Para cerrar la sesión actual, haga clic en **Cerrar sesión**. Se muestra la página inicio de sesión de XClarity Management Hub.
- Haga preguntas y encuentre respuestas en el Sitio web del foro de la comunidad de Lenovo XClarity.
- Envíe ideas sobre XClarity Management Hub haciendo clic en **Enviar ideas** en el menú **Cuenta de usuario** ( ) en la interfaz web de la esquina superior derecha o directamente en Sitio web de Lenovo XClarity Ideation.
- Consulte la documentación en línea haciendo clic en **Guía del usuario**.
- Para ver información sobre la versión de XClarity Management Hub, haga clic en **Acerca de**.
- Para cambiar el idioma de la interfaz de usuario, haga clic en **Cambiar idioma**. Se admiten los siguientes idiomas.
  - Inglés (en)
  - Chino simplificado (zh-CN)
  - Chino tradicional (zh-TW)
  - Francés (fr)
  - Alemán (de)
  - Italiano (it)
  - Japonés (ja)
  - Coreano (ko)
  - Portugués de Brasil (pt-BR)
  - Ruso (ru)
  - Español (es)
  - Tailandés (th)

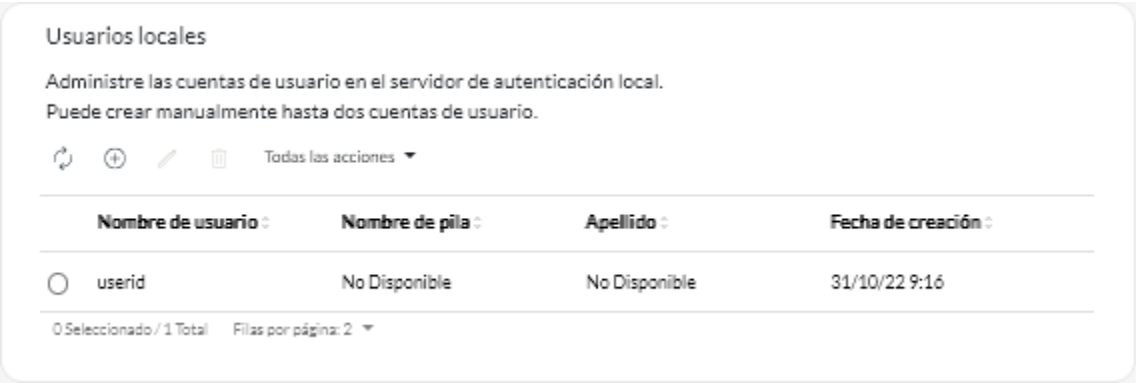
Creación de cuentas de usuario para Lenovo XClarity Management Hub dispositivos de cliente perimetral

Puede crear hasta 10 cuentas de usuario para Lenovo XClarity Management Hub.

Procedimiento

Para crear una cuenta de usuario, siga estos pasos.

Paso 1. En la barra de menús de Lenovo XClarity Management Hub, haga clic en **Seguridad (⚙) → Usuarios locales** para mostrar la tarjeta de Usuarios locales.



Paso 2. Haga clic en el icono **Crear** (⊕) para crear un usuario. Se muestra el cuadro de diálogo Crear nuevo usuario.

Paso 3. Rellene la siguiente información en el cuadro de diálogo.

- Escriba un nombre de usuario único. Puede especificar hasta 32 caracteres, incluidos caracteres alfanuméricos, punto (.), guion (-) y guion bajo (_).

  Nota: Los nombres de usuario no distinguen entre mayúsculas y minúsculas.
- Introduzca la nueva contraseña y confírmela. De manera predeterminada, las contraseñas deben contener de **8** a **256** caracteres y deben cumplir los siguientes criterios.

  Importante: Se recomienda que utilice contraseñas seguras de 16 o más caracteres.
  - (1) Deben contener al menos un carácter alfabético en mayúscula
  - (2) Deben contener al menos un carácter alfabético en minúscula
  - (3) Debe contener al menos un número
  - (4) Debe contener al menos un carácter especial
  - (5) No debe ser igual al nombre de usuario

Paso 4. Haga clic en **Crear**.

La cuenta de usuario se agrega a la tabla.

Después de finalizar

Puede realizar las acciones siguientes desde la tarjeta Usuarios locales.

- Para modificar la contraseña y las propiedades de su cuenta de usuario, haga clic en el icono de **Editar** (✎). Tenga en cuenta que las contraseñas no caducan.
- Elimine un usuario seleccionado haciendo clic en el icono de **Eliminar** (🗑).

Configuración de los valores de red para XClarity Management Hub para los dispositivos de cliente perimetral

Puede configurar una única interfaz de red IPv4 y los valores de enrutamiento de Internet.

Antes de empezar

Revise las consideraciones de red antes de configurarla (consulte Consideraciones de red).

Procedimiento

Para configurar los valores de red , haga clic en **Administración (⚙) → Redes** en la barra de menú de XClarity Management Hub y luego lleve a cabo uno o más de los pasos siguientes.

- **Configurar valores de IP**Para la interfaz eth0, haga clic en la pestaña **Interfaz Eth0**, configure los valores de dirección IPv4 correspondientes y, a continuación, haga clic en **Aplicar**.

