Lenovo XClarity Administrator
Guía de planificación e instalación de entornos Docker

Versión 4.3

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 Administrator.

Cuarta edición (Abril 2025)

Contenido

Figuras

Tablas

Resumen de los cambios

Las revisiones de seguimiento del software de gestión Lenovo XClarity Administrator proporcionan soporte para nuevo hardware, así como 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.

Para obtener información acerca del hardware compatible (incluidos los servidores, los chasis y los conmutadores Flex), consulte Requisitos previos de hardware y software.

Para obtener información sobre cambios en versiones anteriores, consulte Novedades en la documentación en línea de XClarity Administrator.

Esta versión admite el hardware nuevo siguiente.

- **Servidores y dispositivos**
  - ThinkEdge SE100 (7DGR)
  - ThinkSystem SC750 V4 (7DDJ)
  - ThinkSystem SR630 V4 (7DGA, 7DGB, 7DG8, 7DG9, 7DLM)
  - ThinkSystem SR650 V4 (7DGC, 7DGD, 7DGE, 7DGF, 7DLN)
  - ThinkSystem SR680a V3 (7DM9)
- **Conmutadores**
  - ThinkSystem DB710S (7DHN)
- **Dispositivos de almacenamiento**
  - SAS híbrida de ThinkSystem DE4200H (7DCA, 7DCQ)
  - Matriz all-flash de ThinkSystem DE4800F (7DCC)
  - SAS híbrida de ThinkSystem DE4800H (7DCB, , 7DCR, 7DCS)
  - Matriz all-flash de ThinkSystem DG5200 (7DHY)
  - Matriz all-flash de ThinkSystem DG7200 (7DHZ)
  - Matriz all-flash de ThinkSystem DM3200F (7DJ0)
  - Matriz all-flash de ThinkSystem DM5200F (7DJ2)
  - Matriz de flash híbrida de ThinkSystem DM5200H (7DJ1)
  - Matriz all-flash de ThinkSystem DM7200F (7DJ3)

Esta versión no presenta mejoras adicionales en la planificación o instalación.

Capítulo 1. Lenovo XClarity Administrator Descripción general

Lenovo XClarity Administrator es una solución centralizada de gestión de recursos que simplifica la gestión de la infraestructura, acelera las respuestas y mejora la disponibilidad de los sistemas y las soluciones de servidor de Lenovo®. Funciona como un dispositivo virtual que automatiza la detección, el inventario, el seguimiento, la supervisión y el aprovisionamiento de servidores, redes y hardware de almacenamiento en un entorno seguro.

Más información:

- XClarity Administrator: gestión de hardware como software
- XClarity Administrator: descripción general

XClarity Administrator proporciona una interfaz central que permite realizar las siguientes funciones en todos los dispositivos gestionados.

Gestión del hardware

XClarity Administrator permite realizar una gestión del hardware sin agentes. Puede detectar automáticamente dispositivos gestionables, incluyendo servidores, redes y hardware de almacenamiento. Se recopilan datos de los dispositivos gestionados, por lo que es posible obtener una vista rápida del inventario de hardware gestionado y de su estado.

Existen varias tareas de gestión para cada dispositivo compatible, que incluyen la visualización del estado y las propiedades, la configuración del sistema y los valores de red, el inicio de las interfaces de gestión, encender y apagar y el control remoto. Para obtener más información acerca de cómo gestionar dispositivos, consulte Gestión del chasis, Gestión de servidores y Gestión de conmutadores en la documentación en línea de XClarity Administrator.

Consejo: Los servidores, redes y hardware de almacenamiento que se pueden gestionar mediante XClarity Administrator se conocen como *dispositivos*. El hardware que está bajo gestión de XClarity Administrator se conoce como *dispositivos gestionados*.

Puede utilizar la vista de bastidores de XClarity Administrator para agrupar sus dispositivos gestionados a fin de reflejar la configuración física de los bastidores en su centro de datos. Para obtener más

información acerca de los bastidores, consulte Gestión de bastidores en la documentación en línea de XClarity Administrator.

Más información:

- XClarity Administrator: detección
- XClarity Administrator: inventario
- XClarity Administrator: control remoto

Supervisión de hardware

XClarity Administrator proporciona una vista centralizada de todos los sucesos y todas las alertas que se generan en los dispositivos gestionados. Se envía una alerta o un suceso a XClarity Administrator y estos se muestran en el registro de sucesos o de alertas. El Panel de mandos y la barra de estado muestran un resumen de las alertas y de los sucesos que se han producido. Los sucesos y las alertas de un dispositivo específico pueden consultarse en la página de detalles Alertas y Sucesos del dispositivo de gestión de que se trate.

Para obtener más información acerca de cómo supervisar el hardware, consulte Trabajo con sucesos y Trabajo con alertas en la documentación en línea de XClarity Administrator.

Más información: XClarity Administrator: supervisión

Gestión de configuración

Puede aprovisionar y preaprovisionar con rapidez todos sus servidores utilizando una configuración coherente. Los valores de configuración (como el almacenamiento local, los adaptadores de E/S, los valores de arranque, el firmware, los puertos y los valores del controlador de gestión y la UEFI) se guardan como patrón de servidor que puede aplicarse a uno o varios servidores gestionados. Cuando los patrones de servidor se actualizan, los cambios se despliegan automáticamente en los servidores aplicados.

Los patrones de servidor también integran el soporte para la virtualización de direcciones de E/S, por lo que puede virtualizar conexiones de malla Flex System o readaptar servidores sin interrupciones en la malla.

Para obtener más información sobre la configuración de servidores, consulte Configuración de servicios usando XClarity Administrator en la XClarity Administrator documentación en línea.

Más información:

- XClarity Administrator: implementación básica a clúster
- XClarity Administrator: patrones de configuración

Política de conformidad y actualizaciones

La gestión del firmware se simplifica asignando políticas de cumplimiento de firmware a los dispositivos gestionados. Cuando crea y asigna una política de cumplimiento a los dispositivos gestionados, XClarity Administrator supervisa los cambios en el inventario correspondiente a dichos dispositivos y señala los dispositivos que no cumplen dicha política.

Si un dispositivo no cumple una política, puede utilizar XClarity Administrator para aplicar y activar actualizaciones de firmware para todos los dispositivos de dicho dispositivo desde el repositorio de actualizaciones de firmware que esté gestionando.

Nota: La actualización del repositorio y la descarga de actualizaciones de firmware requiere una conexión a Internet. Si XClarity Administrator no dispone de conexión a Internet, puede importar manualmente las actualizaciones de firmware al repositorio.

