



# Guía de planificación e instalación de Lenovo XClarity Orchestrator



**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)**

**© Copyright Lenovo 2020, 2024.**

**AVISO DE DERECHOS LIMITADOS Y RESTRINGIDOS:** si los productos o software se suministran según el contrato "GSA" (General Services Administration), la utilización, reproducción o divulgación están sujetas a las restricciones establecidas en el Contrato Núm. GS-35F-05925.

---

# Contenido

<b>Contenido</b> . . . . .	<b>i</b>	Implementación de alta disponibilidad (ESXi) . . . .	18
<b>Resumen de los cambios</b> . . . . .	<b>.iii</b>	<b>Capítulo 4. Configuración de XClarity Orchestrator por primera vez</b> . . . . .	<b>21</b>
<b>Capítulo 1. Planificación para XClarity Orchestrator</b> . . . . .	<b>1</b>	Acceso a la interfaz web de XClarity Orchestrator por primera vez . . . . .	21
Licencias . . . . .	1	Creación de un usuario local . . . . .	23
Hardware y software admitidos. . . . .	2	Configuración de la red . . . . .	25
Firewall y servidores proxy . . . . .	5	Configuración de fecha y hora . . . . .	27
Disponibilidad de puertos . . . . .	6	Configuración del servidor de autenticación. . . . .	29
Consideraciones de red . . . . .	7	Configuración de valores de seguridad adicionales . . . . .	32
Consideraciones de seguridad . . . . .	8	Configuración y habilitación de la notificación automática de problemas (Llamar a casa). . . . .	33
Consideraciones de un entorno seguro . . . . .	8	Configuración del reenvío de datos de sucesos . . . . .	35
Consideraciones sobre la criptografía . . . . .	9	Conexión de gestores de recursos . . . . .	36
Consideraciones del certificado de seguridad . . . . .	9	<b>Capítulo 5. Aplicación de licencias de XClarity Orchestrator.</b> . . . . .	<b>41</b>
Consideraciones de servidor de autenticación . . . . .	10	<b>Capítulo 6. Actualización de XClarity Orchestrator</b> . . . . .	<b>47</b>
Consideraciones sobre el control de acceso. . . . .	10	<b>Capítulo 7. Desinstalación de XClarity Orchestrator</b> . . . . .	<b>53</b>
Consideraciones de alta disponibilidad. . . . .	10		
<b>Capítulo 2. Instalación de XClarity Orchestrator</b> . . . . .	<b>13</b>		
<b>Capítulo 3. Implementación de alta disponibilidad</b> . . . . .	<b>17</b>		
Implementación de la alta disponibilidad (Hyper-V) . . . . .	17		



---

## Resumen de los cambios

Las revisiones de seguimiento del software de gestión Lenovo XClarity Orchestrator proporcionan soporte para nuevas mejoras del software y soluciones a diversos problemas.

Consulte el archivo de historial de cambios (\*.chg) que se proporciona con el paquete de actualización para obtener más información acerca de la solución de los problemas existentes.

Esta versión admite las siguientes mejoras para la planificación e instalación. Para obtener información sobre los cambios en versiones anteriores, consulte [Novedades](#) en la documentación en línea de XClarity Orchestrator.

Función	Descripción
Planificación e instalación	XClarity Orchestrator requiere un mínimo de 8 núcleos de procesador virtuales (consulte <a href="#">Hardware y software admitidos</a> ).



---

# Capítulo 1. Planificación para XClarity Orchestrator

---

## Licencias

Lenovo XClarity Orchestrator es una aplicación de pago. Puede utilizar XClarity Orchestrator sin costo durante 90 días con la licencia de prueba gratuita; sin embargo, después de que finalice esta prueba gratuita, debe comprar e instalar las licencias adecuadas para seguir utilizando las funciones aplicables de XClarity Orchestrator y para obtener servicio y soporte de XClarity Orchestrator.

XClarity Orchestrator es compatible con las siguientes licencias.

- **XClarity Orchestrator.** Habilita los servidores de funciones de Orchestrator y de gestión base, chasis, conmutadores y dispositivos de almacenamiento, así como la autorización para el servicio y soporte de XClarity Orchestrator. Para las funciones de organización, se necesita una licencia en XClarity Orchestrator para cada dispositivo que admita la configuración del servidor y el despliegue del SO. Para el servicio y soporte de XClarity Orchestrator, se necesita una licencia para *cada dispositivo gestionado*.

El cumplimiento de la licencia se determina en función del número de dispositivos gestionados. El número de dispositivos gestionados no debe superar el número total de licencias en todas las claves de licencia activas de XClarity Orchestrator. Si no se cumple con el número de licencias de XClarity Orchestrator (por ejemplo, si las licencias caducan o si la gestión de dispositivos adicionales supera el número total de licencias activas), tiene un período de gracia de 90 días para instalar las licencias adecuadas. Si el período de gracia (incluida la prueba gratuita) para las licencias finaliza antes de que se instale el número de licencias necesario, *todas* las funciones de XClarity Orchestrator se deshabilitan (incluida la supervisión, la gestión básica y el análisis). Cuando inicie sesión, se le redirigirá a la página de información de licencia donde puede aplicar licencias adicionales.

Por ejemplo, si gestiona 100 servidores ThinkSystem adicionales y 20 conmutadores de bastidor utilizando una instancia existente de XClarity Administrator que está gestionando mediante XClarity Orchestrator, dispone de 90 días para comprar e instalar 100 licencias adicionales de XClarity Orchestrator antes de que todas las funciones se deshabiliten en la interfaz de usuario. No es necesario disponer de licencias para los 20 conmutadores de bastidor para utilizar las funciones de XClarity Orchestrator; no obstante, son necesarias si desea obtener servicio y soporte para XClarity Orchestrator. Si las funciones de XClarity Orchestrator están deshabilitadas, las funciones se vuelven a habilitar después de instalar las licencias suficientes para que se vuelvan a cumplir.

**Importante:** La licencia básica de XClarity Orchestrator es un requisito previo para las licencias de análisis de XClarity Pro y XClarity Orchestrator. Si el número de licencias de XClarity Pro o XClarity Orchestrator es conforme, pero el número de licencias básicas activas *no* es conforme, todas las funciones de XClarity Orchestrator (incluidas las de análisis), se deshabilitarán para todos los dispositivos.

- **Lenovo XClarity Pro.** Habilita las funciones de gestión avanzadas (configuración del servidor y despliegue del SO). Se necesita una licencia en XClarity Orchestrator para cada dispositivo que sea compatible con las funciones de gestión avanzadas.

El cumplimiento de la licencia se determina en función del número de dispositivos gestionados. El número de dispositivos gestionados no debe superar el número total de licencias en todas las claves de licencia activas de XClarity Pro. Cuando el número de licencias de XClarity Pro no es conforme, dispone de un período de gracia de 90 días para instalar las licencias adecuadas. Si el período de gracia (incluida la prueba gratuita) finaliza antes de que se instale el número de licencias necesario, las funciones de configuración del servidor y despliegue del SO se deshabilitan para *todos los dispositivos*.

Para obtener más información sobre las licencias de XClarity Pro, consulte [Licencias y la prueba gratuita de 90 días](#) en la documentación en línea de XClarity Administrator.

- **Análisis de XClarity Orchestrator.** Habilita las funciones de análisis. Se necesita una licencia en XClarity Orchestrator para cada dispositivo que sea compatible con las funciones de gestión avanzadas.

El cumplimiento de la licencia se determina en función del número de dispositivos gestionados. El número de dispositivos gestionados no debe superar el número total de licencias en todas las claves de licencia activas de análisis de XClarity Orchestrator. Si el número de licencias de análisis de XClarity Orchestrator no es conforme (por ejemplo, si las licencias caducan o si la gestión de dispositivos adicionales supera el número total de licencias activas), dispone de un período de gracia de 90 días para instalar las licencias adecuadas. Si el período de gracia (incluida la prueba gratuita) finaliza antes de que se instale el número de licencias necesario, se deshabilitan los menús de **Supervisión → Análisis** se deshabilitan y ya no podrá ver informes de análisis ni crear reglas ni consultas de alertas personalizadas para *todos los dispositivos*.

**Importante:** Después de instalar las licencias de análisis de XClarity Orchestrator, debe actualizar la interfaz de usuario.

**Nota:** Si instala las licencias de análisis de XClarity Orchestrator caducadas (superaron su fecha de caducidad más allá del periodo de caducidad de 90 días) y luego actualiza la interfaz de usuario, las funciones de análisis se deshabilitan. Esto significa que cualquier período activo de prueba o prueba se cancela, se detienen los servicios de análisis y se anulan las funciones de análisis. (Esto puede durar varios minutos). Puede volver a habilitar las funciones de análisis importando nuevas licencias válidas.

Una licencia *no está* vinculada a dispositivos específicos.

El periodo de activación comienza cuando se canjean las licencias.

Las licencias se instalan utilizando una *clave de activación* de licencia. Una vez que haya canjeado las licencias, puede crear una clave de activación para todas las licencias disponibles, o un subconjunto de ellas, y, a continuación, descargar e instalar la clave de activación en XClarity Orchestrator.

Cada vez que XClarity Orchestrator pasa a no estar en cumplimiento, el periodo de gracia se restablece a 90 días.

Si las licencias ya están instaladas, *no* se requieren nuevas licencias para actualizar a una nueva versión de XClarity Orchestrator.

Si está utilizando una licencia de prueba gratuita o dispone de un período de gracia para la conformidad y actualiza a una versión posterior de XClarity Orchestrator, la licencia de prueba o el período de gracia se restablecen a 90 días.

Al actualizar XClarity Orchestrator o si se produce una condición de error que requiera restaurar las claves de activación, puede usar claves de activación exportadas o descargar todas las claves de activación (para cada Id. de cliente) desde [Características del portal web on Demand](#) y luego importar las claves de activación (como claves de activación individuales o en grupo, como un archivo ZIP de claves) en XClarity Orchestrator.

Para obtener información acerca de cómo comprar licencias, póngase en contacto con su representante de Lenovo o con un business partner autorizado.

---

## Hardware y software admitidos

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

### Sistemas host

XClarity Orchestrator se ejecuta en un dispositivo virtual en un sistema.

## Requisitos de hipervisor

Se admiten los siguientes hipervisores para instalar XClarity Orchestrator.

- Microsoft Windows Server 2019 con Hyper-V instalado
- Microsoft Windows Server 2022 con Hyper-V instalado
- VMware ESXi 7.0
- VMware ESXi 6.7, U1, U2 y U3
- VMware ESXi 6.5, U1 y U2

Para Hyper-V, el dispositivo virtual es una imagen de disco virtual (VHD). Para VMware ESXi, el dispositivo virtual es una plantilla OVF.

## Requisitos de hardware

Se deben cumplir los siguientes *requisitos mínimos* para el dispositivo virtual. Dependiendo del tamaño de su entorno y del uso que haga de las funciones de aprovisionamiento (como el despliegue del sistema operativo, las actualizaciones de firmware y la configuración del servidor), puede que se necesiten recursos adicionales para obtener un rendimiento óptimo.

- 8 núcleos de procesador virtual
- 16 GB de memoria
- 551 GB de almacenamiento, a través de dos discos conectados.
  - 251 GB como mínimo para el dispositivo virtual (disco 0)
  - 100 GB para el repositorio de actualizaciones (disco 1)
  - 200 GB para el repositorio de imágenes del SO (disco 2)

**Importante:** No puede aumentar o reducir el tamaño del disco que se utiliza para el repositorio de actualizaciones y de imágenes del SO.

## Requisitos de software

XClarity Orchestrator requiere el siguiente software.

- **Servidor de autenticación.** XClarity Orchestrator utiliza un servidor con protocolo ligero de acceso a directorios (LDAP) interno para realizar la autenticación. Si elige utilizar un servidor de autenticación externo, los siguientes servidores LDAP son compatibles:
  - Microsoft Active Directory se ejecuta en Windows Server 2008 o versiones posteriores
- **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 Orchestrator. Asegúrese de que se pueda acceder a dicho servidor mediante la red de gestión (normalmente, la interfaz Eth0). Considere la posibilidad de utilizar un sistema local en el que XClarity Orchestrator esté instalado como servidor NTP. Si lo hace, asegúrese de que se pueda acceder a dicho sistema local mediante la red de gestión.

## Recursos gestionables

XClarity Orchestrator puede admitir un número ilimitado de gestores de recursos que gestionan colectivamente un máximo de 10,000 dispositivos en total.

XClarity Orchestrator es compatible con los siguientes gestores de recursos.

- **Lenovo XClarity Management Hub 2.0** XClarity Orchestrator gestiona y supervisa dispositivos que se están gestionando mediante XClarity Management Hub 2.0. Cada instancia de XClarity Management Hub 2.0 puede gestionar hasta 5,000 dispositivos.

**Importante:** Las funciones avanzadas (como el despliegue del sistema operativo y la configuración del servidor utilizando patrones de configuración) no son compatibles con este concentrador de gestión.

Encontrará una lista completa de los dispositivos 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 2.0](#).

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

- **Lenovo XClarity Management Hub**XClarity Orchestrator gestiona, supervisa y aprovisiona dispositivos que se están gestionando mediante XClarity Management Hub. Cada instancia de XClarity Management Hub puede gestionar hasta **10.000** dispositivos del cliente ThinkEdge.

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](#).

- **Lenovo XClarity Administrator** v2.6 o posterior XClarity Orchestrator gestiona, supervisa y aprovisiona dispositivos físicos que se están gestionando mediante XClarity Administrator. Cada instancia de XClarity Administrator puede gestionar hasta **1.000** dispositivos (servidores, chasis, conmutadores y almacenamiento).

XClarity Orchestrator admite todos los dispositivos compatibles con XClarity Administrator y XClarity Management Hub, excepto donde se indique lo contrario. Encontrará una lista completa de los dispositivos y opciones compatibles (como E/S, DIMM y adaptadores de almacenamiento), los niveles de firmware mínimos requeridos y las consideraciones de limitaciones en las siguientes páginas web de Lenovo XClarity.

- [Servidores ThinkAgile, ThinkEdge, ThinkSystem, System x, Converged HX y NeXtScale](#)
- [Dispositivos Flex System y ThinkSystem en chasis](#)
- [Servidores ThinkServer](#)
- [Conmutadores](#)
- [Dispositivos de almacenamiento](#)

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

**Nota:** La característica de despliegue del SO requiere XClarity Administrator versión 4.0 o posterior.

- **Schneider Electric EcoStruxure IT Expert**XClarity Orchestrator gestiona y supervisa recursos de infraestructura, como PDU y UPS, gestionados por Experto de TI de EcoStruxure.
- **VMware vRealize Operations Manager**XClarity Orchestrator supervisa las mediciones de la carga de trabajo virtual desde vRealize Operations Manager.

**Nota:** vRealize Operations Manager no se incluye en la lista de gestores de recursos, ya que no gestiona dispositivos en XClarity Orchestrator.

## Navegadores web

La interfaz web XClarity Orchestrator 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)

## Software de terceros

XClarity Orchestrator se integra con el software siguiente.