  Atención:

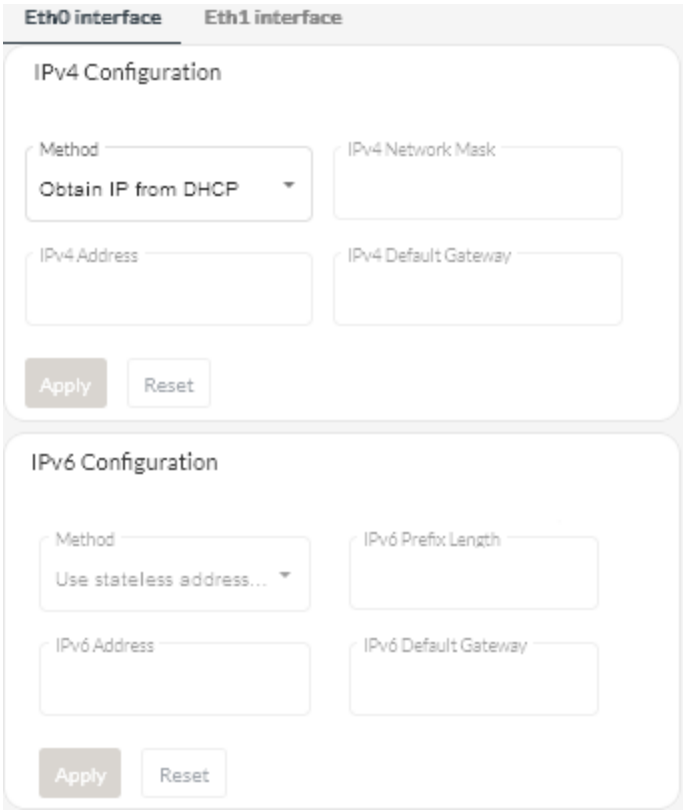
  – Cambiar la dirección IP del dispositivo virtual una vez que XClarity Management Hub está en funcionamiento causará problemas de conectividad con XClarity Orchestrator y con todos los dispositivos gestionados. Si necesita cambiar la dirección IP, desconecte XClarity Management Hub de XClarity Orchestrator y anule la gestión de todos los dispositivos gestionados antes de cambiar la dirección IP y, a continuación, vuelva a gestionar los dispositivos y vuelva a conectar XClarity Management Hub a XClarity Orchestrator una vez completado el cambio de dirección IP.

  Actualmente, solo se admiten direcciones IPv4.

  – **Valores de IPv4**. Puede configurar el método de asignación de IP, la dirección IPv4, la máscara de red y la puerta de enlace predeterminada.Para el método de asignación de IP, puede elegir usar una dirección IP asignada de forma estática, o bien obtener una dirección IP desde un servidor DHCP. Al utilizar una dirección IP estática, debe proporcionar una dirección IP, una máscara de red y una puerta de enlace predeterminada.

    La puerta de enlace predeterminada debe ser una dirección IP válida y debe utilizar la misma máscara de red (la misma subred) que la interfaz habilitada (eth0).

    Si cualquiera de las interfaces utiliza DHCP para obtener una dirección IP, la puerta de enlace predeterminada también utiliza DHCP.



- **Configure los valores de enrutamiento de Internet**Opcionalmente, configure los valores de Sistema de nombres de dominio (DNS) desde la tarjeta Configuración de DNS. Luego, haga clic en **Aplicar**.

  Actualmente, solo se admiten direcciones IPv4.

  Puede cambiar la dirección IP del servidor DNS.

  El nombre de dominio completo (FQDN) y el nombre de host del servidor DNS son los mismos que el servidor del XClarity Management Hub y no se pueden cambiar.

Configuración de la fecha y hora para XClarity Management Hub para dispositivos de cliente perimetral

Debe configurar al menos uno (y hasta cuatro) servidores de protocolo de tiempo de red (NTP) para sincronizar las marcas de tiempo entre XClarity Management Hub y todos los dispositivos gestionados.

Antes de empezar

Se debe poder tener acceso a cada servidor NTP en la red. Considere la posibilidad de configurar el servidor NTP en el un sistema local donde se ejecuta XClarity Management Hub.

Si cambia la hora del servidor NTP, puede que XClarity Management Hub tarde cierto tiempo en sincronizarse con la nueva hora.