Para obtener más información sobre la actualización de firmware, consulte Actualización de firmware en dispositivos gestionados en la XClarity Administrator documentación en línea.

Más información:

- XClarity Administrator: implementación básica a clúster
- XClarity Administrator: actualización de firmware
- XClarity Administrator: aprovisionamiento de actualizaciones de seguridad de firmware

Despliegue del sistema operativo

Puede utilizar XClarity Administrator para gestionar un repositorio de imágenes del sistema operativo y para desplegar imágenes del sistema operativo hasta en 28 servidores gestionados de manera simultánea.

Para obtener más información sobre el despliegue de sistemas operativos, consulte Despliegue de la imagen de un sistema operativo en la XClarity Administrator documentación en línea.

Más información:

- XClarity Administrator: implementación básica a clúster
- XClarity Administrator: despliegue del sistema operativo

Autenticación de dispositivo

XClarity Administrator utiliza los siguientes métodos para la autenticación con chasis y servidores gestionados.

- **Autenticación gestionada**. Al habilitar la autenticación gestionada, las cuentas de usuarios creadas en XClarity Administrator se utilizan para la autenticación en los chasis y servidores gestionados.

  Para obtener más información sobre los usuarios, consulte Gestión de cuentas de usuario en la XClarity Administrator documentación en línea.

- **Autenticación local**. Cuando la autenticación gestionada está deshabilitada, las credenciales almacenadas que se definen en XClarity Administrator se usan para autenticar servidores gestionados. Las credenciales almacenadas deben corresponder con una cuenta de usuario activa en el dispositivo o con Active Directory.

  Para obtener más información sobre credenciales almacenadas, consulte Gestión de credenciales almacenadas en la documentación en línea de XClarity Administrator.

Gestión de autenticación

XClarity Administrator proporciona un servidor de autenticación centralizado para crear y gestionar todas las cuentas de usuario y para gestionar y autenticar las credenciales de los usuarios. El servidor de autenticación se crea automáticamente cuando el servidor de gestión se inicia por primera vez. Las cuentas de usuarios creadas para XClarity Administrator también se utilizan para iniciar sesión en los chasis y servidores gestionados en el modo de autenticación gestionada. Para obtener más información sobre los usuarios, consulte Gestión de cuentas de usuario en la XClarity Administrator documentación en línea.

XClarity Administrator admite tres tipos de servidores de autenticación:

- **Servidor de autenticación local**. De forma predeterminada, XClarity Administrator está configurado para utilizar el servidor de autenticación local que reside en el nodo de gestión.
- **Servidor LDAP externo**. Actualmente, solo se admite Microsoft Active Directory. Este servidor debe residir en un servidor de Microsoft Windows externo conectado a la red de gestión.Cuando se utiliza un servidor LDAP externo, el servidor de autenticación local se deshabilita.
- **SAML externo 2.0 proveedor de identidad**. Actualmente, se admiten Microsoft Active Directory Federation Services (AD FS). Además de ingresar un nombre de usuario y contraseña, se puede

configurar una autenticación de varios factores para habilitar una seguridad adicional al solicitar un código PIN, la lectura de una tarjeta inteligente y un certificado de cliente.

Para obtener más información sobre los tipos de autenticación, consulte Gestión del servidor de autenticación en la XClarity Administrator documentación en línea.

Cuando crea una cuenta de usuario, se asigna a la misma un grupo de roles predefinido o personalizado a fin de controlar el nivel de acceso para dicho usuario. Para obtener más información acerca de los grupos de roles, consulte Creación de un grupo de roles en la documentación en línea de XClarity Administrator.

XClarity Administrator incluye un registro de auditoría que proporciona un historial de las acciones de los usuarios, tales como iniciar sesión , crear nuevos usuarios o cambiar la contraseña de estos. Para obtener más información sobre el registro de auditoría, consulte Trabajo con sucesos en la XClarity Administrator documentación en línea.

Seguridad

Si su entorno debe cumplir con las normas NIST SP 800-131A, XClarity Administrator puede ayudarle a conseguir un entorno que se ajuste plenamente a dichas normas.

XClarity Administrator admite certificados SSL autofirmados (emitidos por una entidad de certificación interna) y certificados SSL externos (emitidos por una entidad de certificación privada o comercial).

Los firewall en chasis y servidores se pueden configurar para que acepten únicamente solicitudes entrantes de XClarity Administrator.

Para obtener más información sobre la seguridad, consulte Implementación de un entorno seguro en la documentación en línea de XClarity Administrator.

Servicio técnico y soporte

XClarity Administrator se puede configurar para que automáticamente recopile y envíe archivos de diagnóstico a su proveedor de servicio de preferencia cuando ocurran ciertos sucesos de mantenimiento en XClarity Administrator y en los dispositivos gestionados. Puede elegir enviar los archivos de diagnóstico a Lenovo Soporte mediante Llamar a casa o a otro proveedor de servicio mediante SFTP. También puede recopilar los archivos de diagnóstico de forma manual, abrir un registro de problemas y enviar archivos de diagnóstico al LenovoCentro de soporte.

Más información:  XClarity Administrator: servicio y soporte

Automatización de tareas utilizando scripts

XClarity Administrator puede integrarse en plataformas externas de gestión y automatización de más alto nivel a través de interfaces de programación de aplicaciones (API) REST. Utilizando las API REST, XClarity Administrator puede integrarse fácilmente con la infraestructura de gestión de la que dispone.

El kit de utilidades PowerShell proporciona una biblioteca de cmdlets para automatizar el aprovisionamiento y la gestión de recursos para una sesión de Microsoft PowerShell. El kit de utilidades de Python proporciona una biblioteca basada en Python de comandos y API para el aprovisionamiento automático y la gestión de recursos del entorno de un OpenStack, como Ansible o Puppet. Ambos kits de herramientas proporcionan una interfaz para que las REST API de XClarity Administrator para automatizar funciones como:

- Inicio de sesión en XClarity Administrator
- Gestionar y anular la gestión de chasis, servidores, dispositivos de almacenamiento y conmutadores de la parte superior del bastidor (dispositivos)
- Recopilación y visualización de datos de inventario para los dispositivos y los componentes
- Despliegue de una imagen del sistema operativo en uno o varios servidores

- Configuración de servidores mediante el uso de patrones de configuración
- Aplicación de actualizaciones de firmware en dispositivos

Integración con otro software gestionado

Los módulos de XClarity Administrator integran XClarity Administrator con el software de gestión de productos de terceros para proporcionar las funciones de detección, supervisión, configuración y gestión para reducir los costes y la complejidad de la administración rutinaria en los dispositivos compatibles.