- Splunk v 7.0.3 y posterior (consulte [Guía del usuario de la aplicación XClarity Orchestrator para Splunk](#))

## 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
<b>Descargue actualizaciones</b> (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
<b>Envíe datos de servicio a Soporte de Lenovo (Llamar a casa) – Solo XClarity Orchestrator</b>		
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
<b>Envíe datos periódicos a Lenovo – Solo XClarity Orchestrator</b>		
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
<b>Recupere la información de garantía</b>		
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 red](#) en 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	<ul style="list-style-type: none"><li>DNS: TCP/UDP en el puerto <b>53</b></li></ul>	<ul style="list-style-type: none"><li>HTTPS: TCP en el puerto <b>443</b></li></ul>
Servidor de autenticación externo	<ul style="list-style-type: none"><li>LDAP: TCP en el puerto <b>389</b><sup>1</sup></li></ul>	No aplicable
Servicios de reenvío de sucesos	<ul style="list-style-type: none"><li>Servidor de correo electrónico (SMTP): UDP en el puerto <b>25</b><sup>1</sup></li><li>Servicio Web REST (HTTP): UDP en el puerto <b>80</b><sup>1</sup></li><li>Splunk – UDP en el puerto <b>8088</b><sup>1</sup>, <b>8089</b><sup>1</sup></li><li>Syslog: UDP en el puerto <b>514</b><sup>1</sup></li></ul>	No aplicable
Servicios de Lenovo (incluyendo Llamar a casa)	<ul style="list-style-type: none"><li>HTTPS (Llamar a casa): TCP en el puerto <b>443</b></li></ul>	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	<ul style="list-style-type: none"> <li>DNS: UDP en el puerto <b>53</b></li> <li>NTP: UDP en el puerto <b>123</b></li> <li>HTTPS: TCP en el puerto <b>443</b></li> <li>SSDP: UDP en el puerto <b>1900</b></li> <li>DHCP: UDP en el puerto <b>67</b></li> </ul>	<ul style="list-style-type: none"> <li>HTTPS: TCP en el puerto <b>443</b></li> <li>Implementación de SSDP: UDP en los puertos <b>32768-65535</b></li> </ul>
Servidores ThinkSystem y ThinkAgile	<ul style="list-style-type: none"> <li>HTTPS: TCP en el puerto <b>443</b></li> <li>Detección de SSDP: UDP en el puerto <b>1900</b></li> </ul>	<ul style="list-style-type: none"> <li>HTTPS: TCP en el puerto <b>443</b></li> </ul>

### 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 <sup>1</sup>	<ul style="list-style-type: none"> <li>DNS: TCP/UDP en el puerto <b>53</b><sup>2</sup></li> </ul>	<ul style="list-style-type: none"> <li>HTTPS: TCP en el puerto <b>443</b></li> <li>MQTT: TCP en el puerto <b>8883</b></li> </ul>
Dispositivos del cliente ThinkEdge <sup>3</sup>	No aplicable	<ul style="list-style-type: none"> <li>MQTT: TCP en el puerto <b>8883</b></li> </ul>

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

XClarity Orchestrator utiliza una única subred (eth0) para la gestión y la comunicación de datos. Revise las siguientes consideraciones antes de configurar la red.

- La interfaz de red se utiliza para la detección y gestión. Debe poder comunicarse con todos los dispositivos que tenga pensado gestionar.
- Si desea enviar manualmente datos de servicio recolectados al soporte de Lenovo o bien notificación automática de problemas (Llamar a casa), las interfaces deben estar conectadas a Internet, preferentemente a través de un firewall.
- Si cambia la dirección IP del dispositivo virtual de XClarity Orchestrator después de conectarse a los gestores de recursos, XClarity Orchestrator perderá la comunicación con los gestores y estos aparecerán fuera de línea. Si necesita cambiar la dirección IP del dispositivo virtual después de que XClarity Orchestrator esté actualizado y funcionando, asegúrese de que todos los gestores de recursos estén desconectados (eliminados) antes de cambiar la dirección IP.
- configure los componentes de los dispositivos de forma que minimicen los cambios de dirección IP. Plántese 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 la dirección IP cambia, deberá desconectar (eliminar) los dispositivos gestionados y luego volver a conectarlos.
- La traducción de dirección de red (NAT), que reasigna el espacio de una dirección IP en otro, no se admite.

---

## Consideraciones de seguridad

Revise las siguientes consideraciones para ayudarlo a planificar la seguridad de Lenovo XClarity Orchestrator y todos los recursos gestionados.

## Consideraciones de un entorno seguro

Es importante que evalúe los requisitos de seguridad de su entorno para poder conocer todos los riesgos de seguridad y reducirlos a un mínimo. Lenovo XClarity Orchestrator incluye varias funciones que pueden ayudarlo a crear un entorno más seguro. Utilice la información siguiente para ayudarlo a implementar el plan de seguridad para su entorno.

**Importante:** Usted es el responsable de evaluar, seleccionar e implementar las funciones de seguridad, procedimientos de configuración y controles apropiados para su entorno. La implementación de las funciones de seguridad que se describen en esta sección no protegen su entorno por completo.

Tenga en cuenta la información siguiente a la hora de evaluar los requisitos de seguridad de su entorno.

- La seguridad física de su entorno es importante. Limite el acceso a salas y bastidores donde se mantiene el hardware de gestión de sistemas.
- Utilice un firewall basado en software para proteger su hardware de red y los datos de amenazas de seguridad desconocidas y emergentes, como virus y accesos no autorizados.
- No cambie los valores de seguridad predeterminados de los conmutadores de red ni de los módulos de paso a través. Los valores predeterminados de fábrica de estos componentes deshabilitan el uso de protocolos no seguros y habilitan el requisito de las actualizaciones de firmware firmadas.
- Como mínimo, asegúrese de que instala actualizaciones de firmware críticas. Después de realizar cualquier cambio, realice siempre una copia de seguridad de la configuración.
- Asegúrese de que todas las actualizaciones relacionadas con la seguridad de los servidores DNS se instalen lo antes posible y se mantengan actualizadas.
- Pida a sus usuarios que no acepten certificados que no sean de confianza. Para obtener más información, consulte [Trabajo con certificados de seguridad](#) en la documentación en línea de XClarity Orchestrator.

- Siempre que sea posible y le resulte práctico, coloque el hardware de gestión de sistemas en una submáscara aparte. Normalmente, solo los supervisores deberían tener acceso al hardware de gestión de sistemas y no se debería conceder acceso a los usuarios básicos.
- Al elegir las contraseñas, no utilice expresiones que se puedan adivinar fácilmente, como “contraseña” o el nombre de su empresa. Mantenga las contraseñas en un lugar seguro y asegúrese de que el acceso a las mismas esté restringido. Implemente una política de contraseñas para su empresa.

**Importante:** Las reglas de contraseñas complejas deberían ser obligatorias para todos los usuarios.

- Establezca contraseñas de encendido para los usuarios como forma de controlar quién tiene acceso a los datos y a los programas de configuración de los servidores. Consulte la documentación que se suministra los hardware para obtener más información acerca de las contraseñas de encendido.

## Consideraciones sobre la criptografía

Lenovo XClarity Orchestrator admite TLS 1.2 y algoritmos criptográficos más seguros para conexiones de red seguras.

Para una mayor seguridad, solo son compatibles los cifrados de alto nivel. El sistema operativo del cliente y los navegadores web deben ser compatibles con una de las siguientes suites de cifrado.

- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-CHACHA20-POLY1305
- ECDHE-RSA-CHACHA20-POLY1305
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES256-GCM-SHA384

## Consideraciones del certificado de seguridad

Lenovo XClarity Orchestrator utiliza certificados de SSL para establecer comunicaciones seguras y de confianza entre XClarity Orchestrator y los gestores de recursos administrados (como Lenovo XClarity Administrator o Schneider Electric EcoStruxure IT Expert), así como comunicaciones de los usuarios con XClarity Orchestrator o con distintos servicios. De forma predeterminada, XClarity Orchestrator y Lenovo XClarity Administrator utilizan certificados generados por XClarity Orchestrator que están autofirmados y han sido emitidos por una entidad de certificación (CA) interna.

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

Para obtener más información sobre los certificados, consulte .

## Consideraciones de servidor de autenticación

Puede optar por utilizar el servidor Protocolo ligero de acceso a directorios (LDAP) local u otro servidor LDAP externo como servidor de autenticación.

El *servidor de autenticación* es un registro de usuario que se utiliza para autenticar las credenciales de usuario. Lenovo XClarity Orchestrator admite dos tipos de servidores de autenticación:

- **Servidor de autenticación local.** De manera predeterminada, XClarity Orchestrator está configurado para utilizar el servidor de LDAP local (integrado) que se encuentra en el servidor de organización.
- **Servidor LDAP externo.** Microsoft Active Directory se admite como servidor LDAP externo. Este servidor debe residir en un servidor de Microsoft Windows externo conectado a la red de gestión.

Para obtener más información sobre la configuración de servidores LDAP externos, consulte .

## Consideraciones sobre el control de acceso

Lenovo XClarity Orchestrator utiliza *listas de control de acceso (ACL)* para determinar los recursos (dispositivos, administradores de recursos y XClarity Orchestrator) a los que pueden acceder los usuarios. Cuando un usuario tiene acceso a un conjunto específico de recursos, dicho usuario puede ver los datos (como el inventario, los sucesos, las alertas y los análisis) que están relacionados solo con dichos recursos.

### Acerca de esta tarea

Un ACL es una unión de grupos de usuarios y grupos de recursos.

- *Los grupos de usuarios* identifican a los usuarios afectados por este ACL. El ACL debe contener un solo grupo de usuarios. Los usuarios que son miembros de un grupo al que se asigna el rol de **Supervisor** predefinido siempre tienen acceso a todos los recursos. No puede limitar el acceso a recursos para los usuarios supervisor.

Cuando el acceso basado en recursos está habilitado, los usuarios que *no son* miembros de un grupo al que se ha asignado el rol de **Supervisor** predefinido no tienen acceso a ningún recurso (dispositivos y gestores de recursos) de manera predeterminada. Debe añadir usuarios no supervisor a un grupo de usuarios que sea parte de una lista de control de acceso para permitir que estos usuarios puedan acceder a un conjunto específico de recursos.

Cuando el acceso basado en recursos está deshabilitado, todos los usuarios tienen acceso a todos los recursos (dispositivos y administradores de recursos) de manera predeterminada.

- *Los grupos de recursos* identifican los recursos (dispositivos, administradores de recursos y XClarity Orchestrator) a los que se puede acceder. El ACL debe contener al menos un grupo de recursos.

**Nota:** Un usuario que tiene acceso a un grupo de administradores no obtiene automáticamente acceso a todos los dispositivos gestionados por ese gestor de recursos. Debe otorgar acceso explícito a los dispositivos utilizando grupos de dispositivos.

Para obtener más información sobre las listas de control de acceso, consulte [Control de acceso a recursos](#) en la documentación en línea de XClarity Orchestrator.

---

## 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. Instalación de XClarity Orchestrator

Instale y configure el dispositivo virtual Lenovo XClarity Orchestrator en un sistema de su entorno local.

### Antes de empezar

Asegúrese de que ha revisado los requisitos previos, incluidos los requisitos de hardware y recomendaciones, para XClarity Orchestrator (consulte [Hardware y software admitidos](#)).

Asegúrese de que estén habilitados todos los puertos apropiados, incluidos los puertos que XClarity Orchestrator necesita (consulte [Disponibilidad de puertos](#)).

Asegúrese de que los gestores de recursos que desea gestionar sean compatibles y tengan los niveles de versión requeridos (consulte [Hardware y software admitidos](#)).

Para obtener más información acerca de cómo actualizar un dispositivo virtual de XClarity Orchestrator que ya esté instalado, consulte [Actualización de XClarity Orchestrator](#).

Para obtener información acerca de cómo configurar un entorno altamente variable, consulte [Implementación de alta disponibilidad](#).

Lenovo XClarity Orchestrator es una aplicación de pago. Puede utilizar XClarity Orchestrator sin costo durante 90 días con la licencia de prueba gratuita; sin embargo, después de que finalice esta prueba gratuita, debe comprar e instalar las licencias adecuadas para seguir utilizando las funciones aplicables de XClarity Orchestrator y para obtener servicio y soporte de XClarity Orchestrator. Para obtener información acerca de cómo comprar licencias, póngase en contacto con su representante de Lenovo o con un business partner autorizado. Para obtener información acerca de la licencia, consulte [Aplicación de licencias de XClarity Orchestrator](#).

### Acerca de esta tarea

Puede asignar la dirección IP del dispositivo virtual usando una dirección IP estática en el puerto eth0 durante la configuración.

Si no asigna una dirección IP durante la configuración, los valores IP se asignan mediante el Protocolo de configuración dinámica de host (DHCP) de forma predeterminada cuando inicia inicialmente el dispositivo virtual. Puede configurar los valores IP de XClarity Orchestrator al iniciar inicialmente el dispositivo virtual. Asegúrese de tener a mano la información de IP necesaria antes de comenzar. Tiene como máximo 60 segundos para introducir los valores en cada mensaje.

- Para los valores IPv4 estáticos, puede cambiar la dirección IP, la máscara de subred, la dirección IP de la puerta de enlace y la dirección IP de DNS 1 (opcional) y la dirección IP de DNS 2 (opcional).
- Para los valores IPv6 estáticos, puede cambiar la dirección IP, la longitud del prefijo y la dirección IP de DNS 1 (opcional) y la dirección IP de DNS 2 (opcional).
- Para la configuración de DHCP, puede cambiar los valores de interfaz primaria y de bucle invertido (auto lo, bucle invertido iface lo inet, auto eth0 y iface eth0 inet dhcp).

**Atención:** Si cambia la dirección IP del dispositivo virtual de XClarity Orchestrator después de conectarse a los gestores de recursos, XClarity Orchestrator perderá la comunicación con los gestores y estos aparecerán fuera de línea. Si necesita cambiar la dirección IP del dispositivo virtual después de que XClarity Orchestrator esté actualizado y funcionando, asegúrese de que todos los gestores de recursos estén desconectados

(eliminados) antes de cambiar la dirección IP. Para obtener más información sobre cómo configurar direcciones IP, consulte [Configuración de la red](#).

## Procedimiento

Para instalar el dispositivo virtual de XClarity Orchestrator, lleve a cabo los pasos siguientes.

Paso 1. Descargue la imagen de XClarity Orchestrator desde [página web de descargas de XClarity Orchestrator](#) al sistema local. Inicie sesión en el sitio web y utilice la clave de acceso que se le facilitó para descargar la imagen.

Para Hyper-V, el dispositivo virtual es una imagen de disco virtual (VHD). Para VMware ESXi, el dispositivo virtual es una plantilla OVF.

Paso 2. Instale y configure el dispositivo virtual en el sistema local.

- **Para ESXi que utiliza VMware vSphere**

1. Conéctese al host a través de VMware vSphere Client.
2. Haga clic con el botón derecho del mouse en **Máquinas virtuales → Crear/registrar VM → Desplegar una máquina virtual desde un archivo OVF u OVA**.
3. Complete cada paso en el asistente de implementación de dispositivo virtual. Tenga en cuenta las siguientes consideraciones mientras avanza en el asistente.
  - **Nombre del dispositivo.** Elija un nombre que sea único en este host.
  - **Storage.** Elija un almacén de datos que tenga como mínimo un almacenamiento de 551 GB disponible.
  - **Formato de disco.** Elija el formato de disco que se ajuste a las necesidades de su organización. Si no está seguro de qué formato elegir, seleccione **Aprovisionamiento fino**.
  - **Valores adicionales.** Opcionalmente, actualice la configuración de red para el dispositivo virtual a fin de establecer la dirección IP estática para la interfaz eth0.