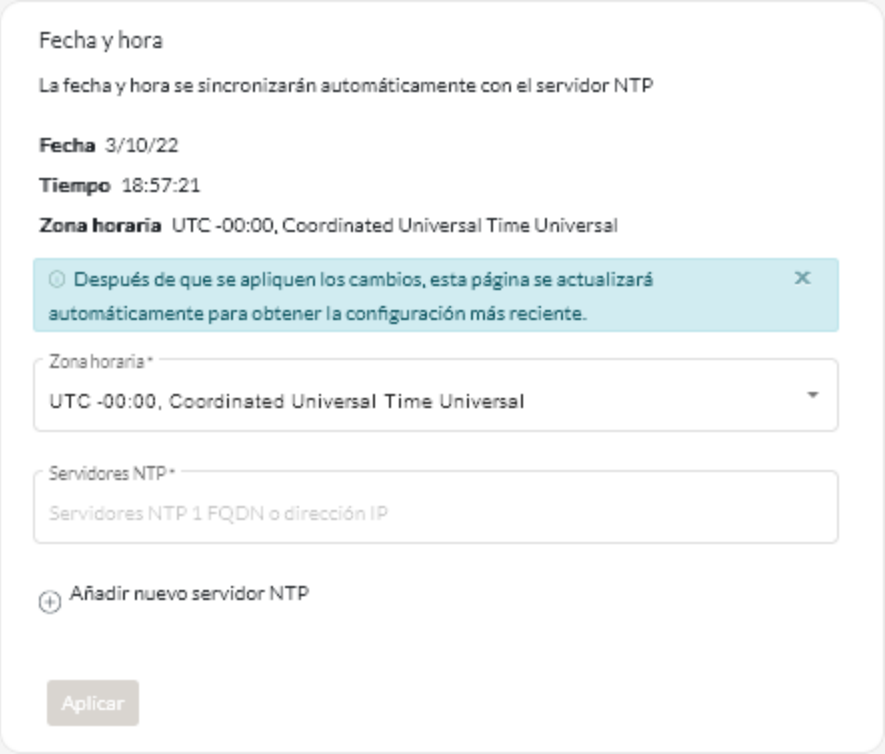
Atención: El dispositivo virtual XClarity Management Hub y su host se deben configurar para sincronizarse con la misma fuente para evitar una falla de sincronización de hora inadvertida entre el XClarity Management Hub y el host. Normalmente, el host está configurado para que sus dispositivos virtuales estén sincronizados con él. Si XClarity Management Hub está definido para sincronizarse con una fuente distinta al host, debe deshabilitar la sincronización de hora del host entre el dispositivo virtual de XClarity Management Hub y su host.

- Para ESXi, siga las instrucciones del VMware: página web de deshabilitar la sincronización de hora.

Procedimiento

Para establecer la fecha y la hora de XClarity Management Hub, lleve a cabo los pasos siguientes.

Paso 1. Desde la barra de menú de XClarity Management Hub, haga clic en **Administración (⚙) → Fecha y hora** para mostrarla tarjeta de Fecha y hora.



Paso 2. Elija la zona horaria en la que está ubicado el host de XClarity Management Hub.

Si la zona horaria seleccionada posee horario de verano (DST), la hora se ajusta automáticamente según DST.

Paso 3. Especifique el nombre de host o la dirección IP para cada servidor NTP en su red. Puede definir hasta cuatro servidores NTP.

Paso 4. Haga clic en **Aplicar**.

Gestión de certificados de seguridad para Lenovo XClarity Management Hub para dispositivos de cliente perimetral

Lenovo XClarity Management Hub utiliza certificados de SSL para establecer comunicaciones seguras y de confianza entre Lenovo XClarity Management Hub y sus dispositivos gestionados, así como comunicaciones de los usuarios con Lenovo XClarity Management Hub o con distintos servicios. De forma predeterminada, Lenovo XClarity Management Hub y XClarity Orchestrator utilizan certificados generados por XClarity Orchestrator que están autofirmados y que han emitido una entidad de certificación (CA) interna.

Antes de empezar

Esta sección está dirigida a administradores que tienen un conocimiento básico del estándar SSL y los certificados SSL, incluidos lo que son y cómo gestionarlos. Para obtener información general sobre los certificados de clave pública, consulte Página web de X.509 en Wikipedia y Página web de Certificado de infraestructura clave pública X.509 y perfil de lista de revocación de certificados (CRL) (RFC5280).

Acerca de esta tarea

El certificado de servidor predeterminado, que se genera de manera exclusiva en cada instancia de Lenovo XClarity Management Hub, proporciona suficiente seguridad para muchos entornos. Puede elegir permitir gestionar los certificados mediante Lenovo XClarity Management Hub o puede adoptar un papel más activo

al personalizar y sustituir los certificados de servidor. Lenovo XClarity Management Hub proporciona opciones que le permiten personalizar certificados para su entorno. Por ejemplo, puede optar por:

- Genere un nuevo par de claves regenerando la entidad de certificación interna o el certificado de servidor final que utilice valores específicos para su organización.
- Genere una solicitud de firma de certificado (CSR) que pueda enviarse a la entidad de certificación de su elección para firmar un certificado personalizado que se pueda cargar después en Lenovo XClarity Management Hub para usarlo como certificado de servidor final para todos los servicios alojados.
- Descargar el certificado de servidor en su sistema local de forma que pueda importar dicho certificado en la lista de certificados de confianza de su navegador web.

Lenovo XClarity Management Hub proporciona varios servicios que aceptan conexiones SSL/TLS entrantes. Cuando un cliente, como un navegador web, se conecta a uno de estos servicios, Lenovo XClarity Management Hub proporciona su *certificado de servidor* para ser identificado por el cliente que intenta realizar la conexión. El cliente debe mantener una lista de certificados en los que confía. Si el certificado de servidor de Lenovo XClarity Management Hub no está incluido en la lista del cliente, el cliente se desconecta de Lenovo XClarity Management Hub para evitar intercambiar cualquier información confidencial de seguridad con una fuente que no sea de confianza.

Lenovo XClarity Management Hub actúa como un cliente al comunicarse con los dispositivos gestionados y los servicios externos. Cuando esto ocurre, el dispositivo gestionado o el servicio externo proporciona su certificado de servidor para que sea verificado por Lenovo XClarity Management Hub. Lenovo XClarity Management Hub mantiene una lista de certificados en los que confía. Si el *certificado de confianza* proporcionado por el dispositivo gestionado o servicio externo no aparece en la lista, Lenovo XClarity Management Hub se desconecta del dispositivo gestionado o servicio externo para evitar intercambiar información confidencial de seguridad con un origen no fiable.