Para obtener más información acerca de XClarity Administrator, consulte los siguientes documentos:
- Lenovo XClarity Integrator para Microsoft System Center
- Lenovo XClarity Integrator para VMware vCenter

Para obtener información adicional, consulte Consideraciones de gestión.

Más información:
-  Descripción general de Lenovo XClarity Integrator para Microsoft System Center
-  Lenovo XClarity Integrator para VMware vCenter

Documentación

La documentación de XClarity Administrator se actualiza en línea de forma periódica en inglés. Para consultar la información y los procedimientos más recientes, consulte la Documentación en línea de XClarity Administrator.

La documentación en línea está disponible en los siguientes idiomas:
- Alemán (de)
- Inglés (en)
- Español (es)
- Francés (fr)
- Italiano (it)
- Japonés (ja)
- Coreano (ko)
- Portugués de Brasil (pt-BR)
- Ruso (ru)
- Tailandés (th)
- Chino simplificado (zh-CN)
- Chino tradicional (zh-TW)

El inglés se muestra de forma predeterminada. Puede cambiar el idioma de la documentación en línea de las siguientes maneras.

- Seleccione su idioma en el menú desplegable de idiomas que se encuentra en el banner.
- Añada <*language_code*> después de `https://pubs.lenovo.com/lxca/`, por ejemplo, para mostrar la documentación en línea en chino simplificado.
  `https://pubs.lenovo.com/lxca/zh-CN/lxca_overview`

Capítulo 2. Planificación para XClarity Administrator

Antes de instalar Lenovo XClarity Administrator, revise las consideraciones siguientes, que le ayudarán a planificar la instalación y la gestión diaria.

Licencias y la prueba gratuita de 90 días

Lenovo XClarity Administrator ofrece una licencia de prueba gratuita de 90 días, que le permite utilizar todas las funciones disponibles durante un tiempo limitado.

Puede determinar el estado de la licencia, incluido el número de días quedan de la licencia de prueba, al hacer clic en el menú de acciones del usuario (

) en la barra de título de XClarity Administrator y, después, al hacer clic en **Acerca de**.

XClarity Administrator es compatible con la siguiente licencia.

- **Lenovo XClarity Pro**. Cada licencia proporciona los siguientes derechos para un único dispositivo.
  - Servicio técnico y soporte para Lenovo XClarity Integrator
  - Servicio técnico y soporte para XClarity Administrator
  - Funciones avanzadas dentro de XClarity Administrator:
    - Configuración de servidores mediante el uso de patrones de configuración
    - Despliegue de sistemas operativos
    - Informar a los problemas de XClarity Administrator mediante la función Llamar a casa (Llamar a casa para las alertas de hardware no se ve afectada).

Debe adquirir una licencia para cada dispositivo gestionado que sea compatible con las funciones avanzadas. Una licencia no está vinculada a un dispositivo específico.

El cumplimiento de la licencia se determina en función del número de dispositivos administrados que admiten las funciones avanzadas. El número de dispositivos administrados no debe superar el número de licencias en todas las claves de licencia activas. Si XClarity Administrator no cumple con las licencias instaladas (por ejemplo, si las licencias caducan o si la administración de dispositivos adicionales supera el número total de licencias activas), tiene un período de gracia de 90 días para instalar las licencias adecuadas. Cada vez que XClarity Administrator pasa a no estar en cumplimiento, el periodo de gracia se restablece a 90 días. Si el periodo de gracia (incluida la prueba gratuita) finaliza antes de que se cumplan las licencias, las funciones avanzadas están deshabilitadas para todos los dispositivos.

Notas:

- Las características de configuración del servidor y de despliegue del sistema operativo se deshabilitan cuando finaliza el periodo de gracia.
- La función Llamar a casa para los problemas de XClarity Administrator (la característica Llamar a casa de software) está deshabilitada cuando las licencias están fuera de conformidad. No hay un periodo de gracia para esta función. Sin embargo, la función Llamar a casa para las alertas de hardware no se ve afectada.

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

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

Para obtener información acerca de cómo instalar la licencia, consulte Instalación de licencia de habilitación de funciones completas en la documentación en línea de XClarity Administrator.

Requisitos previos de hardware y software

El dispositivo de gestión de Lenovo XClarity Administrator se ejecuta en una máquina virtual en un sistema host.

Requisitos de hipervisor

Entornos de contenedor

Se admite que el siguiente entorno de contenedor se ejecute XClarity Administrator como un contenedor.

- Docker v20.10.9
- Docker-compose v1.29.2

Hipervisores

Se admiten los siguientes hipervisores para ejecutar XClarity Administrator como un dispositivo virtual.

- Citrix Hypervisor v8.2
- Citrix XenServer v7.6
- CentOS 8[1]
- Microsoft Windows Server 2022 con Hyper-V instalado
- Microsoft Windows Server 2019 con Hyper-V instalado
- Nutanix Acropolis Hypervisor (AHV)
- Red Hat Enterprise Linux v9.x con la máquina virtual basada en Kernel (KVM) versión 6.2.0 instalada
- RedHat Enterprise Linux v8.x con KVM v2.12.0 instalado
- Rocky Linux 8.x y 9.x con KVM v7.0.0 instalado
- Servidor Ubuntu 22.04.x LTS con KVM v6.2.0 instalado
- Servidor Ubuntu 20.04.2 LTS con KVM v4.2.3 instalado
- VMware ESXi 8.0
- VMware ESXi 7.0, U1, U2 y U3
- VMware ESXi 6.7, U1, U2[2] y U3

Notas:

1. Red Hat ya no actualiza CentOS Linux. Considere la migración a Red Hat Enterprise Linux en su lugar (consulte Red Hat: Cómo convertir de CentOS u Oracle Linux a la página web de RHEL).
2. Para VMware ESXi 6.7 U2, debe utilizar la imagen ISO VMware-ESXi-6.7.0.update02-13981272-LNV-20190630.iso o posterior.

Para VMware y Citrix, la máquina virtual está disponible como plantilla OVF. Para Hyper-V y Nutanix AHV, la máquina virtual es una imagen de disco virtual (VHD). Para CentOS y KVM, la máquina virtual está disponible como formato qcow2.