- **Para ESXi que utiliza VMware vCenter**

1. Conéctese al host a través de VMware vCenter.
2. En “Hosts y clústeres” o “VM y plantillas”, haga clic con el botón derecho del mouse en el host y haga clic en **Archivo → Desplegar plantilla OVF**.
3. Complete cada paso en el asistente de implementación de dispositivo virtual. Tenga en cuenta las siguientes consideraciones mientras avanza en el asistente.
  - **Nombre del dispositivo.** Elija un nombre que sea único en este host.
  - **Storage.** Elija un almacén de datos que tenga como mínimo un almacenamiento de 551 GB disponible.
  - **Formato de disco.** Elija el formato de disco que se ajuste a las necesidades de su organización. Si no está seguro de qué formato elegir, seleccione **Aprovisionamiento fino**.
  - **Personalice la plantilla.** Opcionalmente, actualice la configuración de red para el dispositivo virtual a fin de establecer la dirección IP estática para la interfaz eth0.
4. Si elige definir la dirección IP estática para el dispositivo virtual, lleve a cabo los pasos siguientes.
  - a. Seleccione la VM en el inventario.
  - b. Haga clic en **Configurar → vApp** y, a continuación, seleccione **Habilitar opciones de vApp**.
  - c. Una vez habilitado, seleccione **Entorno OVF** para el esquema de asignación de IP.

- d. En la pestaña **Detalles de OVF**, seleccione “Herramientas de VMware” para el **Transporte de entorno OVF**.

- **Para Microsoft Hyper-V**

1. En el Panel de Server Manager, haga clic en **Hyper-V**.
2. Haga clic en con el botón derecho del ratón en el servidor y haga clic en **Administrador de Hyper-V**.
3. En **Acciones**, haga clic en **Nueva → Máquina virtual** para iniciar el Asistente de nueva máquina virtual y haga clic en **Siguiente**.
4. En la página Especificar nombre y ubicación, escriba el nombre de la nueva máquina virtual (por ejemplo, LXC0-*{version}*).
5. En la página Especificar generación, seleccione **Generación 1**.
6. En la página Asignar memoria, seleccione al menos 16 GB de memoria para utilizarla con esta máquina virtual (consulte [Hardware y software admitidos](#)).
7. En la página Configurar las conexiones de red, elija el Virtual Switch que creó al instalar y configurar el host.
8. En la página Conectar disco duro virtual, haga clic en **Usar un disco duro virtual existente**, vaya a la ubicación donde copió las imágenes VHD de XClarity Orchestrator y seleccione la imagen **\*disk001\*.vhd**.
9. Haga clic en **Finalizar**.
10. Haga clic con el botón derecho en la máquina virtual que ha acabado de crear y haga clic en **Valores**.
11. Configure el número de procesadores para asignar a la máquina virtual.
  - a. Seleccione **Procesador** y especifique al menos 8 procesadores virtuales para utilizar para esta máquina virtual (consulte [Hardware y software admitidos](#)).
  - b. Haga clic en **Aplicar**; a continuación, haga clic en **Aceptar**.
12. Añada la segunda unidad de disco duro al dispositivo virtual.
  - a. Expanda **IDE Controller 0** y, a continuación, seleccione **Unidad de disco duro**.
  - b. En el campo **Disco duro virtual**, vaya a la ubicación donde copió las imágenes VHD de XClarity Orchestrator y, a continuación, seleccione la imagen **\*disk002\*.vhd**.
  - c. Haga clic en **Aplicar**; a continuación, haga clic en **Aceptar**.
13. Añada la tercera unidad de disco duro al dispositivo virtual.
  - a. Expanda **IDE Controller 1** y, a continuación, seleccione **Unidad de disco duro**.
  - b. En el campo **Disco duro virtual**, vaya a la ubicación donde copió las imágenes VHD de XClarity Orchestrator y, a continuación, seleccione la imagen **\*disk003\*.vhd**.
  - c. Haga clic en **Aplicar**; a continuación, haga clic en **Aceptar**.
14. (Opcional) Si lo desea, puede especificar una dirección MAC estática para cada adaptador de red. Para ello, expanda **Adaptador de red** del Virtual Switch, haga clic en **Características avanzadas, Estática** en **Dirección MAC** y luego especifique la dirección MAC.

Paso 3. Encienda el dispositivo virtual.

Cuando se inicia el dispositivo virtual, se enumeran las direcciones IPv4 e IPv6 que asignó DHCP para cada interfaz, tal como se muestra en el ejemplo siguiente.

```
Lenovo XClarity Orchestrator Version x.x.x
```

```
-----  
eth0      Link encap:Ethernet  HWaddr 2001:db8:65:12:34:56
```

```
inet addr: 192.0.2.10 Bcast 192.0.2.255 Mask 255.255.255.0
inet6 addr: 2001:db8:56ff:fe80:bea3/64 Scope:Link
```

```
=====
=====
```

You have 118 seconds to change IP settings. Enter one of the following:

1. To set a static IP address for Lenovo XClarity virtual appliance eth0 port
  2. To use a DHCP address for Lenovo XClarity virtual appliance eth0 port
  3. To select subnet for Lenovo XClarity virtual appliance internal network
  - x. To continue without changing IP settings
- ... ..

Paso 4. Opcionalmente, puede configurar los valores IP del dispositivo virtual desde la consola. Si no realiza una selección dentro del tiempo especificado o si introduce x, el arranque inicial continúa utilizando los valores IP asignados de forma predeterminada.

- **Asigne direcciones IP estáticas para el puerto eth0.** Introduzca 1 y luego siga las indicaciones para cambiar los valores.
- **Asigne nuevas direcciones IP para el puerto eth0 utilizando DHCP.** Introduzca 2 y luego siga las indicaciones para cambiar los valores.
- **Seleccione la subred para la red interna de dispositivo virtual.** Introduzca 3 y luego siga las indicaciones para cambiar los valores. De forma predeterminada, XClarity Orchestrator utiliza la subred **192.168.252.0/24** para su red interna. Si esta subred se superpone con la red de host, cambie la subred a una de las opciones disponibles para evitar los problemas de red.
  - 192.168.252.0/24
  - 172.31.252.0/24
  - 10.255.252.0/24

**Importante:** Si especifica valores no válidos, se devuelve un error. Tiene hasta cuatro intentos para introducir valores válidos.

## Después de finalizar

Inicie sesión y configure XClarity Orchestrator.

---

## Capítulo 3. Implementación de alta disponibilidad

Para implementar una alta disponibilidad para Lenovo XClarity Orchestrator, utilice la función de alta disponibilidad que se proporciona para el entorno de host.

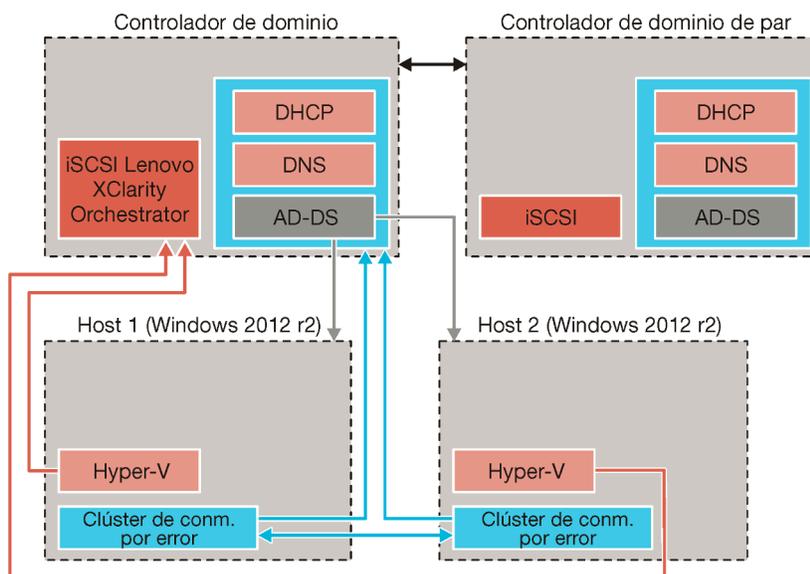
---

### Implementación de la alta disponibilidad (Hyper-V)

Para implementar la alta disponibilidad de Lenovo XClarity Orchestrator en un entorno Microsoft Hyper-V, use la función de alta disponibilidad que se proporciona por Hyper-V.

#### Acerca de esta tarea

En la siguiente figura se proporciona una descripción general de alto nivel de una forma de implementar la alta disponibilidad para XClarity Orchestrator en un entorno Hyper-V. En este ejemplo, la imagen de XClarity Orchestrator está instalada en el almacenamiento compartido y se accede a ella mediante el clúster.



#### Procedimiento

Para configurar un entorno de alta disponibilidad, lleve a cabo los siguientes pasos.

Paso 1. Configure el controlador de dominio.

- Realice la configuración de DHCP inicial.
- Configure DNS.
- Configure Active Directory-Domain Services (AD-DS).
- Complete la configuración de DHCP.

Paso 2. Configure el primer host.

- Instale Microsoft Windows 2012 r2.
- Una el dominio de AD-DS.
- Añada las funciones siguientes.
  - Hyper-V
  - Clúster de conmutación por error

- Paso 3. Configure el segundo host.
- Instale Microsoft Windows 2012 r2.
  - Una el dominio de AD-DS.
  - Añada las funciones siguientes.
    - Hyper-V
    - Clúster de conmutación por error
- Paso 4. Configure el almacenamiento compartido (por ejemplo, iSCSI) en el controlador de dominio y en ambos hosts.
- Paso 5. Configure el clúster de conmutación por error.
- Paso 6. Añada la imagen de XClarity Orchestrator.

---

## Implementación de alta disponibilidad (ESXi)

Para implementar una alta disponibilidad para Lenovo XClarity Orchestrator en un entorno VMware ESXi, utilice la función de alta disponibilidad que se proporciona por ESXi.

### Acerca de esta tarea

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.

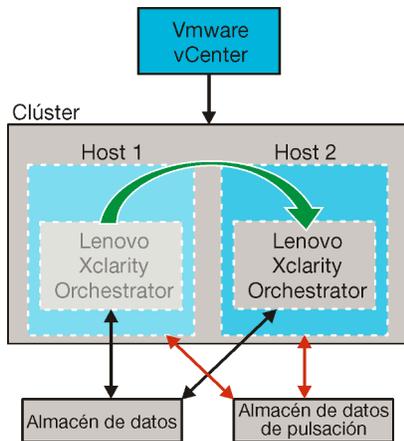
- Dos hosts como mínimo en los que está instalado ESXi. Estos hosts pasan a formar parte del clúster de VMware.
- Un tercer host en el que se instala VMware vCenter.

**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).

En la siguiente figura se muestra una forma de implementar la alta disponibilidad para XClarity Orchestrator en un entorno de ESXi. En este caso, el dispositivo virtual XClarity Orchestrator está instalado en el almacenamiento compartido y se accede a él mediante el clúster.



Para obtener información detallada acerca de la configuración de un clúster de VMware High Availability (VMware 5.0), consulte la [Página web de configuración de alta disponibilidad de VMware](#):

## Procedimiento

Para configurar un entorno de alta disponibilidad, lleve a cabo los siguientes pasos.

- Paso 1. Configure el almacenamiento compartido que deberá estar accesible desde todos los hosts del clúster.
- Paso 2. Instale ESXi en dos servidores, cada uno de ellos con direcciones IP estáticas. Asegúrese de que VMware vCenter está configurado en un servidor independiente.
- Paso 3. Iniciar VMware vCenter.
- Paso 4. Configure los otros dos hosts para que funcionen con VMware vCenter.
  - a. Cree el clúster.
  - b. Añada los hosts al clúster.
  - c. Añada ambos almacenes de datos a los hosts del clúster.

**Nota:** El segundo almacén de datos es necesario para combatir el calor.

- Paso 5. Despliegue XClarity Orchestrator en el clúster.



---

## Capítulo 4. Configuración de XClarity Orchestrator por primera vez

Cuando se accede a Lenovo XClarity Orchestrator por primera vez, debe llevar a cabo varios pasos para completar la configuración inicial.

### Procedimiento

Para configurar XClarity Orchestrator por primera vez, lleve a cabo los siguientes pasos.

- Paso 1. Acceso a la interfaz web de XClarity Orchestrator.
- Paso 2. Cambie la contraseña inicial.
- Paso 3. Lea y acepte el acuerdo de licencia.
- Paso 4. Crear cuentas de usuarios adicionales.
- Paso 5. Configure la fecha y hora.
- Paso 6. Configure el acceso de red, incluidas las direcciones IP para las redes de gestión y de datos.
- Paso 7. Elija utilizar el servidor de autenticación predeterminado o configure un cliente LDAP externo.
- Paso 8. Configure los valores de seguridad adicionales, incluida la importación de certificados de confianza para servicios internos y externos.
- Paso 9. Configure y habilite la notificación automática de problemas, si corresponde.
- Paso 10. Configure XClarity Orchestrator para reenviar sucesos a servicios y aplicaciones específicas, si corresponde.
- Paso 11. Conecte sus gestores de recursos.

---

### Acceso a la interfaz web de XClarity Orchestrator por primera vez

Puede iniciar la interfaz web de Lenovo XClarity Orchestrator desde cualquier sistema que tenga conectividad de red a la máquina virtual de XClarity Orchestrator.

### Antes de empezar

Asegúrese de utilizar uno de los siguientes navegadores web compatibles. Para obtener más información, consulte el apartado [Hardware y software admitidos](#).

- 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**.

XClarity Orchestrator usa una única subred, normalmente eth0.

Si está configurando XClarity Orchestrator 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 Orchestrator desde otra MV que tenga conectividad a XClarity Orchestrator. Por ejemplo, puede acceder a XClarity Orchestrator desde otra MV del host donde esté instalado XClarity Orchestrator.

### Procedimiento

Para acceder a la interfaz web de XClarity Orchestrator por primera vez, lleve a cabo los siguientes pasos.

1. Dirija su navegador a la dirección IP del dispositivo virtual XClarity Orchestrator.

- **Uso de una dirección IPv4 estática** Si especificó una dirección IPv4 durante la instalación, úsela para acceder a la interfaz web utilizando la siguiente URL.