Los servicios de Lenovo XClarity Management Hub utilizan la siguiente categoría de certificados y cualquier cliente que se conecte a él debe confiar en ellos.

- **Certificado del servidor**. Durante el arranque inicial, se generan una clave única y un certificado autofirmado. Estos se usan como la Entidad de certificación de raíz predeterminada, que se puede gestionar en la página de Autoridad de certificación en los valores de seguridad de Lenovo XClarity Management Hub. No es necesario volver a generar el certificado de raíz a menos que se haya comprometido la clave o si su organización tiene una política que todos los certificados se deben reemplazar periódicamente (consulte Nueva generación del certificado de servidor autofirmado para dispositivos de cliente perimetral de XClarity Management Hub).También durante la configuración inicial, se genera una clave separada y se crea un certificado de servidor y es firmado por la autoridad de certificación interna. Este certificado utilizado como el certificado de servidor de Lenovo XClarity Management Hub predeterminado. Se regenera automáticamente cada vez que Lenovo XClarity Management Hub detecta que las direcciones de red (las direcciones IP o DNS) se han modificado para asegurarse de que el certificado contiene las direcciones correctas para el servidor. Se puede personalizar y se generara a demanda (consulte Nueva generación del certificado de servidor autofirmado para dispositivos de cliente perimetral de XClarity Management Hub).

  Puede elegir utilizar un certificado de servidor firmado externamente en lugar del certificado de servidor autofirmado predeterminado generando una solicitud de firma de certificado (CSR), teniendo la CSR firmada por una entidad de certificación raíz de certificado privada o comercial y luego importando la cadena de certificado completa en Lenovo XClarity Management Hub (consulte Instalación de un certificado de servidor firmado externamente y de confianza para dispositivos de cliente perimetral de XClarity Management Hub

  Si elige usar el certificado de servidor autofirmado predeterminado, se recomienda que importe el certificado del servidor en su navegador web como entidad de confianza de raíz para evitar los mensajes de error del certificado en su navegador (consulte Importación del certificado de servidor en un navegador web para Lenovo XClarity Management Hub para dispositivos de cliente perimetral

- **Certificado de despliegue de SO**. El servicio de despliegue del sistema operativo usa un certificado separado para asegurarse de que el instalador del sistema operativo pueda conectarse de forma segura al servicio de despliegue durante el proceso de despliegue. Si se ha comprometido la clave, puede volver a generarla reiniciando el Lenovo XClarity Management Hub.

Nueva generación del certificado de servidor autofirmado para dispositivos de cliente perimetral de XClarity Management Hub

Puede generar un nuevo certificado de servidor para sustituir el certificado de servidor firmado actual de Lenovo XClarity Management Hub o para reinstalar un certificado generado por XClarity Management Hub si XClarity Management Hub utiliza actualmente un certificado de servidor firmado externamente personalizado. El nuevo certificado de servidor autofirmado se usa en XClarity Management Hub para el acceso HTTPS.

Antes de empezar

Atención: Si vuelve a generar el certificado de servidor de XClarity Management Hub utilizando una nueva CA raíz, XClarity Management Hub pierde su conexión con los dispositivos gestionados y debe volver a gestionar los dispositivos. Si vuelve a generar el certificado de servidor de XClarity Management Hub sin cambiar la CA raíz (por ejemplo, cuando el certificado ha caducado), no es necesario volver a gestionar los dispositivos.

Acerca de esta tarea

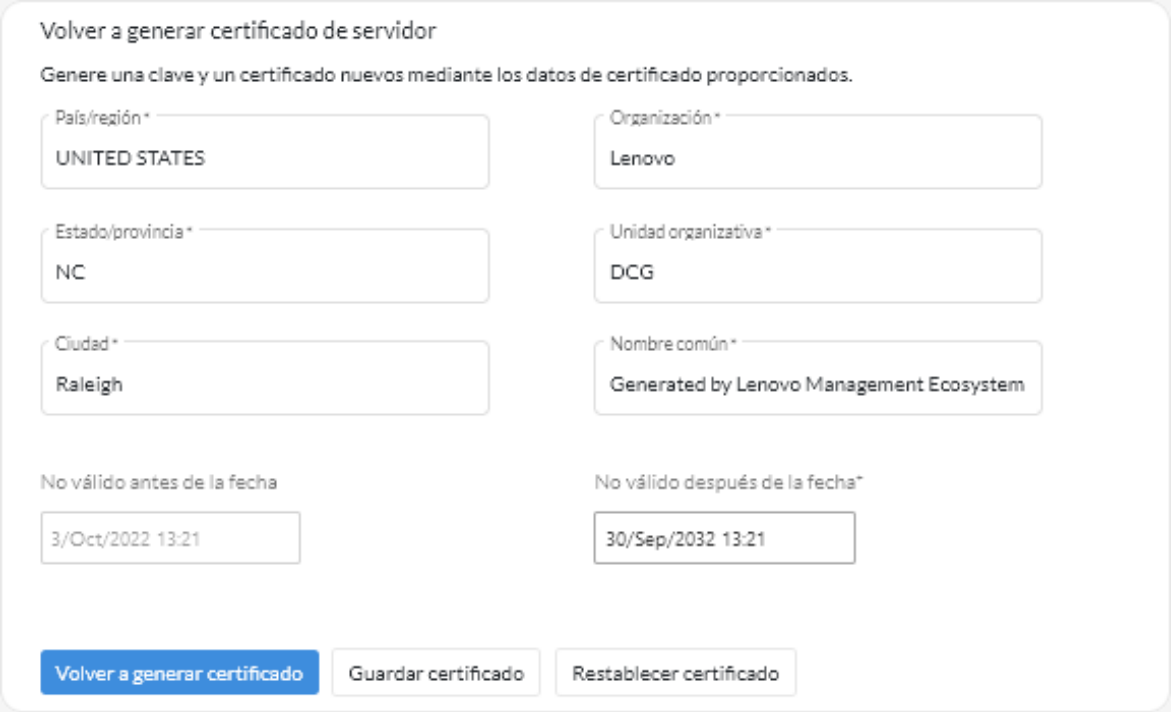
El certificado de servidor que está actualmente en uso, ya sea autofirmado o firmado externamente, permanece en uso hasta que se vuelva a generar, firmar e instalar un nuevo certificado de servidor.