Importante: Para entornos Hyper-V que se ejecutan en invitados Linux con una base kernel 2.6 y que utilizan grandes cantidades de memoria para el dispositivo virtual, debe deshabilitar el uso del acceso no uniforme a la memoria (NUMA) en el panel de valores de Hyper-V del administrador de Hyper-V. El cambio de este valor requiere un reinicio de su servicio Hyper-V, que también reinicia todas las máquinas virtuales que se encuentran en ejecución. Si este valor no está deshabilitado, el dispositivo virtual de XClarity Administrator puede experimentar problemas durante el arranque inicial.

Requisitos de hardware

Se deben cumplir los siguientes *requisitos mínimos* para XClarity Administrator. Dependiendo del tamaño de su entorno y del uso que haga de los Patrones de configuración, puede que se necesiten recursos adicionales para obtener un óptimo rendimiento.

- Dos microprocesadores virtuales

  Notas: XClarity Administrator v4.2 y versiones posteriores requieren el uso del conjunto de instrucciones AVX.
  - Intel: procesador de núcleo Sandy Bridge o versiones posteriores, Tiger Lake o later Celeron, o procesador Pentium
  - AMD: procesador Bulldozer o versiones posteriores
- 8 GB de memoria
- 192 GB de almacenamiento para su uso por el dispositivo virtual XClarity Administrator.
- Mostrar con una resolución mínima de 1024 píxeles de ancho (XGA)

La siguiente tabla enumera las configuraciones recomendadas mínimas para un número especificado de dispositivos. Tenga en cuenta que si ejecuta la configuración mínima, puede experimentar tiempos de finalización mayores que lo previsto para las tareas de gestión. Para las tareas de aprovisionamiento como el despliegue del sistema operativo, las actualizaciones de firmware y la configuración de servidor, es posible que deba aumentar los recursos temporalmente.

Cantidad de dispositivos gestionados	Configuración de CPU/memoria virtual
0 a 100 dispositivos	2 vCPU, 8 GB de RAM
100 a 200 dispositivos	4 vCPU, 10 GB de RAM
200 a 400 dispositivos	6 vCPU, 12 GB de RAM
400 a 600 dispositivos	8 vCPU, 16 GB de RAM
600 a 800 dispositivos	10 vCPU, 20 GB de RAM
800 a 1000 dispositivos	12 vCPU, 24 GB de RAM

Notas:

- Una instancia única XClarity Administrator puede admitir un máximo de 1000 dispositivos.
- Para las recomendaciones más recientes y las consideraciones de rendimiento adicionales, consulte el XClarity Administrator: guía de rendimiento (documentación técnica).
- Dependiendo del tamaño de su entorno gestionado y del modelo utilizado en su instalación, es posible que deba agregar recursos para mantener un rendimiento aceptable. Si bebe frecuentemente que el uso del procesador en el panel de recursos del sistema muestra valores altos o muy altos, considere agregar 1 a 2 núcleos de procesador virtuales. Si persiste el uso de memoria superior al 80 % en inactividad, considere la posibilidad de agregar 1 a 2 GB de RAM. Si su sistema responde en una configuración como se define en la tabla, considere la posibilidad de ejecutar la máquina virtual durante un período más largo para determinar el rendimiento del sistema.
- Para obtener información acerca de cómo liberar espacio del disco borrando recursos de XClarity Administrator que ya no necesita, consulte Gestión del espacio en el disco duro en la documentación en línea de XClarity Administrator.

Requisitos de software

- **Servidor de organización**

  Si gestiona una gran cantidad de dispositivos con varias instancias de XClarity Administrator, puede centralizar la supervisión, la gestión, el aprovisionamiento y el análisis con Lenovo XClarity Orchestrator.

XClarity Orchestrator puede admitir un número ilimitado de instancias de XClarity Administrator que gestionan de forma conjunta un máximo de **10 000** dispositivos que no son del cliente ThinkEdge.

Para gestionar instancias de XClarity Administrator versión 4.0 o posterior con Lenovo XClarity Orchestrator, se requiere XClarity Orchestrator versión 2.0 o posterior.

- **Servidor de autenticación**

  De forma predeterminada, XClarity Administrator usa un servidor con Lightweight Directory Access Protocol (LDAP) para autenticar credenciales de usuario. Puede optar por utilizar un servidor de autenticación externo en su lugar.

  Si decide usar un servidor de autenticación externo, solo se admite Microsoft Active Directory en ejecución en Windows Server 2008 o posterior.

  Si decide usar un proveedor de identidad SAML, solo se admiten las versiones 2.0 o posterior de Microsoft Active Directory Federation Services (AD FS) en ejecución en Windows Server 2012.

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

  Consejo: considere la posibilidad de utilizar un sistema host en el que XClarity Administrator esté instalado como servidor NTP. Si lo hace, asegúrese de que se pueda acceder a dicho sistema mediante la red de gestión.

Recursos gestionables

Una sola instancia de XClarity Administrator puede gestionar, supervisar y aprovisionar un máximo de **1000** dispositivos físicos.

Encontrará una lista completa de los dispositivos y las opciones compatibles (como I/O, DIMM y adaptadores de almacenamiento), niveles de firmware mínimos necesarios y consideraciones sobre las limitaciones en el Soporte de XClarity Administrator: página web de compatibilidad haciendo clic en la pestaña **Compatibilidad** y después en el enlace de los tipos de dispositivos correspondientes.

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

Restricción: si el sistema host en el que está instalado XClarity Administrator es un servidor de bastidor o un nodo de cálculo gestionado, no puede utilizar XClarity Administrator para aplicar actualizaciones de firmware a dicho sistema host o al chasis entero al mismo tiempo. Al aplicar las actualizaciones de firmware en el sistema host, este debe reiniciarse. Al reiniciar el sistema host, también se reinicia XClarity Administrator, por lo que XClarity Administrator deja de estar disponible para completar las actualizaciones en el sistema host.

Navegadores web compatibles

La interfaz web XClarity Administrator funciona con los siguientes navegadores web.
- Chrome™ 48.0 o posterior (55.0 o superior para Consola remota)
- Firefox® ESR 38.6.0 o posterior
- Microsoft® Internet Explorer® 11
- Microsoft Edge
- Safari® 9.0.2 o posterior (IOS7 o posterior y OS X)

Firewall y servidores proxy

Algunas funciones de Lenovo XClarity Administrator, incluidas las actualizaciones de servidor de gestión y firmware, además de servicio y soporte, requieren acceso a Internet. Si tiene firewalls en su red, configúrelos para habilitar el servidor de gestión XClarity Administrator a fin de que ejecute estas operaciones. Si el servidor de gestión no tiene acceso a Internet, configure XClarity Administrator para utilizar un servidor proxy.