`https://{IPv4_address}/#/login.html`

Por ejemplo:

`https://192.0.2.10/#/login.html`

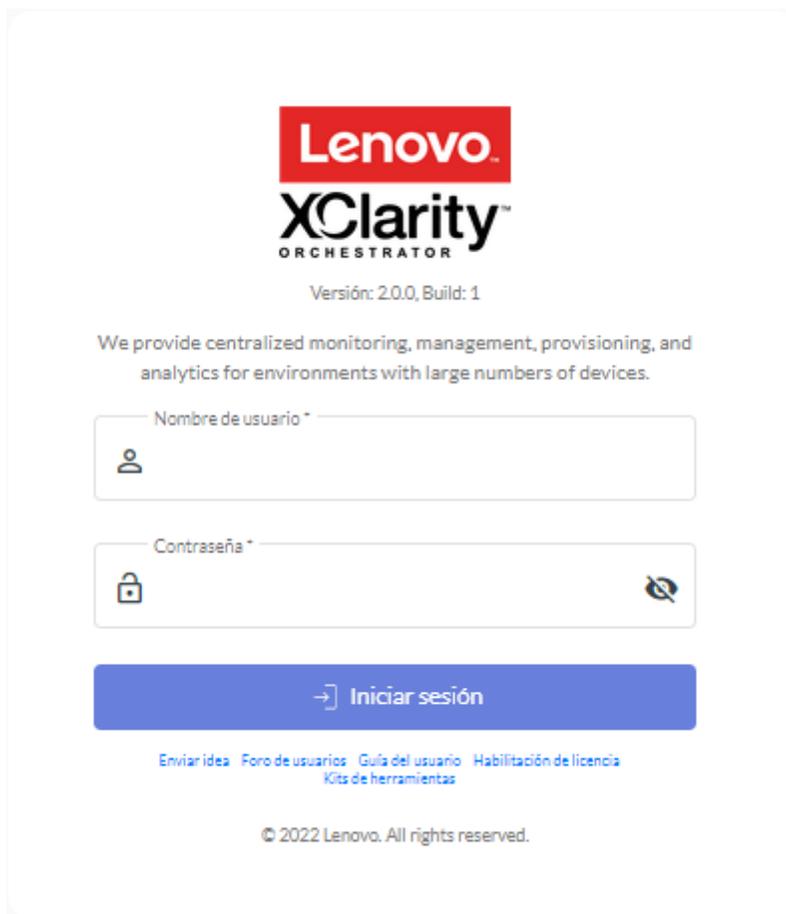
- **Uso de un servidor DHCP en el mismo dominio de difusión que XClarity Orchestrator** Si hay configurado un servidor DHCP en el mismo dominio de difusión que XClarity Orchestrator, utilice la dirección IPv4 que se muestra en la consola del dispositivo virtual de XClarity Orchestrator para acceder a la interfaz web utilizando la siguiente URL.

`https://{IPv4_address}/#/login.html`

Por ejemplo:

`https://192.0.2.10/#/login.html`

Se muestra la primera página de inicio de sesión.



Desde la página de inicio de sesión puede llevar a cabo las siguientes acciones:

- Envíe ideas para XClarity Orchestrator en [Sitio web de Lenovo XClarity Ideation](#) o haciendo clic en **Enviar idea**.
- Haga preguntas y reciba respuestas en el [Sitio web del foro de la comunidad de Lenovo XClarity](#) haciendo clic en **Foro de usuarios**.
- Para obtener información sobre cómo utilizar XClarity Orchestrator, haga clic en **Guía del usuario**.

- Busque y gestione todas sus licencias de Lenovo desde [Características del portal web on Demand](#) haciendo clic en **Habilitación de licencia**.
  - Para obtener información acerca de las API disponibles, haga clic en **Kits de herramientas**.
2. Seleccione el idioma deseado en la lista desplegable Idioma.

**Nota:** Es posible que algunos de los datos de configuración proporcionados por los gestores de recursos y dispositivos gestionados solo estén disponibles en inglés.

3. Introduzca las credenciales predeterminadas `USERID` y `PASSWORD` (donde 0 es cero) y luego haga clic en **Iniciar sesión**. La primera vez que se usa una cuenta de usuario específica para iniciar sesión en XClarity Orchestrator, se le pedirá que cambie la contraseña. De manera predeterminada, las contraseñas deben contener los caracteres **8 - 256** y deben cumplir los siguientes criterios.

**Importante:** Se recomienda que utilice contraseñas seguras de 16 o más caracteres.

- Debe contener al menos un carácter alfabético y no debe tener más de dos caracteres secuenciales, incluidas las secuencias de caracteres alfabéticos, dígitos y las teclas del teclado QWERTY (por ejemplo “abc”, “123” y “asd” no están permitidos)
- Debe contener por lo menos un número
- Deben contener al menos dos de los siguientes caracteres.
  - Caracteres alfabéticos en mayúscula (A - Z)
  - Caracteres alfabéticos en minúscula (a - z)
  - Caracteres especiales ; @ \_ ! ' \$ & +Los espacios en blanco no están permitidos.
- No se debe repetir ni invertir el nombre de usuario.
- No debe contener más de dos caracteres iguales consecutivamente (por ejemplo, “aaa”, “111” y “...” no están permitidos).

## Después de finalizar

**Importante:** Es posible que reciba advertencias de seguridad o de certificado la primera vez que acceda a XClarity Orchestrator. Puede hacer caso omiso de las advertencias.

Continúe la configuración inicial visitando [Creación de un usuario local](#).

---

## Creación de un usuario local

Puede crear manualmente las cuentas de usuario en el servidor de autenticación local (integrado). *Las cuentas de usuarios locales* se utilizan para iniciar sesión en Lenovo XClarity Orchestrator y autorizar el acceso a los recursos.

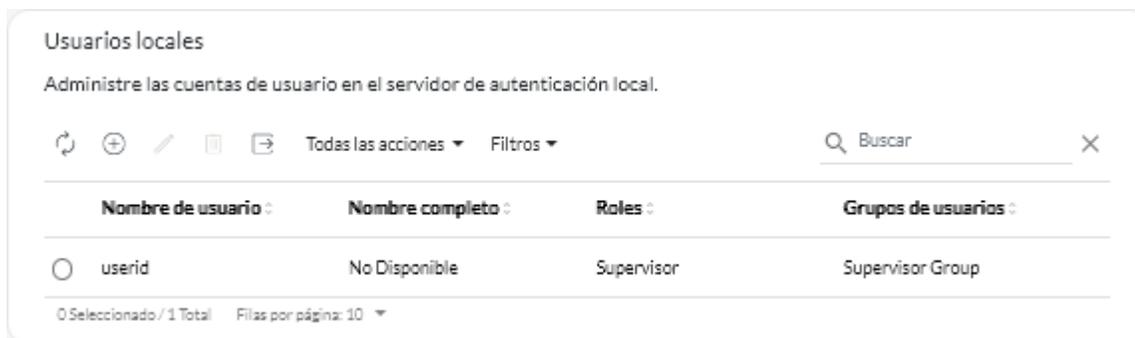
### Acerca de esta tarea

Como medida de seguridad adicional, cree al menos dos cuentas de usuario.

### Procedimiento

Para crear un usuario local, lleve a cabo los pasos siguientes.

- Paso 1. En la barra de menú de XClarity Orchestrator, haga clic en **Administración** (🔧) → **Seguridad** y luego haga clic en **Usuarios locales** en el panel de navegación izquierdo 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 los caracteres **8 - 256** y deben cumplir los siguientes criterios.

**Importante:** Se recomienda que utilice contraseñas seguras de 16 o más caracteres.

- Debe contener al menos un carácter alfabético y no debe tener más de dos caracteres secuenciales, incluidas las secuencias de caracteres alfabéticos, dígitos y las teclas del teclado QWERTY (por ejemplo “abc”, “123” y “asd” no están permitidos)
- Debe contener por lo menos un número
- Deben contener al menos dos de los siguientes caracteres.
  - Caracteres alfabéticos en mayúscula (A - Z)
  - Caracteres alfabéticos en minúscula (a - z)
  - Caracteres especiales ; @ \_ ! ' \$ & +
- Los espacios en blanco no están permitidos.
- No se debe repetir ni invertir el nombre de usuario.
- No debe contener más de dos caracteres iguales consecutivamente (por ejemplo, “aaa”, “111” y “...” no están permitidos).

- (Opcional) Especifique la información de contacto de la cuenta del usuario, incluido el nombre completo, la dirección de correo electrónico y el número de teléfono.

**Consejo:** para el nombre completo, puede especificar hasta 128 caracteres, incluidos letras, números, espacios, puntos, guiones, apóstrofos y comas.

Paso 4. Haga clic en la pestaña **Grupos de usuarios** y seleccione los grupos de usuarios de los que será miembro este usuario.

**Consejo:** si no se selecciona un grupo de usuarios, **OperatorGroup** se asigna de forma predeterminada

Paso 5. Haga clic en **Crear**.

La cuenta de usuario se agrega a la tabla.

## Después de finalizar

Continúe la configuración inicial visitando [Configuración de la red](#).

---

## Configuración de la red

Al configurar inicialmente Lenovo XClarity Orchestrator, debe configurar una interfaz de red única (utilizando los valores de IPv4 e IPv6). También puede configurar los valores de enrutamiento de Internet.

### Antes de empezar

Revise las siguientes consideraciones al elegir la interfaz.

- La interfaz se debe configurar para que admita la detección y gestión. Debe poder comunicarse con los gestores de recursos y los dispositivos que gestionan.
- Si desea enviar manualmente datos de servicio recolectados al soporte de Lenovo o bien notificación automática de problemas (Llamar a casa), las interfaces deben estar conectadas a Internet, preferentemente a través de un firewall.

### Atención:

- Si cambia la dirección IP del dispositivo virtual de XClarity Orchestrator después de conectarse a los gestores de recursos, XClarity Orchestrator perderá la comunicación con los gestores y estos aparecerán fuera de línea. Si necesita cambiar la dirección IP del dispositivo virtual después de que XClarity Orchestrator esté actualizado y funcionando, asegúrese de que todos los gestores de recursos estén desconectados (eliminados) antes de cambiar la dirección IP.
- Si la interfaz de red está configurada para utilizar el Protocolo de configuración dinámica de host (DHCP), puede que la dirección IP de la interfaz de gestión cambie cuando caduque la concesión de DHCP. Si la dirección IP cambia, deberá desconectar (eliminar) los gestores de recursos y luego volver a conectarlos. Para evitar este problema puede cambiar la interfaz de red a una dirección IP estática o asegurarse de que la configuración del servidor DHCP esté definida para que la dirección de DHCP se base en una dirección MAC o que la concesión de DHCP no caduque.
- La traducción de dirección de red (NAT), que reasigna el espacio de una dirección IP en otro, no se admite.

### Procedimiento

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

- **Configurar valores de IP** Puede elegir utilizar los valores de red IPv4 e IPv6 desde las tarjetas de Configuración de IPv4 y Configuración de IPv6. Habilite y modifique los valores de configuración de IP aplicables y luego haga clic en **Aplicar**.
  - **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 que debe estar en la misma subred que la interfaz de red.

Si se utiliza DHCP para obtener una dirección IP, la puerta de enlace predeterminada también utiliza DHCP.
  - **Valores de IPv6.** Puede configurar el método de asignación de IP, la dirección IPv6, la longitud de prefijo y la puerta de enlace predeterminada. Para el método de asignación de IP, puede elegir utilizar una dirección IP asignada de forma estática, una configuración de dirección de estado (DHCPv6) o una configuración automática de dirección sin estado. Al utilizar una dirección IP estática, debe proporcionar una dirección IPv6, una longitud de prefijo y una puerta de enlace. La puerta de enlace debe ser una dirección IP válida que debe estar en la misma subred que la interfaz de red.

### Configuration de IPv4

Enabled

Método Obtain IP from DHCP	Máscara de red IPv4 255.255.224.0
Dirección IPv4 10.243.14.36	Puerta de enlace predeterminad... 10.243.0.1

### Configuration de IPv6

Enabled

Método Use stateless address...	Longitud del prefijo de IPv6 64
Dirección IPv6 fd55:faaf:e1ab:2021:20c:2'	Puerta de enlace predeterm... fe80::5:73ff:fea0:2c

- **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.

Elija si va a utilizar DHCP para obtener las direcciones IP o para especificar direcciones IP estáticas habilitando o deshabilitando **DHCP DNS**. Si elige utilizar direcciones IP estáticas, especifique la dirección IP de al menos uno y hasta dos servidores DNS.

Especifique el nombre de host y el nombre de dominio de DNS. Puede elegir recuperar el nombre de dominio de un servidor DHCP o especificar un nombre de dominio personalizado.

#### Notas:

- Si elige utilizar un servidor DHCP para obtener la dirección IP, cualquier cambio que efectúe en los campos Servidor DNS se sobrescribirá la próxima vez que XClarity Orchestrator renueve la concesión de DHCP.
- Al cambiar cualquier valor de DNS, debe reiniciar manualmente la máquina virtual para aplicar los cambios.
- Si cambia el valor de DNS de DHCP a una dirección IP estática, asegúrese de que también cambia la dirección IP del servidor DNS.

**Configuración de DNS**

Si cambia la configuración de DNS, deberá reiniciar el servidor XClarity Orchestrator para aplicar los cambios.

Tipo de dirección DNS de preferencia  IPv4  IPv6

Enabled

Primera dirección DNS: 10.240.0.10

Método: Use domain name o...

Segunda dirección DNS: 10.240.0.11

Nombre de dominio:

Nombre de host: lxco

Aplicar Restablecer

- **Configuración de valores de proxy HTTP.** Opcionalmente, habilite y especifique el nombre de host del servidor proxy, el puerto y las credenciales opcionales desde la tarjeta de Configuración del proxy. Luego, haga clic en **Aplicar**.

**Notas:**

- 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.

**Configuración de proxy**

Disabled

Nombre de host del servidor pro... Nombre de usuario

Puerto del servidor proxy Contraseña

Aplicar Restablecer

**Después de finalizar**

Continúe la configuración inicial visitando [Configuración de fecha y hora](#).

**Configuración de fecha y hora**

Debe configurar al menos uno (y hasta cuatro) servidores de protocolo de tiempo de red (NTP) para sincronizar las marcas de tiempo de Lenovo XClarity Orchestrator con sucesos que se reciben de los gestores de recursos.

## 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 Orchestrator.

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

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

- **ESXi** Siga las instrucciones del [VMware: página web de deshabilitar la sincronización de hora](#).
- **Hyper-V** Desde el Administrador de Hyper-V, haga clic en XClarity Orchestrator máquina virtual y luego haga clic en **Valores**. En el cuadro de diálogo, haga clic en **Gestión** → **Servicios de integración** en el panel de navegación y luego desactive **Sincronización de hora**.

## Procedimiento

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

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

The screenshot shows the 'Fecha y hora' (Date and Time) configuration page in the XClarity Orchestrator interface. At the top, it states 'La fecha y hora se sincronizarán automáticamente con el servidor NTP'. Below this, the current settings are displayed: 'Fecha' (Date) is 3/10/22, 'Tiempo' (Time) is 18:57:21, and 'Zona horaria' (Time Zone) is UTC -00:00, Coordinated Universal Time Universal. A light blue notification banner indicates that the page will refresh automatically after changes. There are two input fields: 'Zona horaria\*' (Time Zone) with a dropdown menu currently showing 'UTC -00:00, Coordinated Universal Time Universal', and 'Servidores NTP\*' (NTP Servers) with a text input field containing 'Servidores NTP 1 FQDN o dirección IP'. Below the input fields is a button with a plus icon and the text 'Añadir nuevo servidor NTP'. At the bottom left, there is an 'Aplicar' (Apply) button.

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

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**.

## Después de finalizar

Continúe la configuración inicial visitando [Configuración del servidor de autenticación](#).

---

## Configuración del servidor de autenticación

Lenovo XClarity Orchestrator incluye un servidor de autenticación local (integrado). También puede elegir utilizar su propio servidor LDAP externo de Active Directory.