Importante: Cuando se modifica el certificado de servidor, el concentrador de gestión se reinicia y todas las sesiones de usuario finalizan. Los usuarios deben iniciar sesión de nuevo para continuar trabajando en la interfaz web.

Procedimiento

Para generar un certificado de servidor autofirmado de XClarity Management Hub, siga estos pasos.

Paso 1. En la barra de menús de XClarity Management Hub, haga clic en **Seguridad ( ) → Certificado de servidor** para mostrar la nueva tarjeta **Volver a generar certificado de servidor autofirmado**.



Paso 2. En la tarjeta **Volver a generar certificado de servidor autofirmado**, complete los campos para la solicitud.

- Código ISO 3166 de dos letras del país o región de origen para asociar a la organización de certificados (por ejemplo, US para Estados Unidos).
- Nombre completo del estado o provincia que se va a asociar al certificado (por ejemplo, California o New Brunswick).
- Nombre completo de la ciudad que se va a asociar con el certificado (por ejemplo, San Jose). La longitud del valor no puede sobrepasar de 50 caracteres.
- Organización (compañía) propietaria del certificado. Normalmente, este es el nombre de incorporación legal de una compañía. Debe incluir cualquier sufijo, como Ltd., Inc. o Corp (por ejemplo, ACME International Ltd.). La longitud de este valor no puede sobrepasar de 60 caracteres.
- (Opcional) Unidad organizativa propietaria del certificado (por ejemplo, división ABC). La longitud de este valor no puede sobrepasar de 60 caracteres.
- Nombre común del propietario del certificado. Normalmente, este es el nombre de dominio completamente calificado (FQDN) o la dirección IP del servidor que está utilizando el certificado (por ejemplo, `www.domainname.com` o `192.0.2.0`). La longitud de este valor no puede sobrepasar de 63 caracteres.

  Nota: Actualmente, este atributo no afecta al certificado.
- Fecha y hora en las que el certificado de servidor ya no es válido.

  Nota: Actualmente, estos atributos no afectan al certificado.

Nota: No puede cambiar los nombres alternativos del asunto al volver a generar el certificado de servidor.

Paso 3. Haga clic en **Volver a generar certificado de servidor autofirmado** para volver a generar el certificado autofirmado y, a continuación, haga clic en **Volver a generar certificado** para confirmar.Se reinicia el concentrador de gestión y todas las sesiones de usuario establecidas finalizan.

Paso 4. Vuelva a iniciar sesión en el navegador web.

Después de finalizar

Puede realizar las siguientes acciones desde la tarjeta Volver a generar certificado de servidor autofirmado.
- Guarde el certificado de servidor actual en el sistema local en formato PEM; para ello, haga clic en **Guardar certificado**.
- Volver a generar el certificado de servidor utilizando la configuración predeterminada haciendo clic en **Restablecer certificado**. Cuando se le indique, presione Ctrl+F5 para actualizar el navegador y luego vuelva a establecer la conexión con la interfaz web.

Instalación de un certificado de servidor firmado externamente y de confianza para dispositivos de cliente perimetral de XClarity Management Hub

Puede optar por utilizar un certificado de servidor de confianza firmado por una entidad de certificación (CA) privada o comercial. Para utilizar el certificado de servidor firmado externamente, debe generar una solicitud de firma de certificado (CSR) e importar el certificado de servidor resultante para sustituir el certificado de servidor existente.

Antes de empezar

Atención:

- Si instala un certificado de servidor de confianza firmado externamente del Lenovo XClarity Management Hub utilizando una nueva CA raíz, XClarity Management Hub pierde su conexión con los dispositivos gestionados y debe volver a gestionar los dispositivos. Si instala un certificado de servidor firmado externamente de Lenovo XClarity Management Hub sin cambiar la CA raíz (por ejemplo, cuando el certificado ha caducado), no es necesario volver a gestionar los dispositivos.
- Si se añaden nuevos dispositivos después de generar la CSR y antes de importar el certificado de servidor firmado, esos dispositivos deben reiniciarse para recibir el nuevo certificado de servidor.

Acerca de esta tarea

Como práctica recomendada, utilice siempre los certificados firmados v3.

El certificado de servidor firmado externamente se debe haber creado a partir de la solicitud de firma de certificado generada más recientemente con el botón **Generar archivo CSR**.