Firewalls

Asegúrese de que los siguientes nombres y puertos DNS estén abiertos en el firewall. Cada DNS representa un sistema distribuido geográficamente con una dirección IP dinámica.

Nombre DNS	Puertos	Protocolos
Descargue las claves de activación de la licencia		
fod.lenovo.com	443	https
Recuperar boletines de servicio		
download.lenovo.com/servers/LXCA_Bulletin_Service.json	443	https
Descargue actualizaciones (actualizaciones del servidor de gestión, actualizaciones de firmware, UpdateXpress System Packs (controladores de dispositivos del SO) y paquetes de repositorio)		
download.lenovo.com	443	https
support.lenovo.com	443	https y http
Envíe datos del servicio al Soporte de Lenovo (Llamar a casa)		
soaus.lenovo.com	443	https
logupload.lenovo.com/BLL/Logupload.ashx	443 y 80	https
Envíe los datos del servicio a la herramienta de actualización de Lenovo		
esupportwebapi.lenovo.com	443 y 80	https
Recupere la información de garantía		
csapi.lenovo.com.cn (solo para China)	443	https
supportapi.lenovo.com (todo el mundo)	443 y 80	https y http

Servidor proxy

Si el servidor de gestión no dispone de conexión directa a Internet, asegúrese de que el servidor proxy esté configurado para utilizar un servidor proxy HTTP (consulte “Configuración del acceso de red” en la página 91).

- 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.

Disponibilidad de puertos

Debe haber varios puertos disponibles, dependiendo de cómo estén implementados los firewalls en su entorno. Si los puertos necesarios están bloqueados o se utilizan en otro proceso, puede que algunas funciones de Lenovo XClarity Administrator no estén operativas.

Consulte las secciones siguientes para determinar los puertos que deben estar abiertos en función de su entorno. Las tablas de estas secciones incluyen información acerca de cómo se utiliza cada puerto en XClarity Administrator, el dispositivo gestionado afectado, el protocolo (TCP o UDP) y la dirección del flujo de tráfico. *El tráfico entrante* identifica los flujos desde el dispositivo gestionado o los sistemas externos a XClarity Administrator, por lo que los puertos deben estar abiertos en el dispositivo XClarity Administrator. El flujo de tráfico *saliente* desde XClarity Administrator al dispositivo gestionado.

- Acceso al servidor de XClarity Administrator
- Acceso entre XClarity Administrator y dispositivos gestionados
- Acceso entre XClarity Administrator y la red de datos con soporte para despliegue del SO y actualizaciones de controladores de dispositivos

Acceso al servidor de XClarity Administrator

Si el servidor de XClarity Administrator y todos los dispositivos gestionados se rigen por un firewall y tiene pensado acceder a estos dispositivos a través de un navegador que está fuera del firewall, debe asegurarse de que los puertos de XClarity Administrator estén abiertos. Si está utilizando SNMP y SMTP para la gestión de sucesos, puede que también necesite asegurarse de que los puertos que se utilizan en el servidor de XClarity Administrator para el reenvío de sucesos estén abiertos.

El servidor de XClarity Administrator escucha los puertos enumerados en la tabla y responde a través de ellos.

Notas:

- XClarity Administrator es una aplicación RESTful que se comunica de forma segura a través de TCP en el puerto 443.
- XClarity Administrator 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 Administrator)**
Dispositivo XClarity Administrator	• DNS: TCP/UDP en el puerto **53**	• HTTPS: TCP en el puerto **443**
Servidor de autenticación externo	• LDAP: TCP en el puerto **389**[1] • LDAPs: TCP en el puerto **636** • Autenticación SAML: TCP en los puertos **3268, 3269**	No aplicable

Servicio	Salida (puertos abiertos en sistemas externos)	Entrada (puertos abiertos en el dispositivo XClarity Administrator)
Servicios de reenvío de sucesos	• Servidor FTP: TCP en el puerto **21**[1] • Servidor de correo electrónico (SMTP): UDP en el puerto **25**[1] • Servicio Web REST (HTTP): TCP en el puerto **80**[1] • Gestor SNMP: UDP en el puerto **161**[2], **162**[1] • MS Azure: UDP en el puerto **443**[1] • Syslog: UDP en el puerto **514**[1] • Apple push[3]: TCP en los puertos **443, 2195, 5223** • Google push [4]: TCP en los puertos **443, 5288, 5299, 5230**	• SNMP: TCP/UDP en el puerto **161**
Servicios de Lenovo (incluyendo Llamar a casa)	• Garantía (solo China): TCP en el puerto **83**[5] • HTTPS (Llamar a casa): TCP en el puerto **443**	No aplicable

1. Este es el puerto predeterminado. Puede configurar este puerto desde la interfaz de usuario.
2. Este puerto se utiliza cuando está configurado el reenvío de sucesos SNMP con autenticación del usuario.
3. Abra este puerto cuando wifi se encuentre detrás de un firewall o un nombre de punto de acceso privado (APN) para datos móviles. Se requiere una conexión directa sin proxy a los servidores de APN en este puerto. Este puerto se usa en caso de errores únicamente en wifi, cuando los dispositivos no pueden acceder al servicio de notificaciones automáticas de Apple en el puerto 5223. El rango de direcciones IP es 17.0.0.0/8.
4. Para el rango de direcciones IP, consulte Google ASN 15169. El dominio es android.googleapis.com.
5. Aunque no se requiere fuera de China, XClarity Administrator puede intentar conectarse a este servicio en otros países.

Acceso entre XClarity Administrator y dispositivos gestionados

Si los dispositivos gestionados (como los nodos de cálculo o los servidores de bastidor), se rigen por un firewall y tiene pensado gestionar estos dispositivos desde un servidor de XClarity Administrator que está fuera de ese firewall, debe asegurarse de que todos los puertos implicados en las comunicaciones entre XClarity Administrator y el controlador de gestión de la placa base de cada dispositivo gestionado estén abiertos.

Si tiene intención instalar sistemas operativos en dispositivos gestionados utilizando XClarity Administrator, asegúrese de revisar la lista de puertos en Acceso entre XClarity Administrator y la red de datos con soporte para despliegue del SO y actualizaciones de controladores de dispositivos.