### Antes de empezar

Antes de que un usuario LDAP externo pueda iniciar sesión en XClarity Orchestrator, el usuario debe ser miembro directo de un grupo de usuarios LDAP que se haya clonado en XClarity Orchestrator. XClarity Orchestrator no reconoce los usuarios que son miembros de grupos de usuarios que están anidados en el grupo de usuarios LDAP clonado definido en el servidor LDAP externo.

Asegúrese de que todos los puertos requeridos para el servidor de autenticación externo estén abiertos en la red y en los firewalls. Para obtener información sobre los requisitos de puerto, consulte [Disponibilidad de puertos](#).

### Acerca de esta tarea

Si no se configura un servidor LDAP externo, XClarity Orchestrator siempre autentica a un usuario utilizando el servidor de autenticación local.

Si no se configura un servidor LDAP externo, XClarity Orchestrator primero intenta autenticar a un usuario utilizando el servidor de autenticación local. Si la autenticación produce un error, XClarity Orchestrator intenta autenticarse utilizando la dirección IP del servidor LDAP. Si la autenticación produce un error, el cliente LDAP intenta autenticarse mediante la dirección IP del siguiente servidor LDAP.

Cuando un usuario LDAP externo inicia sesión en XClarity Orchestrator por primera vez, una cuenta de usuario con el nombre <nombreusuario>@<dominio> se clona automáticamente en XClarity Orchestrator. Puede añadir usuarios de LDAP externos clonados a grupos de usuario o utilizar grupos LDAP para el control de acceso. También puede añadir privilegios de supervisor a un usuario de LDAP externo.

### Procedimiento

Para configurar XClarity Orchestrator para que use un servidor de autenticación LDAP externo, lleve a cabo los pasos siguientes.

Paso 1. En la barra de menú de XClarity Orchestrator, haga clic en **Administración** (⚙️) → **Seguridad** y luego haga clic en **Cliente LDAP** en el panel de navegación izquierdo para mostrar la tarjeta Cliente LDAP.

**ไคลเอ็นต์ LDAP**

คุณสามารถกำหนดค่า XClarity Orchestrator เพื่อใช้เซิร์ฟเวอร์ LDAP ภายนอกเพื่อตรวจสอบความถูกต้องผู้ใช้ได้ เซิร์ฟเวอร์ตรวจสอบความถูกต้องภายในทำการตรวจสอบความถูกต้องก่อนเสมอ หากการตรวจสอบความถูกต้องไม่สำเร็จ ไคลเอ็นต์ LDAP จะพยายามตรวจสอบความถูกต้องโดยใช้ที่อยู่ IP ของเซิร์ฟเวอร์ LDAP ภายนอกเครื่องแรก หากการตรวจสอบความถูกต้องไม่สำเร็จ ไคลเอ็นต์ LDAP จะพยายามตรวจสอบความถูกต้องโดยใช้ที่อยู่ IP ของเซิร์ฟเวอร์เครื่องถัดไป

**ข้อมูลเซิร์ฟเวอร์**

โดเมน\*  ที่อยู่เซิร์ฟเวอร์\*  พอร์ต\*

Active Directory  LDAP แบบกำหนดค่า LDAP ผ่าน SSL

**การกำหนดค่า**

ชื่อที่ประทับพื้นที่สำหรับผู้ใช้\*

ชื่อที่ประทับพื้นที่สำหรับกลุ่ม\*

**การผูกข้อมูลประจำตัว** ⓘ

วิธีการแยก

การแยกชื่อผู้ใช้\*

การเข้ารหัสลับ\*

ตั้งข้อมูลใบรับรองหรือวางใบรับรองที่อยู่ในรูปแบบ PEM (ตรวจสอบว่าการมีเครื่องหมาย BEGIN และ END): ⓘ

```

-----BEGIN CERTIFICATE-----
เนื้อหาของใบรับรอง
-----END CERTIFICATE-----

```

Paso 2. Siga estos pasos para configurar cada servidor LDAP externo.

1. Haga clic en el icono de **Añadir** (+) para agregar un servidor LDAP.
2. Especifique el nombre de dominio, la dirección IP y el puerto para el servidor LDAP externo.

Si el número de puerto *no* se ha establecido explícitamente en 3268 o 3269, se da por hecho que la entrada identifica un controlador de dominio.

Cuando el número de puerto se establece en 3268 o 3269, se da por hecho que la entrada identifica un catálogo global. El cliente LDAP intenta autenticarse usando el controlador de dominio de la primera dirección IP de servidor configurada. Si esto falla, el cliente LDAP intenta autenticarse usando el controlador de dominio de la siguiente dirección IP de servidor.

3. Opcionalmente, elija activar la personalización de la configuración avanzada. Cuando elige usar una configuración personalizada, puede especificar el filtro de búsqueda del usuario. Si no especifica un filtro de búsqueda del usuario, se utiliza (&(objectClass=user)(!(userPrincipalName={0})(sAMAccountName={0}))) de forma predeterminada.

Si la configuración avanzada está deshabilitada, se utiliza la configuración predeterminada de Active Directory.

4. Especifique el nombre distinguido base de LDAP completamente calificado desde el que el cliente LDAP inicia la búsqueda para la autenticación del usuario.
5. Especifique el nombre distinguido base de LDAP completamente calificado desde el que el cliente LDAP inicia la búsqueda de grupos de usuario (por ejemplo, `dc=company,dc=com`).
6. Opcionalmente, especifique las credenciales para vincular XClarity Orchestrator con el servidor de autenticación externo. Puede utilizar uno de los dos métodos de vinculación.

- **Credenciales configuradas.** Use este método de vinculación para utilizar un nombre y una contraseña de cliente específicos que se deberán utilizar para vincular XClarity Orchestrator con el servidor de autenticación externo. Si el enlace falla, también fallará el proceso de autenticación. Especifique el nombre distinguido de LDAP (por ejemplo, `cn=somebody,dc=company,dc=com`) o la dirección de correo electrónico (por ejemplo, `somebody@company.com`) de la cuenta de usuario, además de la contraseña que se va a utilizar para la autenticación LDAP a fin de vincular XClarity Orchestrator con el servidor LDAP. Si el enlace falla, también fallará el proceso de autenticación.

El nombre distinguido debe ser una cuenta de usuario con el dominio que tiene al menos privilegios de solo lectura.

Si el servidor LDAP no tiene subdominios, puede especificar el nombre de usuario sin el dominio (por ejemplo, `user1`). Sin embargo, si el servidor LDAP no tiene subdominios (por ejemplo, subdominio `new.company.com` en dominio `company.com`), entonces debe especificar el nombre de usuario y el dominio (por ejemplo, `user1@company.com`).

**Atención:** Si cambia la contraseña del cliente en el servidor LDAP externo, asegúrese de actualizar también la nueva contraseña en XClarity Orchestrator (consulte [No se puede iniciar sesión en XClarity Orchestrator](#) en la documentación en línea de XClarity Orchestrator).

- **Credenciales de inicio de sesión.** Use este método de vinculación para utilizar el nombre de usuario y la contraseña de XClarity Orchestrator de LDAP para vincular XClarity Orchestrator con el servidor de autenticación externo. Especifique el nombre distinguido de LDAP completamente calificado de una cuenta de usuario *de prueba* y la contraseña que se utilizará para la autenticación LDAP a fin de validar la conexión con el servidor de autenticación.

Estas credenciales de usuario no se guardan. Si se realiza correctamente, todos los vínculos futuros utilizan el nombre de usuario y la contraseña que usó para iniciar sesión en XClarity Orchestrator. Si el enlace falla, también fallará el proceso de autenticación.

**Nota:** Debe haber iniciado sesión en XClarity Orchestrator, utilizando un Id. de usuario completamente calificado (por ejemplo, `administrator@domain.com`).

7. Si lo desea, puede elegir usar LDAP seguro. Para ello, seleccione el conmutador de **LDAP sobre SSL** y luego haga clic en **Captar** para recuperar e importar el certificado SSL de confianza. Cuando se muestre el cuadro de diálogo Captar certificado de servidor, haga clic en **Aceptar** para usar el certificado. Si elige utilizar LDAP sobre SSL, XClarity Orchestrator utiliza el protocolo LDAPS para conectarse de forma segura al servidor de autenticación externo. Cuando se selecciona esta opción, los certificados de confianza se utilizan para habilitar la compatibilidad de LDAP seguro.

**Atención:** Si elige deshabilitar LDAP sobre SSL, XClarity Orchestrator utiliza un protocolo no seguro para conectarse al servidor de autenticación externo. Si elige esta configuración, el hardware puede quedar vulnerable a los ataques contra la seguridad.

8. Opcionalmente, puede volver a ordenar los servidores LDAP mediante los iconos de **Subir** (↑) y **Bajar** (↓). El cliente LDAP intenta autenticarse mediante la primera dirección IP de servidor. Si la autenticación produce un error, el cliente LDAP intenta autenticarse mediante la siguiente dirección IP de servidor.

**Importante:** Para la autenticación LDAP segura, use el certificado para la entidad de certificación (CA) raíz del servidor LDAP o uno de los certificados intermedios del servidor. Puede recuperar el certificado raíz o intermedio de la CA de un indicador de comando ejecutando el siguiente comando, donde *{FullyQualifiedHostNameOrIpAddress}* es el nombre completamente calificado del servidor LDAP externo. El certificado de CA raíz o intermedio es típicamente el último certificado en la salida, la última sección BEGIN - -END.

```
openssl s_client -showcerts -connect {FullyQualifiedHostNameOrIpAddress}:636
```

9. Haga clic en **Aplicar los cambios**. XClarity Orchestrator intenta probar la dirección IP, el puerto, los certificados SSL y las credenciales de enlace, y valida la conexión del servidor LDAP para detectar errores comunes. Si la validación se realiza correctamente, la autenticación del usuario en el servidor de autenticación externo se lleva a cabo cuando un usuario inicia sesión en XClarity Orchestrator. Si la validación falla, se muestran mensajes de error que indican el origen de los errores.

**Nota:** Si la validación tiene éxito y las conexiones al servidor LDAP se realizan correctamente, la autenticación del usuario puede fallar si el nombre distinguido raíz es incorrecto.

## Después de finalizar

Continúe la configuración inicial visitando [Configuración de valores de seguridad adicionales](#).

---

## Configuración de valores de seguridad adicionales

Puede configurar valores de seguridad adicionales, incluidos los certificados y valores de seguridad de la cuenta de usuario.

### Procedimiento

Para configurar la seguridad adicional, lleve a cabo uno o más de los pasos siguientes.

- Lenovo XClarity Orchestrator utiliza certificados de SSL para establecer comunicaciones seguras y de confianza entre XClarity Orchestrator y los gestores de recursos (como Lenovo XClarity Administrator), así como comunicaciones de los usuarios con XClarity Orchestrator. De forma predeterminada, XClarity Orchestrator y los gestores de recursos utilizan certificados generados por XClarity Orchestrator que están autofirmados y que ha emitido una entidad de certificación (CA) interna. Puede elegir generar una solicitud de firma de certificado (CSR) para firmar con una entidad de certificación externa, como la entidad de certificación de su organización o una entidad de certificación de terceros (consulte [Instalación de un certificado de servidor de XClarity Orchestrator de confianza firmado externamente](#) en la documentación en línea de XClarity Orchestrator).
- Puede importar certificados de confianza para servicios externos en el almacén de confianza de XClarity Orchestrator para establecer una conexión segura con los gestores de recursos y despachadores de sucesos, como Splunk (consulte [Adición de un certificado de confianza para servicios externos](#) en la documentación en línea de XClarity Orchestrator).
- Puede importar certificados de confianza para servicios internos en el almacén de confianza de XClarity Orchestrator para establecer una conexión segura con los gestores de recursos y los servidores LDAP de confianza (consulte [Adición de un certificado de confianza para servicios internos](#) en la documentación en línea de XClarity Orchestrator).
- Configure los valores de seguridad de complejidad de la contraseña, bloqueo de la cuenta y tiempo de espera por inactividad de la sesión web. Para obtener información sobre estos valores, consulte [Configuración de los valores de seguridad del usuario](#) en la documentación en línea de XClarity Orchestrator.

## Después de finalizar

Continúe la configuración inicial visitando [Configuración y habilitación de la notificación automática de problemas \(Llamar a casa\)](#).

---

## Configuración y habilitación de la notificación automática de problemas (Llamar a casa)

Puede configurar Lenovo XClarity Orchestrator para que abra automáticamente un informe de servicio y envíe datos de servicio recolectados al soporte de Lenovo mediante la función Llamar a casa cuando un dispositivo específico genera ciertos sucesos de mantenimiento, como una memoria no recuperable, para que se pueda abordar el problema.

### Antes de empezar

Asegúrese de que todos los puertos requeridos por XClarity Orchestrator y por la función Llamar a casa estén disponibles antes de habilitar la opción Llamar a casa. Para obtener más información sobre los puertos, consulte [Disponibilidad de puertos](#) en la documentación en línea de XClarity Orchestrator.

Asegúrese de que exista una conexión a las direcciones de Internet requeridas por la opción Llamar a casa. Para obtener información acerca de los firewalls, consulte [Firewall y servidores proxy](#) en la documentación en línea de XClarity Orchestrator.

Si XClarity Orchestrator accede a Internet mediante un proxy HTTP, asegúrese de que el servidor proxy esté configurado para usar la autenticación básica y que no esté configurado como un proxy de terminación. Para obtener más información sobre la configuración del proxy, consulte [Configurar valores de red](#) en la documentación en línea de XClarity Orchestrator.

**Importante:** Si la opción Llamar a casa está habilitada en XClarity Orchestrator y Lenovo XClarity Administrator, asegúrese de que se utilice Lenovo XClarity Administrator v2.7 o posterior para evitar duplicar los informes de servicio. Si la función Llamar a casa está habilitada en XClarity Orchestrator y deshabilitada en Lenovo XClarity Administrator, entonces Lenovo XClarity Administrator se admite v2.6 o posterior.

### Acerca de esta tarea

Cuando Llamar a casa está configurado y habilitado, y se produce un suceso de mantenimiento en un dispositivo específico, XClarity Orchestrator abre *automáticamente* un informe de servicio y transfiere los datos de servicio de ese dispositivo al Centro de Soporte de Lenovo.

**Importante:** Lenovo está comprometido con la seguridad. Los datos de servicio que normalmente se cargarían de forma manual a Soporte de Lenovo se envían automáticamente al Centro de Soporte de Lenovo a través de HTTPS utilizando TLS 1.2 o posterior. Los datos profesionales no se transmiten nunca. El acceso a los datos de servicio en el Centro de Soporte de Lenovo está restringido al personal de servicio autorizado.

Cuando Llamar a casa no está habilitado, puede abrir manualmente un informe de servicio y enviar los archivos de servicio al Centro de Soporte de Lenovo; para ello, siga las instrucciones de [Cómo abrir una página web de informe de soporte](#). Para obtener más información sobre recolectar archivos de servicio, consulte [Apertura manual de un informe de servicio en el Centro de Soporte de Lenovo](#) en la documentación en línea de XClarity Orchestrator.

Para obtener información sobre cómo ver los informes de servicio que se han abierto automáticamente mediante la función Llamar a casa, consulte [Visualización de estados e informes de servicio](#) en la documentación en línea de XClarity Orchestrator.