El contenido del certificado de servidor firmado externamente debe ser un conjunto de certificados que contiene toda la cadena de firma de la CA, incluido el certificado raíz de la CA, todos los certificados intermedios y el certificado de servidor.

Si el nuevo certificado de servidor no fue firmado por un tercero de confianza, la próxima vez que conecte a Lenovo XClarity Management Hub, el navegador web mostrará un mensaje de seguridad y un cuadro de diálogo que le pide que acepte el nuevo certificado en el navegador. Para evitar los mensajes de seguridad, puede importar el certificado de servidor en la lista de certificados de confianza del navegador web (consulte Importación del certificado de servidor en un navegador web para Lenovo XClarity Management Hub para dispositivos de cliente perimetral).

XClarity Management Hub comienza a utilizar el nuevo certificado de servidor sin finalizar la sesión actual. Las nuevas sesiones se establecen utilizando el nuevo certificado. Para usar el nuevo certificado en uso, reinicie el navegador web.

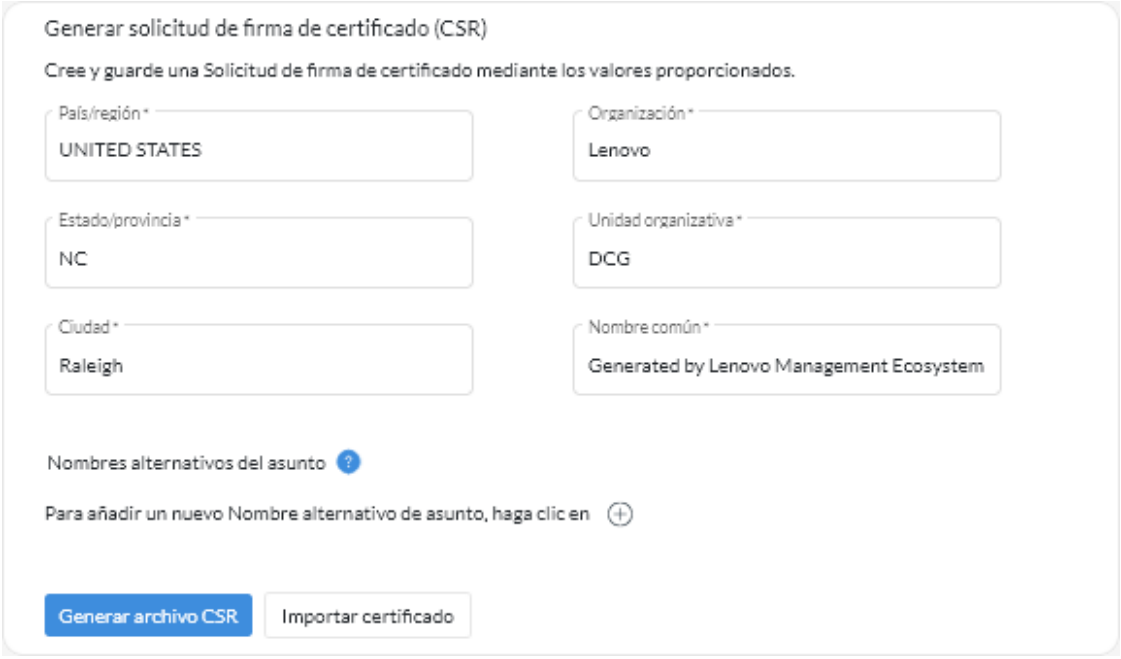
Importante: Cuando se modifica el certificado de servidor, todas las sesiones de usuario establecidas deben aceptar el nuevo certificado pulsando Ctrl + F5 para actualizar el navegador web y volver a establecer su conexión con XClarity Management Hub.

Procedimiento

Para generar e instalar un certificado de servidor firmado externamente, complete los pasos siguientes.

Paso 1. Cree una solicitud de firma de certificado y guarde el archivo en el sistema local.

1. En la barra de menús de XClarity Management Hub, haga clic en **Seguridad** ( ) → **Certificado de servidor** para mostrar la tarjeta de Generar solicitud de firma de certificado.



2. Desde la tarjeta Generar solicitud de firma de certificado (CSR), complete los campos para la solicitud.
   - Código ISO 3166 de dos letras del país o región de origen asociado a la organización de certificados (por ejemplo, US para Estados Unidos).
   - Nombre completo del estado o provincia que se va a asociar con el certificado (por ejemplo, California o New Brunswick).
   - Nombre completo de la ciudad que se va a asociar con el certificado (por ejemplo, San Jose). La longitud del valor no puede sobrepasar de 50 caracteres.
   - Organización (compañía) que es propietaria del certificado. Normalmente, este es el nombre de incorporación legal de una compañía. Debe incluir cualquier sufijo, como Ltd., Inc. o Corp (por ejemplo, ACME International Ltd.). La longitud de este valor no puede sobrepasar de 60 caracteres.
   - (Opcional) Unidad organizativa que es propietaria del certificado (por ejemplo, división ABC). La longitud de este valor no puede sobrepasar de 60 caracteres.
   - Nombre común del propietario del certificado. Este debe ser el nombre de host del servidor que está utilizando el certificado. La longitud de este valor no puede sobrepasar de 63 caracteres.

     Nota: Actualmente, este atributo no afecta al certificado.