- **CMM de chasis Flex**

Tipo de dispositivo	Salida (puertos abiertos en sistemas externos)	Entrada (puertos abiertos en el dispositivo XClarity Administrator)
CMM de chasis de Flex	– SLP: UDP/TCP en el puerto **427** – CIM: HTTP/TCP en el puerto **5988**[2] – CIM: HTTP/TCP en el puerto **5989** – Comando TCP: TCP en el puerto **6090**[2] – Comando TCP seguro: TCP en el puerto **6091**	– SFTP: TCP en el puerto **22**[1] – Indicaciones de CIM HTTPS: TCP **9090** – LDAPs: TCP en los puertos **50637**

1. Este puerto se utiliza para transferir actualizaciones de firmware mediante SFTP.
2. De forma predeterminada, la gestión se realiza a través de puertos seguros. Los puertos no seguros son opcionales.

- **Servidores y nodos de cálculo**

Tipo de dispositivo	Salida (puertos abiertos en sistemas externos)	Entrada (puertos abiertos en el dispositivo XClarity Administrator)
Servidores ThinkSystem y ThinkAgile	– Detección de SSDP: UDP en el puerto **1900** – SFTP: TCP en el puerto **115**[4] – HTTPS: TCP en el puerto **443** – Control remoto: TCP en el puerto **3888**[3] – CIM: HTTP/TCP en el puerto **5989**[8] – Actualizaciones de firmware: TCP en el puerto **6990**[4, 7] – SLP: UDP/TCP en el puerto **427**[6]	– SFTP: TCP en el puerto **22**[1] – HTTPS: TCP en el puerto **443** – Actualizaciones de firmware: TCP en el puerto **6990**[4, 7] – Indicaciones de CIM HTTPS: TCP **9090** – LDAPs: TCP en los puertos **50636**[5] – LDAPs: TCP en los puertos **50637**[9]
System x	– SLP: UDP/TCP en el puerto **427** – HTTPS: TCP en el puerto **443** – IPMI: TCP en el puerto **623** – Control remoto: TCP en el puerto **3888**[3] – CIM: HTTP/TCP en el puerto **5988**[2] – CIM: HTTP/TCP en el puerto **5989**[2,8] – Actualizaciones de firmware: TCP en el puerto **6990**[4, 7]	– SFTP: TCP en el puerto **22**[1] – HTTPS: TCP en el puerto **443** – Actualizaciones de firmware: TCP en el puerto **6990**[4, 7] – Indicaciones de CIM HTTPS: TCP **9090**[8] – LDAPs: TCP en los puertos **50636**[5] – LDAPs: TCP en los puertos **50637**[9]

Tipo de dispositivo	Salida (puertos abiertos en sistemas externos)	Entrada (puertos abiertos en el dispositivo XClarity Administrator)
Flex System	– SLP: UDP/TCP en el puerto **427** – Control remoto: TCP en el puerto **3888**[3] – CIM: HTTP/TCP en el puerto **5988**[2] – CIM: HTTP/TCP en el puerto **5989**[2,8] – Actualizaciones de firmware: TCP en el puerto **6990**[4, 7]	– SFTP: TCP en el puerto **22**[1] – HTTPS: TCP en el puerto **443** – Actualizaciones de firmware: TCP en el puerto **6990**[4, 7] – Indicaciones de CIM HTTPS: TCP **9090** – LDAPs: TCP en los puertos **50636**[5] – LDAPs: TCP en los puertos **50637**[9]
ThinkServer	– Interrupciones SNMP: UDP en el puerto **162** – IPMI: UDP en el puerto **623**	– Interrupciones SNMP: UDP en el puerto **162**

1. Este puerto se utiliza para transferir actualizaciones de firmware mediante SFTP, para cargar, descargar y quitar los archivos de datos de servicio, y para almacenar la herramienta de borrado de la unidad que obtiene el SO de la BMU al borrar de forma segura los datos de la unidad.
2. De forma predeterminada, la gestión se realiza a través de puertos seguros. Los puertos no seguros son opcionales.
3. El control remoto y KVM remoto se inician desde el navegador web, no desde el servidor XClarity Administrator.
4. Este puerto es necesario para que las actualizaciones de firmware de la BMU carguen el paquete de actualización de firmware en el controlador de gestión.
5. Este puerto es necesario para configurar los servidores con patrones de configuración.
6. Este puerto solo es necesario para los servidores ThinkSystem SR635 y SR655.
7. Este puerto es necesario para montar la imagen de la BMU cuando se borran los datos de la unidad de forma segura. Este puerto debe estar abierto tanto en el controlador de gestión de la placa base como en el dispositivo XClarity Administrator.
8. Este puerto solo es necesario para los servidores ThinkSystem V1. Este puerto se requiere para los servidores System X, Flex System y ThinkSystem V1.
9. Este puerto es necesario para utilizar la autenticación gestionada.

- **Conmutadores Rack y Flex**

Tipo de dispositivo	Salida (puertos abiertos en sistemas externos)	Entrada (puertos abiertos en el dispositivo XClarity Administrator)
Conmutadores Rack	– SSH: TCP en el puerto **22**[1, 3] – SNMP: UDP en el puerto **161**[2] – SLP: UDP/TCP en el puerto **427**[6] – HTTPS: TCP en el puerto **443**[7]	– SFTP: TCP en el puerto **22**[4] – Interrupciones SNMP: TCP en los puertos **162**[2]
Conmutadores Flex	– SSH: TCP en el puerto **22**[3] – SNMP: UDP en el puerto **161**[5]	– SFTP: TCP en el puerto **22**[4] – Interrupciones SNMP: TCP en el puerto **162**[2]

1. Para conmutadores Rack ENOS, este puerto se utiliza para configurar las credenciales de Head of Stack (HoS) utilizadas entre los switches CMM y Flex, activar la ranura de firmware y borrar las claves del host de SSH antes de las operaciones de transferencia de archivos SFTP.
2. Este puerto debe estar abierto en el dispositivo XClarity Administrator (entrada) cuando los conmutadores están en una red distinta de XClarity Administrator, para que XClarity Administrator pueda recibir sucesos para esos dispositivos.
3. Este puerto se utiliza para la gestión (SSH).
4. Este puerto se utiliza para transferir actualizaciones de firmware mediante SFTP.
5. Para los conmutadores de bastidor ENOS, este puerto se utiliza para transferir datos de inventario.
6. Este puerto se utiliza para la detección.
7. Este puerto se utiliza para aplicar actualizaciones de firmware.