### Procedimiento

Para configurar Llamar a casa para la notificación automática de problemas, lleve a cabo los pasos siguientes.

Paso 1. En la barra de menú de XClarity Orchestrator, haga clic en **Administración** (⚙️) → **Servicio y soporte** y luego haga clic en **Configuración de Llamar a casa** en el panel de navegación izquierdo para mostrar la tarjeta Configuración de Llamar a casa.

### Configuración de Llamar a casa

Desde esta página, puede configurar una acción de Llamar a casa que envía automáticamente datos de servicio para cualquier punto final gestionado al soporte técnico de Lenovo, cuando ocurren ciertos sucesos de mantenimiento en un punto final gestionado.

[Declaración de privacidad de Lenovo](#)

Acepto la declaración de privacidad de Lenovo

#### Detalles del cliente

Número de cliente

#### Contacto principal para uso de varias asignaciones de grupos ?

Primera asignación de grupo

Última asignación de grupo

#### Contacto predeterminado

Estado de Llamar a casa: Habilitado Deshabilitado

Nombre de contacto	Calle
Correo electrónico	Ciudad
Número de teléfono	Estado/provincia
Nombre de la empresa	País/región
Método para contacto	Código zip/código postal

Ubicación del sistema ?

Paso 2. Revise el [Declaración de privacidad de Lenovo](#) y luego haga clic en **Acepto la Declaración de privacidad de Lenovo**

Paso 3. Especifique el número de cliente de Lenovo predeterminado para utilizarlo al notificar problemas.

Puede encontrar su número de cliente en el correo electrónico de prueba de derecho que recibió cuando compró su licencia de XClarity Orchestrator.

Paso 4. Cambie el estado de Llamar a casa a **Habilitar**.

Paso 5. Seleccione el contacto principal que desea utilizar de varias asignaciones de grupo.

Puede asignar un contacto de soporte principal a un grupo de dispositivos. Si un dispositivo pertenece a varios grupos, es posible que a cada grupo se le asigne un contacto principal diferente. Puede elegir usar la asignación de contacto principal para el primer grupo o el último grupo al que se asignó el dispositivo.

Paso 6. Rellene la información de contacto y el método de contacto preferido por el Soporte de Lenovo.

Si un dispositivo no pertenece a un grupo con un contacto principal asignado, el contacto predeterminado se usa para Llamar a casa.

Paso 7. Rellene la información de ubicación del sistema.

Paso 8. Haga clic en **Prueba de conexión de Llamar a casa** para verificar que XClarity Orchestrator pueda comunicarse con el Centro de Soporte de Lenovo.

Paso 9. Haga clic en **Aplicar**.

## Después de finalizar

Continúe la configuración inicial visitando [Configuración del reenvío de datos de sucesos](#).

---

## Configuración del reenvío de datos de sucesos

Puede reenviar los datos de suceso, de inventario y métricas desde Lenovo XClarity Orchestrator a aplicaciones externas, que puede utilizar para supervisar y analizar datos.

### Acerca de esta tarea

#### Datos de sucesos

XClarity Orchestrator puede despachar sucesos que se producen en su entorno a herramientas externas, según los criterios (filtros) que especifique. Todos los sucesos generados se supervisan para ver si coinciden con los criterios. Si coincide, el suceso se reenvía a la ubicación especificada utilizando el protocolo indicado.

XClarity Orchestrator admite el despacho de datos de suceso a las siguientes herramientas externas.

- **Correo electrónico.** Los datos de suceso se despachan a una o más direcciones de correo electrónico mediante SMTP.
- **Intelligent Insights.** Los datos de sucesos se reenvían en un formato predefinido a SAP Data Intelligence. A continuación, puede utilizar SAP Data Intelligence para gestionar y supervisar los datos de los sucesos.
- **REST.** Los datos de suceso se despachan a través de la red a un servicio web REST.
- **Syslog.** Los datos de suceso se despachan a través de la red a un servidor de registro central donde se pueden utilizar herramientas nativas para supervisar el syslog.

XClarity Orchestrator utiliza *filtros globales* para definir el alcance de los datos de suceso que se despacharán. Puede crear filtros de sucesos para despachar solo los sucesos con propiedades específicas, incluidos los códigos de suceso, las clases de suceso, los niveles de gravedad del suceso y los tipos de servicio. También puede crear filtros de dispositivo para despachar solo los sucesos generados por dispositivos específicos.

### Datos de inventario y de sucesos

XClarity Orchestrator puede reenviar todos los datos de inventario y de sucesos para todos los dispositivos hacia aplicaciones externas, que puede utilizar para supervisar y analizar datos.

- **Splunk.** Los datos de sucesos se reenvían en un formato predefinido a una aplicación Splunk. Entonces, puede utilizar Splunk para crear gráficos y tablas basados en datos de suceso. Puede definir múltiples configuraciones de Splunk; sin embargo, XClarity Orchestrator puede reenviar sucesos solo a una configuración de Splunk. Por lo tanto, solo se puede habilitar una configuración de Splunk a la vez.

### Datos de métrica

XClarity Orchestrator puede reenviar datos de métricas que recopila sobre dispositivos gestionados a la siguiente herramienta externa.

- **TruScale Infrastructure Services.** Los datos de métricas se reenvían en un formato predefinido a Lenovo TruScale Infrastructure Services. A continuación, puede utilizar TruScale Infrastructure Services para gestionar y supervisar los datos de métricas.

**Atención:** La información sobre el despachador de TruScale Infrastructure Services está destinada solo a los representantes del servicio de Lenovo.

Aunque puede definir varias configuraciones de despachadores de TruScale Infrastructure Services, XClarity Orchestrator solo puede reenviar datos de métricas a un despachador de TruScale Infrastructure Services. Por lo tanto, solo se puede habilitar un despachador de TruScale Infrastructure Services a la vez.

**Más información:**  [Conozca Lenovo TruScale Infrastructure Services](#)

Para obtener más información sobre el reenvío de datos de sucesos, consulte [Reenvío de datos de sucesos, inventario y métricas](#) en la documentación en línea de XClarity Orchestrator.

## Después de finalizar

Continúe la configuración inicial visitando [Conexión de gestores de recursos](#).

---

## Conexión de gestores de recursos

Lenovo XClarity Orchestrator supervisa y gestiona dispositivos a través de gestores de recursos y de aplicación.

### Antes de empezar

XClarity Orchestrator puede admitir un número ilimitado de gestores de recursos que gestionan colectivamente un máximo de 10,000 dispositivos en total.

Asegúrese de que los gestores de recursos sean compatibles (consulte [Hardware y software admitidos](#) en la documentación en línea de XClarity Orchestrator.).

Asegúrese de que los gestores de recursos estén en línea y sean accesibles en la red desde XClarity Orchestrator.

Asegúrese de que la cuenta de usuario que utiliza para la autenticación del gestor de recursos tenga los privilegios correctos. En el caso de XClarity Administrator, las cuentas de usuarios deben tener asignado el rol **lxc-supervisor**, **lxc-admin**, **lxc-security-admin**, **lxc-hw-admin** o **lxc-recovery**.

Asegúrese de que el administrador de recursos no tenga el número máximo de despachadores de sucesos admitidos. XClarity Orchestrator crea un despachador de sucesos en el gestor de recursos cuando se crea una conexión con ese gestor de recursos.

Cuando conecte un gestor de recursos que tenga un certificado firmado externamente:

- Asegúrese de que es un certificado X.509 v3. XClarity Orchestrator no se puede conectar a un gestor de recursos que tenga un certificado v1 firmado externamente.
- Asegúrese de que los detalles del certificado incluyan los siguientes requisitos.
  - El uso de clave debe contener
    - Acuerdo clave
    - Firma digital
    - Cifrado de clave
  - El uso de clave mejorada debe contener
    - Autenticación de servidor (1.3.6.1.5.5.7.3.1)
    - Autenticación de cliente (1.3.6.1.5.5.7.3.2)

## Acerca de esta tarea

XClarity Orchestrator es compatible con los siguientes gestores de recursos y de aplicación.

- **Lenovo XClarity Management Hub 2.0.** Gestiona, supervisa y aprovisiona dispositivos ThinkSystem y ThinkAgile. Se debe instalar un agente de UDC en cada dispositivo del cliente ThinkEdge para permitir la comunicación entre el dispositivo y XClarity Orchestrator.

**Importante:** El XClarity Management Hub 2.0 del proceso de registro es diferente del de otro gestor de recursos. Para obtener instrucciones detalladas, consulte .

- **Lenovo XClarity Management Hub.** Gestiona, supervisa y aprovisiona dispositivos del cliente ThinkEdge. Se debe instalar un agente de UDC en cada dispositivo del cliente ThinkEdge para permitir la comunicación entre el dispositivo y XClarity Orchestrator.

**Importante:** El XClarity Management Hub del proceso de registro es diferente del de otro gestor de recursos. Para obtener instrucciones detalladas, consulte .

- **Lenovo XClarity Administrator.** Gestiona, supervisa y aprovisiona dispositivos Lenovo con controladores de gestión de placa base.
- **Schneider Electric EcoStruxure IT Expert.** Gestiona y supervisa los recursos de la infraestructura.
- **VMware vRealize Operations Manager.**

Cuando conecta un XClarity Management Hub o un gestor de recursos de XClarity Administrator, XClarity Orchestrator:

- Recupera información acerca de todos los dispositivos gestionados por el gestor de recursos.
- Crea y habilita un despachador de sucesos (para un servicio web REST) en el servidor de gestión para supervisar y reenviar sucesos a XClarity Orchestrator.

La dirección de red (dirección IP o nombre de host) que proporciona se utiliza como nombre de gestor.

## Procedimiento

Para conectar un gestor de recursos o aplicación, siga estos pasos.

- Paso 1. Desde la barra de menú de XClarity Orchestrator, haga clic en **Recursos**  → **Gestores de recursos** para mostrarla tarjeta de Gestores de recursos.



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

Paso 3. Seleccione el tipo de gestor de recursos y rellene la información necesaria.

- **XClarity Management Hub 2.0 o XClarity Management Hub**
  1. Introduzca la clave de registro generada por la instancia del concentrador de gestión y, a continuación, haga clic en **Conectar**. Para obtener el token de solicitud de registro, inicie sesión en el portal del concentrador de gestión, haga clic en **Registro** y, a continuación, haga clic en **Crear clave de registro**.
  2. Copie la clave de registro de XClarity Orchestrator generada.

3. En el portal del concentrador de gestión, haga clic en **Registro**, después en **Instalar clave de registro**, pegue el token de registro de XClarity Orchestrator y, a continuación, haga clic en **Conectar**.

- **XClarity Administrator**

- Especifique el nombre de dominio o la dirección IP (IPv4 o IPv6) totalmente cualificados.No se admite el uso del nombre de host sin el nombre de dominio.
- Opcionalmente, cambie el puerto del gestor de recursos. El valor predeterminado es 443.
- Especifique la cuenta de usuario y contraseña que utilizará para iniciar sesión en Gestor de recursos.
- Opcionalmente, habilite **Recopilación de datos de análisis de unidad**. Cuando está habilitado, los datos de análisis de la unidad para los dispositivos ThinkSystem y ThinkAgile se recopilan a diario y se usan para fines de análisis predictivo.La Recopilación de datos de análisis de unidad solo se admite en XClarity Administrator v3.3.0 y versiones posteriores de los gestores de recursos.

**Atención:** El rendimiento del sistema podría verse afectado durante la recopilación de datos.

- **Experto de TI de EcoStruxure**. Especifique el nombre, la clave de token y la URL que se van a utilizar para la conexión.

- **vRealize Operations Manager**

- Especifique el nombre de dominio o la dirección IP (IPv4 o IPv6) totalmente cualificados.No se admite el uso del nombre de host sin el nombre de dominio.
- Opcionalmente, cambie el puerto del gestor de recursos. El valor predeterminado es 443.
- Opcionalmente, seleccione el origen de la autorización para los usuarios y los grupos.
- Especifique la cuenta de usuario y contraseña que utilizará para iniciar sesión en vRealize Operations Manager.

Paso 4. Haga clic en **Conectar**.

Se crea un trabajo para llevar a cabo esta operación. Puede supervisar el progreso del trabajo desde la tarjeta **Supervisión** (📄) → **Trabajos**. Si el trabajo no finalizó correctamente, haga clic en el enlace del trabajo para mostrar los detalles correspondientes (consulte .)

Cuando se establece una conexión con el gestor de recursos, el gestor se añade a la tabla.

Paso 5. Si eligió conectarse a un XClarity Management Hub, se muestra un cuadro de diálogo con una clave de registro.

Para completar la conexión, haga clic en **Copiar en el portapapeles** para copiar la clave de registro. A continuación, inicie sesión en XClarity Management Hub, haga clic en **Administración** → **Configuración de concentrador** y después en **Instalar clave de registro**. A continuación, pegue la clave de registro y haga clic en **Enviar**.

## Después de finalizar

Se completó la configuración inicial.



---

## Capítulo 5. Aplicación de licencias de XClarity Orchestrator

Lenovo XClarity Orchestrator es una aplicación de pago. Puede utilizar XClarity Orchestrator sin costo durante 90 días con la licencia de prueba gratuita; sin embargo, después de que finalice esta prueba gratuita, debe comprar e instalar las licencias adecuadas para seguir utilizando las funciones aplicables de XClarity Orchestrator y para obtener servicio y soporte de XClarity Orchestrator.

### Antes de empezar

Para obtener información acerca de cómo comprar licencias, póngase en contacto con su representante de Lenovo o con un business partner autorizado.

Se necesita una licencia para cada dispositivo gestionado que admita funciones avanzadas (configuración del servidor y despliegue del SO).

- Una licencia de chasis proporciona licencias para 14 dispositivos.
- Para los servidores de complejo escalable System x3850 X6 (6241), cada servidor necesita una licencia por separado, independientemente de las particiones.
- Para los servidores de complejo escalable System x3950 X6 (6241), si no están particionados, cada servidor necesita una licencia distinta. Si está particionado, cada partición necesita una licencia independiente.
- Los siguientes dispositivos *no admiten* funciones avanzadas y, por lo tanto, *no requieren* licencias para estas características; no obstante, se debe adquirir una licencia para cada uno de estos dispositivos con el fin de obtener servicio y soporte de XClarity Orchestrator.
  - Servidores ThinkServer
  - Servidores System x M4
  - Servidores System x X5
  - Servidores System x3850 X6 y x3950 X6 (3837)
  - Dispositivos de almacenamiento
  - Conmutadores

Debe ser miembro de un grupo de usuarios al que esté asignado el rol de **Supervisor** predefinido.

### Acerca de esta tarea

XClarity Orchestrator es compatible con las siguientes licencias.

- **XClarity Orchestrator.** Habilita los servidores de funciones de Orchestrator y de gestión base, chasis, conmutadores y dispositivos de almacenamiento, así como la autorización para el servicio y soporte de XClarity Orchestrator. Para las funciones de organización, se necesita una licencia en XClarity Orchestrator para cada dispositivo que admita la configuración del servidor y el despliegue del SO. Para el servicio y soporte de XClarity Orchestrator, se necesita una licencia para *cada dispositivo gestionado*.