- (Opcional) Los nombres alternativos de asunto que se personalizan, eliminan y añaden a la extensión X.509 “subjectAltName” cuando se genera la CSR. Los nombres alternativos de asunto especificados están validados (según el tipo especificado) y se añaden a la CSR después de generar la CSR. De forma predeterminada, XClarity Management Hub define automáticamente los nombres alternativos de asunto para CSR según la dirección IP y el nombre de host que se detectó mediante las interfaces de red del sistema operativo invitado de XClarity Management Hub.

  Atención: Los nombres alternativos del asunto deben incluir el nombre de dominio completo (FQDN) o la dirección IP del concentrador de gestión, y el nombre del asunto debe establecerse con FQDN del concentrador de gestión. Compruebe que estos campos obligatorios estén presentes y sean correctos antes de iniciar el proceso de CSR para asegurarse de que el certificado resultante esté completo. Si faltan datos de certificado, puede que las conexiones no sean de confianza al intentar conectar el concentrador de gestión a Lenovo XClarity Orchestrator.

  El nombre que especifique debe ser válido para el tipo seleccionado.
  - **DNS** (utilice el FQDN, por ejemplo, hostname.labs.company.com)
  - **Dirección IP** (por ejemplo, 192.0.2.0)
  - **Correo electrónico** (por ejemplo, example@company.com)

Paso 2. Proporcione una entidad emisora de certificación de confianza (CA) para CSR. La CA firma el CSR y arroja un certificado de servidor.

Paso 3. Importe el certificado de servidor firmado externamente y el certificado de la CA a XClarity Management Hub y sustituya el certificado de servidor actual.

1. En la tarjeta generar solicitud de firma de certificado (CSR) , haga clic en **Importar certificado** para mostrar el cuadro de diálogo Importar certificado.
2. Copie y pegue el certificado de servidor y el certificado de la CA en formato PEM. Debe proporcionar toda la cadena de certificados, comenzando con el certificado de servidor y terminando en el certificado de CA raíz.
3. Haga clic en **Importar** para almacenar el certificado de servidor en el almacén de confianza de XClarity Management Hub.

Paso 4. Acepte el nuevo certificado pulsando Ctrl+F5 para actualizar el navegador y luego vuelva a establecer la conexión con la interfaz web. Esto debe ser realizado por todas las sesiones de usuario establecidas.

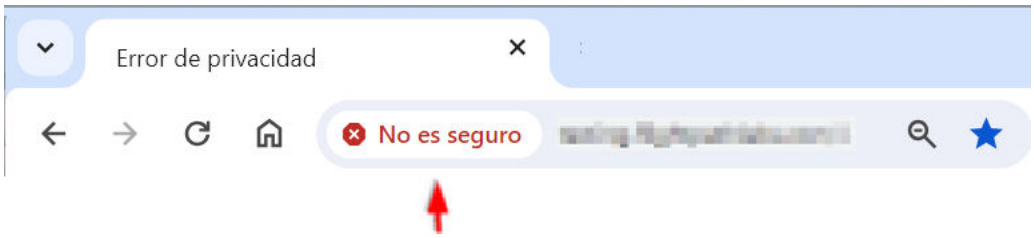
Importación del certificado de servidor en un navegador web para Lenovo XClarity Management Hub para dispositivos de cliente perimetral

Puede guardar una copia del certificado de servidor, en formato PEM, a su sistema local. Luego puede importar el certificado a la lista de certificados de confianza del navegador web o a otras aplicaciones para evitar los mensajes de advertencia de seguridad del navegador web cuando accede a Lenovo XClarity Management Hub.

Procedimiento

Para importar el certificado de servidor a un navegador web, complete los siguientes pasos.

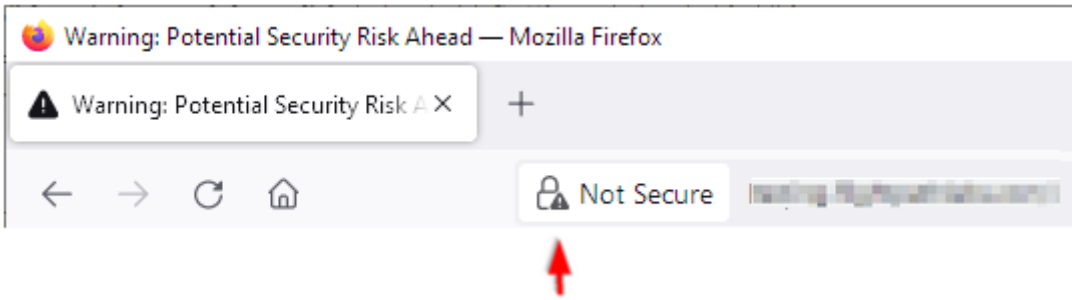
- **Chrome**
  1. Exportación del certificado de servidor de Lenovo XClarity Management Hub.
     a. Haga clic en el icono de advertencia “No seguro” de la barra de direcciones superior, por ejemplo:



b. Haga clic en **El certificado no es válido** para mostrar el cuadro de diálogo Certificado.
c. Haga clic en la pestaña **Detalles**.
d. Pulse **Exportar**.
e. Especifique el nombre y la ubicación del archivo del certificado y, a continuación, haga clic en **Guardar** para exportar el certificado.
f. Cierre el cuadro de diálogo Visor de certificados.