- **Dispositivos de almacenamiento**

Tipo de dispositivo	Salida (puertos abiertos en sistemas externos)	Entrada (puertos abiertos en el dispositivo XClarity Administrator)
Dispositivos de almacenamiento	– FTP: TCP en el puerto **21** – SFTP: TCP en el puerto **22**[2] – SLP: UDP/TCP en el puerto **427** – HTTPS: TCP en el puerto **443**[1] – HTTPS: TCP en el puerto **3031**[3]	– HTTPS: TCP en el puerto **443**[2] – Interrupciones SNMP: UDP en el puerto **115**

1. Este puerto se utiliza para transferir actualizaciones de firmware.
2. Este puerto se utiliza para transferir y aplicar actualizaciones de firmware.
3. Este puerto se utiliza para la detección de dispositivos de almacenamiento de Biblioteca de cintas.

Acceso entre XClarity Administrator y la red de datos con soporte para despliegue del SO y actualizaciones de controladores de dispositivos

Tipo de dispositivo	Salida (puertos abiertos en sistemas externos)	Entrada (puertos abiertos en el dispositivo XClarity Administrator)
Implementación de SO[1, 2, 3]		• Comunicación de SMB: TCP en el puerto **445**[4] • HTTPS (excepto ThinkServer): TCP en el puerto **8443**[6]
Actualizaciones de controladores de dispositivos de SO[2]	• WinRM sobre HTTP: TCP en el puerto **5985**[5] • WinRM sobre HTTPS: TCP en el puerto **5986**[6]	• Comunicación de SMB: TCP en el puerto **445**[4]

1. Si está configurando XClarity Administrator para utilizar una red de despliegue del sistema operativo, los puertos deben estar abiertos en esa red.
2. Consulte Disponibilidad de puertos para sistemas operativos desplegados en la documentación en línea de XClarity Administrator para ver una lista de los puertos que deben estar disponibles para desplegar sistemas operativos. Por ejemplo, si el despliegue del sistema operativo está configurado para usar la red de datos (eth1), estos puertos deben estar abiertos en esa red.
3. Cada instancia de XClarity Administrator tiene Entidad de certificación (CA) única que se utiliza solo para el despliegue del SO. Ese CA firma un certificado que se utiliza para el servidor de destino en el puerto 8443. Cuando se inicia el despliegue del SO, el certificado de CA se incluye en la imagen del SO que se

inserta en el servidor de destino. Como parte del proceso de despliegue, dicho servidor vuelve a conectarse al puerto 8443 y verifica el certificado que proporciona el puerto 8443 durante el protocolo de enlace porque tienen el certificado de CA.

4. Este puerto se utiliza para transferir archivos de controlador de Windows.
5. Este puerto se utiliza para conectarse al servidor de destino WinRM.
6. Este puerto se utiliza para intercambiar datos entre el SO de destino y XClarity Administrator, incluidas las imágenes del SO y el estado.

Consideraciones de gestión

Hay varias alternativas para elegir a la hora de gestionar dispositivos. Dependiendo de los dispositivos que se estén gestionando, puede que necesite ejecutar a la vez varias soluciones de gestión.

Un dispositivo solo se puede gestionar mediante una única instancia de Lenovo XClarity Administrator. Sin embargo, puede utilizar otro software de gestión (como VMware vRealize Operations Manager) junto con Lenovo XClarity Administrator para *supervisar* dispositivos gestionados por XClarity Administrator.

Atención: Se debe tener más cuidado cuando se utilicen varias herramientas de gestión para gestionar los dispositivos, con el fin de evitar conflictos imprevistos. Por ejemplo, enviar cambios en el estado de la alimentación con otra herramienta podría entrar en conflicto con los trabajos de configuración o actualización en ejecución en XClarity Administrator.

Dispositivos ThinkSystem, ThinkServer y System x

Si tiene intención de utilizar otro software de gestión para supervisar los dispositivos gestionados, cree un nuevo usuario local con los valores de SNMP o IPMI correctos desde la interfaz del IMM. Asegúrese de otorgar privilegios de SNMP o IPMI, según sus necesidades.

Dispositivos Flex System

Si tiene pensado utilizar un software de gestión distinto para supervisar los dispositivos gestionados y si ese software de gestión utiliza la comunicación SNMPv3 o IPMI, deberá preparar su entorno siguiendo los pasos que se indican a continuación para cada CMM gestionado:

1. Inicie sesión en la interfaz web del controlador de gestión del chasis utilizando el nombre de usuario y la contraseña `RECOVERY_ID`.
2. Si la política de seguridad está configurada como **Segura**, cambie el método de autenticación del usuario.
   a. Haga clic en **Gestión del módulo de gestión → Cuentas de usuarios**.
   b. Haga clic en la pestaña **Cuentas**.
   c. Haga clic en **Valores de inicio de sesión globales**.
   d. Haga clic en la pestaña **General**.
   e. Seleccione **Externo primero, luego autenticación local** para el método de autenticación del usuario.
   f. Haga clic en **Aceptar**.
3. Cree un nuevo usuario local con los valores de SNMP o IPMI correctos de la interfaz web del controlador de gestión.
4. Si la política de seguridad está configurada como **Segura** cierre la sesión y luego inicie la sesión en la interfaz web del controlador de gestión mediante los nuevos nombre de usuario y contraseña. Cuando se le solicite, cambie la contraseña para el usuario nuevo.

Ahora puede utilizar el nuevo usuario como usuario activo de SNMP o IPMI.

Nota: Si cancela la gestión y luego gestiona el chasis de nuevo, esta nueva cuenta de usuario se bloquea y se deshabilitada. En este caso, repita estos pasos para crear una nueva cuenta de usuario.

Consideraciones de red

A la hora de planificar la instalación de Lenovo XClarity Administrator, tenga en cuenta la topología de red que está implementada en su entorno, así como la forma en la que XClarity Administrator encaja en dicha topología.

Importante: configure los componentes de los dispositivos de forma que minimicen los cambios de dirección IP. Plantéese la posibilidad de utilizar direcciones IP estáticas en lugar del protocolo de configuración dinámica de host (DHCP). Si se utiliza DHCP, asegúrese de que los cambios de dirección IP se minimizan.

Limitaciones de configuración de IP

Para las funciones y los dispositivos gestionados siguientes, las interfaces de red se deben configurar con una dirección IPv4. No se admiten las direcciones IPv6.
- Actualizaciones de firmware para dispositivos Lenovo Storage
- Servidores ThinkServer
- Dispositivos Lenovo Storage

No se admite la gestión de dispositivos de RackSwitch mediante IPv6 enlace local a través de un puerto de datos o de gestión.

La traducción de dirección de red (NAT), que reasigna el espacio de una dirección IP en otro, no se admite.

Tipos de red

En general, en la mayoría de entornos se implementan los siguientes tipos de red. Según sus requisitos, puede implementar solamente una de estas redes o implementar las tres.