El cumplimiento de la licencia se determina en función del número de dispositivos gestionados. El número de dispositivos gestionados no debe superar el número total de licencias en todas las claves de licencia activas de XClarity Orchestrator. Si no se cumple con el número de licencias de XClarity Orchestrator (por ejemplo, si las licencias caducan o si la gestión de dispositivos adicionales supera el número total de licencias activas), tiene un período de gracia de 90 días para instalar las licencias adecuadas. Si el período de gracia (incluida la prueba gratuita) para las licencias finaliza antes de que se instale el número de licencias necesario, *todas* las funciones de XClarity Orchestrator se deshabilitan (incluida la supervisión, la gestión básica y el análisis). Cuando inicie sesión, se le redirigirá a la página de información de licencia donde puede aplicar licencias adicionales.

Por ejemplo, si gestiona 100 servidores ThinkSystem adicionales y 20 conmutadores de bastidor utilizando una instancia existente de XClarity Administrator que está gestionando mediante XClarity Orchestrator, dispone de 90 días para comprar e instalar 100 licencias adicionales de XClarity Orchestrator antes de que todas las funciones se deshabiliten en la interfaz de usuario. No es necesario disponer de licencias para los 20 conmutadores de bastidor para utilizar las funciones de XClarity Orchestrator; no obstante, son necesarias si desea obtener servicio y soporte para XClarity Orchestrator. Si las funciones de XClarity Orchestrator están deshabilitadas, las funciones se vuelven a habilitar después de instalar las licencias suficientes para que se vuelvan a cumplir.

**Importante:** La licencia básica de XClarity Orchestrator es un requisito previo para las licencias de análisis de XClarity Pro y XClarity Orchestrator. Si el número de licencias de XClarity Pro o XClarity Orchestrator es conforme, pero el número de licencias básicas activas *no* es conforme, todas las funciones de XClarity Orchestrator (incluidas las de análisis), se deshabilitarán para todos los dispositivos.

- **Lenovo XClarity Pro.** Habilita las funciones de gestión avanzadas (configuración del servidor y despliegue del SO). Se necesita una licencia en XClarity Orchestrator para cada dispositivo que sea compatible con las funciones de gestión avanzadas.

El cumplimiento de la licencia se determina en función del número de dispositivos gestionados. El número de dispositivos gestionados no debe superar el número total de licencias en todas las claves de licencia activas de XClarity Pro. Cuando el número de licencias de XClarity Pro no es conforme, dispone de un período de gracia de 90 días para instalar las licencias adecuadas. Si el período de gracia (incluida la prueba gratuita) finaliza antes de que se instale el número de licencias necesario, las funciones de configuración del servidor y despliegue del SO se deshabilitan para *todos los dispositivos*.

Para obtener más información sobre las licencias de XClarity Pro, consulte [Licencias y la prueba gratuita de 90 días](#) en la documentación en línea de XClarity Administrator.

- **Análisis de XClarity Orchestrator.** Habilita las funciones de análisis. Se necesita una licencia en XClarity Orchestrator para cada dispositivo que sea compatible con las funciones de gestión avanzadas.

El cumplimiento de la licencia se determina en función del número de dispositivos gestionados. El número de dispositivos gestionados no debe superar el número total de licencias en todas las claves de licencia activas de análisis de XClarity Orchestrator. Si el número de licencias de análisis de XClarity Orchestrator no es conforme (por ejemplo, si las licencias caducan o si la gestión de dispositivos adicionales supera el número total de licencias activas), dispone de un período de gracia de 90 días para instalar las licencias adecuadas. Si el período de gracia (incluida la prueba gratuita) finaliza antes de que se instale el número de licencias necesario, se deshabilitan los menús de **Supervisión → Análisis** se deshabilitan y ya no podrá ver informes de análisis ni crear reglas ni consultas de alertas personalizadas para *todos los dispositivos*.

**Importante:** Después de instalar las licencias de análisis de XClarity Orchestrator, debe actualizar la interfaz de usuario.

**Nota:** Si instala las licencias de análisis de XClarity Orchestrator caducadas (superaron su fecha de caducidad más allá del periodo de caducidad de 90 días) y luego actualiza la interfaz de usuario, las funciones de análisis se deshabilitan. Esto significa que cualquier período activo de prueba o prueba se cancela, se detienen los servicios de análisis y se anulan las funciones de análisis. (Esto puede durar varios minutos). Puede volver a habilitar las funciones de análisis importando nuevas licencias válidas.

Una licencia *no está* vinculada a dispositivos específicos.

El periodo de activación comienza cuando se canjean las licencias.

Las licencias se instalan utilizando una *clave de activación* de licencia. Una vez que haya canjeado las licencias, puede crear una clave de activación para todas las licencias disponibles, o un subconjunto de ellas, y, a continuación, descargar e instalar la clave de activación en XClarity Orchestrator.

Cada vez que XClarity Orchestrator pasa a no estar en cumplimiento, el periodo de gracia se restablece a 90 días.

Si las licencias ya están instaladas, *no* se requieren nuevas licencias para actualizar a una nueva versión de XClarity Orchestrator.

Si está utilizando una licencia de prueba gratuita o dispone de un período de gracia para la conformidad y actualiza a una versión posterior de XClarity Orchestrator, la licencia de prueba o el período de gracia se restablecen a 90 días.

Al actualizar XClarity Orchestrator o si se produce una condición de error que requiera restaurar las claves de activación, puede usar claves de activación exportadas o descargar todas las claves de activación (para cada Id. de cliente) desde [Características del portal web on Demand](#) y luego importar las claves de activación (como claves de activación individuales o en grupo, como un archivo ZIP de claves) en XClarity Orchestrator.

Puede ver una lista de licencias de software actuales desde el [Características del portal web on Demand](#).

## Procedimiento

Para instalar licencias de XClarity Orchestrator, lleve a cabo los pasos siguientes.

Paso 1. Póngase en contacto con su representante de Lenovo o su socio comercial autorizado para adquirir licencias basadas en el número de dispositivos que desea gestionar.

Después de comprar licencias, se le envía un código de autorización en un *correo electrónico de prueba de derecho*. También puede recuperar el código de autorización de [Características del portal web on Demand](#), haciendo clic en **Recuperar código de autorización**. Si no recibe el correo electrónico y compró la licencia mediante un Business Partner, póngase en contacto con su Business Partner para solicitar el código de autorización.

El código de autorización es una cadena alfanumérica de 22 caracteres. Necesitará el código de autorización para completar el siguiente paso.

Paso 2. Obtenga las claves de activación de las licencias.

- **Creación de claves de activación a partir de un código de autorización**

1. Abra el [Características del portal web on Demand](#) desde un navegador web e inicie sesión en el portal utilizando su dirección de correo electrónico como su Id. de usuario.
2. Haga clic en la **clave de activación de solicitud**.
3. Seleccione **Ingresar un código de autorización único**.
4. Introduzca el código de autorización de 22 caracteres y haga clic en **Continuar**.
5. Introduzca el número de cliente de Lenovo en el campo **Número de cliente de Lenovo**.
6. Especifique el número de licencias que desea canjear en el campo **Canjear cantidad** y, a continuación, haga clic en **Continuar**. Para canjear todas las licencias disponibles en esta clave, coincida con el número en el campo **Licencias disponibles**.

Si canjea un subconjunto de licencias disponibles, puede canjear el resto de las licencias en otra clave de activación utilizando el mismo código de autorización.

7. Siga las indicaciones para introducir los detalles del producto y la información de contacto y haga clic en **Continuar** para generar la clave de activación.
8. Opcionalmente, especifique destinatarios adicionales para recibir las claves de activación.
9. Haga clic en **Enviar** para enviar las claves de activación. La persona asignada al pedido de compra y los destinatarios adicionales recibirán un correo electrónico con la clave de activación. La clave de activación es un archivo en formato .KEY.

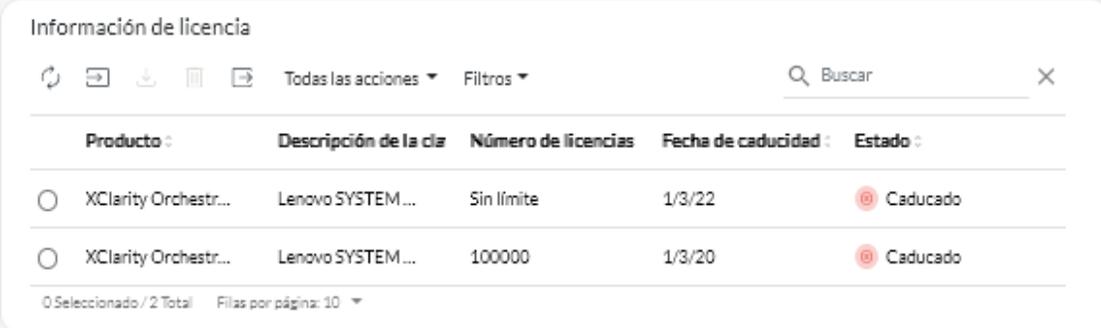
**Nota:** También puede descargar claves de activación (individualmente o en lote) desde el [Características del portal web on Demand](#) haciendo clic en el enlace **Descargar**.

- **Descarga de claves de activación existentes**

1. Abra el [Características del portal web on Demand](#) desde un navegador web e inicie sesión en el portal utilizando su dirección de correo electrónico como su Id. de usuario.
2. Haga clic en **Recuperar historial**.
3. Seleccione “Buscar en el historial mediante Número de cliente de Lenovo” como el **Tipo de búsqueda**.
4. Introduzca el Número de cliente de Lenovo en el campo **Valor de búsqueda**. El formato de número de cliente es 121XXXXXXX.
5. Haga clic en **Seleccionar todo** para descargar todas las claves de activación o seleccione las claves de activación individuales de la lista.
6. Haga clic en **Correo electrónico** para enviar por correo electrónico las claves, o haga clic en **Descargar** para descargar las claves a su sistema local.

Paso 3. Aplique licencias en XClarity Orchestrator.

1. En la barra de menús de XClarity Orchestrator, haga clic en **Mantenimiento**  y, a continuación, haga clic en la pestaña **Licencias** para mostrar la tarjeta de Información de licencia.



Producto	Descripción de la clave	Número de licencias	Fecha de caducidad	Estado
XClarity Orchestr...	Lenovo SYSTEM...	Sin límite	1/3/22	Caducado
XClarity Orchestr...	Lenovo SYSTEM...	100000	1/3/20	Caducado

2. Haga clic en el icono **Importar y aplicar**  para aplicar las licencias.
3. Arrastre y suelte el archivo de clave de activación para las licencias que desea aplicar al cuadro de diálogo Importar, o haga clic en **Examinar** para ubicar el archivo.

Para importar varias claves de activación, comprima el archivo .KEY en un archivo ZIP y seleccione el archivo ZIP para importarlo.

4. Haga clic en el icono **Importar** para importar y aplicar las licencias. Una vez completada la instalación, la clave de activación (licencia) se muestra en la tabla con el número de licencias instaladas y el periodo de activación (fechas de inicio y caducidad).

Paso 4. Si ha aplicado las licencias válidas después de que se hayan deshabilitado las funciones, cierre la sesión y, a continuación, vuelva a iniciar sesión para habilitar las funciones aplicables.

## Después de finalizar

Puede realizar las siguientes acciones desde la tarjeta de Información de licencia.

- Guarde una o más claves de activación seleccionadas en el sistema local haciendo clic en el icono **Guardar** .

Al exportar varias claves de activación, los archivos se descargan como un único archivo ZIP.

- Elimine claves de activación específicas haciendo clic en el icono de **Eliminar** .

## Cómo obtener ayuda

- Si tiene problemas y utilizó un Business Partner, póngase en contacto con su Business Partner para verificar la transacción y autorización.
- Si no recibe el comprobante electrónico de autorización, los códigos de autorización o las claves de activación, o si se enviaron a la persona incorrecta, póngase en contacto con uno de los representantes regionales, según su ubicación geográfica.
  - [ESDNA@lenovo.com](mailto:ESDNA@lenovo.com) (países de Norteamérica)
  - [ESDAP@lenovo.com](mailto:ESDAP@lenovo.com) (países de Asia-Pacífico)
  - [ESDEMEA@lenovo.com](mailto:ESDEMEA@lenovo.com) (países de Europa, Medio Oriente y Asia)
  - [ESDLA@lenovo.com](mailto:ESDLA@lenovo.com) (países de Latinoamérica)
  - [ESDChina@Lenovo.com](mailto:ESDChina@Lenovo.com) (China)
- Si la información acerca de la autorización no es correcta, póngase en contacto con Soporte de Lenovo en [SW\\_override@lenovo.com](mailto:SW_override@lenovo.com) e incluya la siguiente información.
  - Número de pedido
  - Su información de contacto, incluida la dirección de correo electrónico
  - La dirección física
  - Cambios que desea realizar
- Si tiene problemas o preguntas sobre cómo descargar la licencia, póngase en contacto con el Soporte de Lenovo en [-eSupport\\_-\\_Ops@lenovo.com](mailto:-eSupport_-_Ops@lenovo.com).



---

## Capítulo 6. Actualización de XClarity Orchestrator

Puede actualizar Lenovo XClarity Orchestrator para usar el software de organización más reciente.

### Antes de empezar

Más información:  [Cómo actualizar XClarity Orchestrator](#)

Debe ser miembro de un grupo de usuarios al que esté asignado el rol de **Supervisor** predefinido.

Solo se puede aplicar un paquete de correcciones de XClarity Orchestrator (como la v1.4.2) a una versión del mismo producto (como la v1.4.0 o la v1.4.1). Un paquete de correcciones contiene todas las correcciones anteriores (por ejemplo, la v1.4.2 contiene las mismas correcciones que la v1.4.1 y otras adicionales); sin embargo, un paquete de correcciones no contiene toda la base de código.

**Atención:** Revise las siguientes consideraciones antes de actualizar XClarity Orchestrator.

- **Para XClarity Orchestrator v2.0** El almacenamiento mínimo necesario para el dispositivo virtual es un **total de 551 GB** entre tres discos conectados. También debe conectar un tercer disco (disco 2) con un mínimo de 200 GB.

El dispositivo virtual de XClarity Orchestrator se debe apagar antes de añadir un nuevo disco duro.

Para añadir un nuevo disco duro al dispositivo virtual, lleve a cabo los siguientes pasos.

#### – Para ESXi que utiliza VMware vSphere

1. Conéctese al host a través de VMware vSphere Client.
2. Apague la máquina virtual de XClarity Orchestrator.
3. Haga clic en con el botón derecho del ratón en la máquina virtual y, a continuación, haga clic en **Editar valores**.
4. Seleccione **Añadir un nuevo dispositivo → Disco duro**.
5. Cambie el tamaño a 200 GB.
6. Haga clic en **Aceptar**.
7. Encienda la máquina virtual de XClarity Orchestrator.

#### – Para ESXi que utiliza VMware vCenter

1. Conéctese al host a través de VMware vCenter.
2. Apague la máquina virtual.
3. Abra la configuración de la máquina virtual y, a continuación, haga clic en **Añadir**.
4. Haga clic en **Disco duro → Crear un nuevo disco virtual**.
5. Seleccione **SCSI** para el formato de disco.
6. Configure la capacidad de HDD en 200 GB.
7. Haga clic en **Aceptar**.
8. Encienda la máquina virtual.