2. Importe el certificado de servidor Lenovo XClarity Management Hub en la lista de certificados de confianza de la autoridad raíz del navegador.
a. Desde el navegador Chrome, haga clic en los tres puntos de la esquina superior derecha de la ventana y, a continuación, haga clic en **Valores** para abrir la página Valores.
b. Haga clic en **Privacidad y seguridad** y, a continuación, haga clic en **Seguridad** para mostrar la página Seguridad.
c. Desplácese a la sección **Avanzado** y, a continuación, haga clic en **Gestionar certificados de dispositivos**.
d. Haga clic en **Importar** y luego en **Siguiente**.
e. Seleccione el archivo de certificado que exportó anteriormente y, a continuación, haga clic en **Siguiente**.
f. Elija dónde almacenar el certificado y haga clic en **Siguiente**.
g. Haga clic en **Finalizar**.
h. Cierre y vuelva a abrir el navegador Chrome y, a continuación, abra Lenovo XClarity Management Hub.

- **Firefox**
1. Exportación del certificado de servidor de Lenovo XClarity Management Hub.
a. Haga clic en el icono de advertencia “No seguro” de la barra de direcciones superior, por ejemplo:



b. Haga clic en **Conexión no segura** y, a continuación, haga clic en **Más información**.
c. Haga clic en **Ver certificado**.
d. Desplácese hacia abajo a la sección **Varios** y haga clic en el enlace **PEM (cert)** para guardar el archivo en el sistema local.
2. Importe el certificado de servidor Lenovo XClarity Management Hub en la lista de certificados de confianza de la autoridad raíz del navegador.

a. Abra el navegador y haga clic en **Herramientas → Valores** y, a continuación, haga clic en **Privacidad & Seguridad**.
b. Desplácese hacia abajo a la sección **Seguridad**.
c. Haga clic en **Ver certificados** para mostrar el cuadro de diálogo Gestor de certificados.
d. Haga clic en la pestaña **Sus certificados**.
e. Haga clic en **Importar** y vaya a la ubicación donde se descargó el certificado.
f. Seleccione el certificado y haga clic en **Abrir**.
g. Cierre el cuadro de diálogo Gestor de certificados.

Conexión de XClarity Management Hub para dispositivos de cliente perimetral a XClarity Orchestrator

Después de registrar (conectar) Lenovo XClarity Management Hub con Lenovo XClarity Orchestrator, puede empezar a gestionar y supervisar sus dispositivos.

Antes de empezar

Asegúrese de que se pueda acceder a XClarity Management Hub en la red desde XClarity Orchestrator y de que se pueda acceder a XClarity Orchestrator en la red desde XClarity Management Hub.

Procedimiento

Lleve a cabo los pasos siguientes para registrar XClarity Management Hub.

Paso 1. Cree la clave de registro del concentrador de gestión.

1. En la barra de menús de Management Hub , haga clic en **Registro** para mostrar la página Registro.

2. Haga clic en **Crear clave de registro**.
3. Haga clic en **Copiar en el portapapeles** para copiar la clave de registro y, a continuación, cierre el cuadro de diálogo.

Paso 2. Añada la clave de registro del concentrador de gestión a XClarity Orchestrator.

1. Desde la barra de menú de XClarity Orchestrator, haga clic en **Recursos ( ) → Gestores de recursos** para mostrar la tarjeta de Gestores de recursos.

2. Haga clic en el icono **Conectar** ( ) para mostrar el Gestor de recursos. El cuadro de diálogo Conectar gestor de recursos.

3. Seleccione **XClarity Management Hub** como gestor de recursos.
4. Copie la clave de registro en el campo **Token de registro**.
5. Haga clic en **Conectar** para mostrar el cuadro de diálogo Conectar gestor de recursos que contiene la clave de registro de XClarity Orchestrator.
6. Haga clic en **Copiar en el portapapeles** para copiar la clave de registro y, a continuación, cierre el cuadro de diálogo.

Paso 3. Añada la clave de registro de XClarity Orchestrator al concentrador de gestión.

1. En la barra de menús de Management Hub , haga clic en **Registro** para mostrar la página Registro.
2. Haga clic en **Instalar clave de registro**.
3. Copie la clave de registro en el campo **Token de registro**.
4. Haga clic en **Conectar**.

Después de finalizar

- Gestione dispositivos mediante el concentrador de gestión (consulte Gestión de dispositivos del cliente ThinkEdge en la documentación en línea de XClarity Orchestrator).
- Elimine la clave de registro actual del concentrador de gestión haciendo clic en **Restablecer registro**.

Capítulo 3. Desinstalación de XClarity Management Hub para dispositivos de cliente perimetral

Siga estos pasos para desinstalar un dispositivo virtual del XClarity Management Hub.

Procedimiento

Para desinstalar un dispositivo virtual del XClarity Management Hub, siga estos pasos.

Paso 1. Anule la gestión de todos los dispositivos que actualmente se estén gestionando mediante el XClarity Management Hub.

Paso 2. Dependiendo del sistema operativo, desinstale el XClarity Management Hub.

- **ESXi**
  1. Conéctese al host a través de VMware vSphere Client.
  2. Haga clic en con el botón derecho en la máquina virtual y, a continuación, haga clic en **Alimentación → Apagar**.
  3. Haga clic en con el botón derecho otra vez en la máquina virtual y, a continuación, haga clic en **Eliminar del disco**.

Lenovo