#### – Para Microsoft Hyper-V

1. En el Panel de Server Manager, haga clic en **Hyper-V**.
2. Haga clic en con el botón derecho del ratón en el servidor y haga clic en **Administrador de Hyper-V**.
3. Seleccione la máquina virtual de XClarity Orchestrator y, a continuación, haga clic en **Apagar** en el panel de acciones.
4. Haga clic en **Valores** para mostrar el cuadro de diálogo Valores.
5. Seleccione **IDE Controller 1**.

6. En el panel derecho, seleccione **Disco duro** y, a continuación, haga clic en **Añadir** para añadir un nuevo disco duro.
  7. En el panel derecho, seleccione **Archivo de disco duro virtual (.vhd)** y, a continuación, haga clic en **Nuevo** para mostrar el Asistente de nuevo disco duro virtual.
  8. Complete el asistente según se le solicite. Asegúrese de especificar un nombre de unidad de disco utilizando el formato .vhd (por ejemplo, LXC0-disk3.vhd) y establezca el tamaño en 200 GB.
  9. Seleccione la máquina virtual de XClarity Orchestrator y, a continuación, haga clic en **Iniciar** en el panel Acciones.
- **A XClarity Orchestrator v1.6.** Para actualizar a XClarity Orchestrator v1.6 se necesita XClarity Orchestrator v1.5. Si no está ejecutando XClarity Orchestrator v1.5, debe actualizar a XClarity Orchestrator v1.5 antes de actualizar a XClarity Orchestrator v1.6.
  - **A XClarity Orchestrator v1.5.** La actualización a XClarity Orchestrator versión 1.5 requiere XClarity Orchestrator versión 1.4. Si no está ejecutando XClarity Orchestrator versión 1.4, debe actualizar a XClarity Orchestrator versión 1.4 antes de actualizar a XClarity Orchestrator versión 1.5.
  - **A XClarity Orchestrator v1.4.** La actualización a XClarity Orchestrator versión 1.4 requiere XClarity Orchestrator versión 1.3. Si no está ejecutando XClarity Orchestrator versión 1.3, debe actualizar a XClarity Orchestrator versión 1.3 antes de actualizar a XClarity Orchestrator versión 1.4.
  - **A XClarity Orchestrator v1.3**
    - La actualización a XClarity Orchestrator versión 1.3 puede demorar dos horas o más en completarse. Para determinar si la actualización se completó, haga clic en **Mantenimiento** → **Actualizaciones del servidor de organización** y compruebe que la nueva versión aparece y que el Estado aplicado ya no es “Aplicando”.
    - **Atención:** Antes de actualizar XClarity Orchestrator a la versión 1.3, asegúrese de que el nombre de host del dispositivo virtual de XClarity Orchestrator sea **lxco** y que no haya ningún nombre de dominio establecido en la tarjeta Configuración de DNS en la página **Administración** (🔗) → **Redes**.
    - Los usuarios que tienen asignado el rol de **Supervisor** se agregan automáticamente al grupo de usuarios **SupervisorGroup** durante la actualización.
    - Los usuarios que tienen asignado el rol de **Operador** se agregan automáticamente al grupo de usuarios **OperatorLegacyGroup** durante la actualización. El grupo de usuarios **OperatorLegacyGroup** está asociado al rol **Heredado del operador**, que proporciona a los usuarios los mismos privilegios que el rol de **Operador** en las versiones anteriores. El rol **Heredado del operador** y el grupo de usuarios **OperatorLegacyGroup** quedarán obsoletos en una futura versión. Los grupos de usuarios existentes se asignan al rol **Operador** durante la actualización.
    - Se simplifica la creación de reglas para alertas de desaprobación personalizadas y personalizadas en XClarity Orchestrator versión 1.3. Las reglas de alertas personalizadas existentes no se migran al nuevo formato y se perderán después de que se complete la actualización.
  - **Desde XClarity Orchestrator versión 1.1**
    - Los usuarios que tienen asignado el rol de **Supervisor** se agregan automáticamente al grupo de usuarios **SupervisorGroup** durante la actualización.
    - Los usuarios que tienen asignado el rol de **Operador** se agregan automáticamente al grupo de usuarios **OperatorLegacyGroup** durante la actualización. El grupo de usuarios **OperatorLegacyGroup** está asociado al rol **Heredado del operador**, que proporciona a los usuarios los mismos privilegios que el rol de **Operador** en las versiones anteriores. El rol **Heredado del operador** y el grupo de usuarios **OperatorLegacyGroup** quedarán obsoletos en una futura versión. Los grupos de usuarios existentes se asignan al rol **Operador** durante la actualización.
    - Se simplifica la creación de reglas para alertas de desaprobación personalizadas y personalizadas en XClarity Orchestrator versión 1.3. Las reglas de alertas personalizadas existentes no se migran al nuevo formato y se perderán después de que se complete la actualización.

- El almacenamiento mínimo necesario para el dispositivo virtual es un **total de 301 GB** entre dos discos conectados. Debe aumentar el almacenamiento para el disco 0 al mínimo de 251 GB. También debe conectar un segundo disco (disco 1) con un mínimo de 100 GB. El dispositivo virtual de XClarity Orchestrator se debe apagar antes de añadir un nuevo disco duro.

Para añadir un nuevo disco duro al dispositivo virtual, lleve a cabo los siguientes pasos.

- **Para ESXi que utiliza VMware vSphere**

1. Conéctese al host a través de VMware vSphere Client.
2. Apague la máquina virtual de XClarity Orchestrator.
3. Haga clic en con el botón derecho del ratón en la máquina virtual y, a continuación, haga clic en **Editar valores**.
4. Seleccione **Añadir un nuevo dispositivo → Disco duro**.
5. Cambie el tamaño a 100 GB.
6. Haga clic en **Aceptar**.
7. Encienda la máquina virtual de XClarity Orchestrator.

- **Para ESXi que utiliza VMware vCenter**

1. Conéctese al host a través de VMware vCenter.
2. Apague la máquina virtual.
3. Abra la configuración de la máquina virtual y, a continuación, haga clic en **Añadir**.
4. Haga clic en **Disco duro → Crear un nuevo disco virtual**.
5. Seleccione **SCSI** para el formato de disco.
6. Configure la capacidad de HDD en 100 GB.
7. Haga clic en **Aceptar**.
8. Encienda la máquina virtual.

- **Para Microsoft Hyper-V**

1. En el Panel de Server Manager, haga clic en **Hyper-V**.
2. Haga clic en con el botón derecho del ratón en el servidor y haga clic en **Administrador de Hyper-V**.
3. Seleccione la máquina virtual de XClarity Orchestrator y, a continuación, haga clic en **Apagar** en el panel de acciones.
4. Haga clic en **Valores** para mostrar el cuadro de diálogo Valores.
5. Seleccione **IDE Controller 0**.
6. En el panel derecho, seleccione **Disco duro** y, a continuación, haga clic en **Añadir** para añadir un nuevo disco duro.
7. En el panel derecho, seleccione **Archivo de disco duro virtual (.vhd)** y, a continuación, haga clic en **Nuevo** para mostrar el Asistente de nuevo disco duro virtual.
8. Complete el asistente según se le solicite. Asegúrese de especificar un nombre de unidad de disco utilizando el formato .vhd (por ejemplo, LX00-disk2.vhd) y establezca el tamaño en 100 GB.
9. Seleccione la máquina virtual de XClarity Orchestrator y, a continuación, haga clic en **Iniciar** en el panel Acciones.

- **A XClarity Orchestrator v1.1**

- Todos los usuarios se añaden automáticamente al grupo de usuarios **SupervisorGroup**. Todos los usuarios tienen privilegios de supervisor de forma predeterminada una vez que se completa la actualización. Un usuario supervisor puede quitar los privilegios de supervisor de otros usuarios que no deben tener esos privilegios.
- Se quitan las configuraciones de LDAP externas existentes. Debe volver a configurar los servidores de autenticación LDAP externos una vez completada la actualización.

Durante el proceso de actualización, se cierra la sesión de todos los usuarios cuando se reinicia el servidor de organización. Debe esperar varios minutos hasta que el reinicio se complete. Una vez completada la

actualización y reiniciado el equipo, borre la memoria caché del navegador web y actualícelo antes de volver a iniciar sesión.

Asegúrese de realizar una copia de seguridad del dispositivo virtual de XClarity Orchestrator antes de instalar una actualización (consulte [Creación de copia de seguridad y restauración de datos de servidor de gestión](#) en la documentación en línea de XClarity Orchestrator).

Asegúrese de que todos los puertos y direcciones de Internet requeridos están disponibles antes de que intente actualizar XClarity Orchestrator. Para obtener más información, consulte [Disponibilidad de puertos y Firewall y servidores proxy](#).

## Procedimiento

Lleve a cabo los pasos siguientes para actualizar XClarity Orchestrator.

Paso 1. Descargue el archivo del paquete de actualización (.tgz) de [página web de descargas de XClarity Orchestrator](#) en una estación de trabajo que tenga conexión de red con el host de XClarity Orchestrator.

El archivo del paquete de actualización contiene todos los archivos necesarios: archivo de carga útil (.tar.gz), metadatos (.xml), historial de cambios (.chg) y léame (.txt).

Paso 2. En el menú principal de XClarity Orchestrator, haga clic en **Mantenimiento**  y luego haga clic en **Actualizaciones del servidor de organización** para mostrar la tarjeta Actualizaciones del servidor de organización.

Las del servidor de organización que son anteriores a la versión actualmente instalada se enumeran en la tabla con el estado de aplicado “No aplicable” y no pueden aplicarse al servidor de organización.

Actualización de Orchestrator Server

Actualice el software del servidor de organización al nivel más reciente.

Durante el proceso de actualización, se cierra la sesión de todos los usuarios cuando se reinicia el servidor de organización. Espere algunos minutos hasta que se complete el reinicio antes de volver a iniciar sesión.

Antes de actualizar, asegúrese de realizar una copia de seguridad del servidor de organización. [Más información.](#)

Todas las acciones Filtros Buscar

Archivo	Notas de li	Versión	Número d	Fecha de l	Estado apl	Reinicio ol	Tipo	Tamaño
No Di...	1	No Di...	No Di...	No Di...	Not A...	No Di...	No Di...	0.004...

0 Seleccionado / 1 Total Filas por página: 15

Paso 3. Pulse el icono de **Importar**  para mostrar el cuadro de diálogo Importar.

Paso 4. Arrastre el archivo del paquete de actualización completo (.tgz) y suéltelo en el cuadro de diálogo Importar, o bien haga clic en **Examinar** para ubicar el archivo.

Paso 5. Haga clic en **Importar**.

**Atención:** La importación de los archivos de actualización puede tardar varios minutos. Debe permanecer en la tarjeta de Actualizaciones del servidor de organización hasta que se complete el proceso de importación. Si se desplaza fuera de la tarjeta de Actualizaciones del servidor de organización, se cancelará el proceso de importación.

Una vez completada la importación, la actualización del servidor de organización se muestra en la tabla de la tarjeta Archivos del servidor de organización.

Puede supervisar el progreso de la importación haciendo clic en **Supervisión** (📈) → **Trabajos** en la barra de menú de XClarity Orchestrator.

Paso 6. En la tarjeta de Archivos del servidor de organización, seleccione el paquete de actualización que desea instalar.

Paso 7. Haga clic en el icono **Aplicar actualizaciones** (📄).

Puede supervisar el progreso de la actualización haciendo clic en **Supervisión** (📈) → **Trabajos** en la barra de menú de XClarity Orchestrator.

Paso 8. Espere a que se complete la actualización y que XClarity Orchestrator se reinicie. El proceso de actualización puede tardar varios minutos.

Si tiene acceso al host del dispositivo virtual, puede controlar el progreso desde la consola del dispositivo virtual, por ejemplo:

```
Lenovo XClarity Orchestrator Version x.x.x
```

```
-----
```

```
eth0    Link encap:Ethernet  HWaddr 2001:db8:65:12:34:56
        inet addr: 192.0.2.10  Bcast 192.0.2.55  Mask 255.255.255.0
        inet6 addr: 2001:db8:56ff:fe80:bea3/64 Scope:Link
```

```
=====
=====
```

```
You have 118 seconds to change IP settings. Enter one of the following:
 1. To set a static IP address for Lenovo XClarity virtual appliance eth0 port
 2. To use a DHCP address for Lenovo XClarity virtual appliance eth0 port
 3. To select subnet for Lenovo XClarity virtual appliance internal network
 x. To continue without changing IP settings
... ..
```

Paso 9. Borre la memoria caché del navegador web y vuelva a cargarlo.

Una vez completada, la columna **Estado aplicado** cambia a “Aplicado”.

## Después de finalizar

Puede realizar las siguientes acciones desde la tarjeta Archivos del servidor de organización.

- Ver la versión actual y el número de Build para la instancia de XClarity Orchestrator haciendo clic en el menú de **Cuenta de usuario** (👤) en la barra de título de XClarity Orchestrator y luego haciendo clic en **Acerca de**.
- Ver el historial de actualizaciones para una actualización específica que se aplicó a XClarity Orchestrator al hacer clic en el vínculo de estado de la actualización de la columna **Estado aplicado**.
- Guardar una actualización seleccionada del servidor de organización en el sistema local haciendo clic en el icono **Guardar como** (📄).
- Eliminar una actualización del servidor de organización seleccionado al hacer clic en el icono **Eliminar** (🗑️).



---

## Capítulo 7. Desinstalación de XClarity Orchestrator

Puede desinstalar el dispositivo virtual Lenovo XClarity Orchestrator mediante las herramientas de gestión de la máquina virtual.

### Procedimiento

Para desinstalar XClarity Orchestrator, lleve a cabo los pasos siguientes.

Paso 1. Desconecte y quite todo Gestores de recursos.

- a. Desde la barra de menú de XClarity Orchestrator, haga clic en **Recursos** (⚙️) → **Gestor de recursos** para mostrar la tarjeta de Gestores de recursos.
- b. Seleccionar todo Gestores de recursos
- c. Haga clic en el icono **Eliminar** (🗑️).

Paso 2. Desinstale XClarity Orchestrator utilizando sus herramientas de gestión de máquina virtual.

- **ESXi que utiliza VMware vCenter**

1. Conéctese al host a través de VMware vCenter.
2. Haga clic con el botón derecho del ratón en la XClarity Orchestrator máquina virtual en el inventario de cliente del **Host VMware** y luego seleccione **SO de invitado** en el menú emergente.
3. Haga clic en **Apagar**.
4. Haga clic con el botón derecho del ratón en la máquina virtual en el inventario de cliente del **Host VMware** y luego seleccione **SO de invitado** en el menú emergente.
5. Haga clic en **Eliminar**.

- **ESXi usando VMware vSphere**

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

- **Hyper-V**

1. En el panel de **Gestor de servidor**, haga clic en **Hyper-V**.
2. Haga clic con el botón derecho del ratón en el servidor y haga clic en **Administrador de Hyper-V**.
3. Haga clic con el botón derecho en la XClarity Orchestrator máquina virtual y, a continuación, haga clic en **Apagar**.
4. Haga clic con el botón derecho otra vez en la máquina virtual y, a continuación, haga clic en **Eliminar**.





**Lenovo**