- **Red de gestión**

  La red de gestión suele estar reservada para las comunicaciones entre Lenovo XClarity Administrator y los procesadores de gestión de los dispositivos gestionados. Por ejemplo, la red de gestión puede estar configurada para incluir XClarity Administrator, los CMM para cada chasis gestionado y el controlador de gestión de la placa base de cada servidor que se esté gestionando mediante XClarity Administrator.
- **Red de datos**

  La red de datos se suele utilizar para las comunicaciones entre los sistemas operativos que están instalados en los servidores y la intranet de la empresa, Internet o ambos.
- **Red de despliegue del sistema operativo**

  En algunos casos, se configura una red de despliegue del sistema operativo para separar las comunicaciones que son necesarias para desplegar sistemas operativos en servidores. Si está implementada, esta red normalmente incluye XClarity Administrator y todos los hosts de servidor.

  En lugar de implementar una red de despliegue del sistema operativo por separado, puede optar por combinar esta funcionalidad con la red de gestión o la red de datos.

Configuraciones de red

Puede configurar Lenovo XClarity Administrator para utilizar una o dos interfaces de red.

Atención:

- Si cambia la dirección IP de XClarity Administrator después de gestionar dispositivos, es posible que los dispositivos queden en estado fuera de línea en XClarity Administrator. Asegúrese de anular la gestión de todos los dispositivos antes de cambiar la dirección IP.

- Puede habilitar o deshabilitar la comprobación de direcciones IP duplicadas en la misma subred haciendo clic en el icono de alternación **Comprobación de dirección IP duplicada**. Está deshabilitado de forma predeterminada. Cuando está habilitado, XClarity Administrator genera una alerta si se intenta cambiar la dirección IP de XClarity Administrator o gestionar un dispositivo que tiene la misma dirección IP que otro dispositivo ya gestionado u otro dispositivo que se encuentra en la misma subred.

  Nota: Cuando está habilitado, XClarity Administrator ejecuta una detección de ARP para buscar dispositivos IPv4 activos en la misma subred. Para evitar la detección de ARP, deshabilite la **Verificación de dirección IP duplicada**.
- Cuando ejecute XClarity Administrator como un dispositivo virtual, si la interfaz de red de la red de gestión 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 anular la gestión del chasis y de los servidores de bastidor y torre y, a continuación, volver a gestionarlos. Para evitar este problema puede cambiar la interfaz de gestión 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.
- Si *no* tiene pensado utilizar XClarity Administrator para desplegar el sistema operativo o actualizar los controladores de dispositivo del SO puede deshabilitar servidores Samba y Apache cambiando la interfaz de red para utilizar la opción **Detectar y gestionar hardware únicamente**. Tenga en cuenta que el servidor de gestión se reinicia después de cambiar la interfaz de red.
- Al ejecutar XClarity Administrator como contenedor, asegúrese de que la red macvlan esté configurada en el sistema host.

XClarity Administrator tiene dos interfaces de red separadas que se pueden definir para su entorno, dependiendo de la topología de red que implemente. Para los dispositivos virtuales, estas redes se denominan eth0 y eth1. Para los nombres originales, puede elegir los nombres personalizados.

- Cuando solo hay una interfaz de red (eth0):
  - La interfaz debe estar configurada para admitir la detección de dispositivos y de gestión (como la configuración del servidor y las actualizaciones de firmware). Debe poder comunicarse con los CMM y los conmutadores Flex en cada chasis gestionado, el controlador de gestión de la placa base en cada servidor gestionado y cada conmutador RackSwitch.
  - Si tiene pensado adquirir actualizaciones de firmware y de controlador de dispositivo de SO usando XClarity Administrator, al menos una de las interfaces de red también debe estar conectada con Internet, preferentemente a través de un firewall. Si no es así, tiene que importar las actualizaciones al repositorio.
  - Si desea recopilar datos del servicio o bien notificación automática de problemas (incluido Llamar a casa y la herramienta de carga de Lenovo), al menos una de las interfaces de red debe estar conectada a Internet, preferentemente a través de un firewall.
  - Si desea desplegar imágenes del sistema operativo y actualizar controladores de dispositivos de SO, la interfaz debe tener conectividad de red IP a la interfaz de red del servidor que se utiliza para acceder al sistema operativo del host.

    Nota: Si implementó una red aparte para desplegar SO y actualizar controladores de dispositivos de SO, puede configurar la segunda interfaz de red para conectarse a esa red en lugar de hacerlo a la red de datos. Sin embargo, si el sistema operativo de cada servidor no tiene acceso a la red de datos, deberá configurar una interfaz adicional en los servidores para proporcionar conectividad desde el sistema operativo host a la red de datos para el despliegue del SO y las actualizaciones de controlador de dispositivo de SO, de ser necesario.
- Cuando hay dos interfaces de red (eth0 y eth1):
  - La primera interfaz de red (normalmente, la interfaz Eth0) debe estar conectada a la red de gestión y configurada para que admita la detección de dispositivos y gestión (incluidas las actualizaciones de

firmware y configuración del servidor. Debe poder comunicarse con los CMM y los conmutadores Flex en cada chasis gestionado, el controlador de gestión en cada servidor gestionado y cada conmutador RackSwitch.

- La segunda interfaz de red (normalmente la interfaz eth1) se puede configurar para comunicarse con una red de datos interna, con una red de datos pública o ambas.
- Si tiene pensado adquirir actualizaciones de firmware y de controlador de dispositivo de SO usando XClarity Administrator, al menos una de las interfaces de red también debe estar conectada con Internet, preferentemente a través de un firewall. Si no es así, tiene que importar las actualizaciones al repositorio.
- Si desea recopilar datos del servicio o bien notificación automática de problemas (incluido Llamar a casa y la herramienta de carga de Lenovo), al menos una de las interfaces de red debe estar conectada a Internet, preferentemente a través de un firewall.
- Si tiene pensado desplegar imágenes del sistema operativo y actualizar los controladores de dispositivo del SO, puede elegir utilizar la interfaz eth1 o eth0. Sin embargo, la interfaz que use debe tener la conectividad de red IP hacia la interfaz de red del servidor que se usa para acceder al sistema operativo host.

  Nota: Si implementó una red aparte para desplegar SO y actualizar controladores de dispositivos de SO, puede configurar la segunda interfaz de red para conectarse a esa red en lugar de hacerlo a la red de datos. Sin embargo, si el sistema operativo de cada servidor no tiene acceso a la red de datos, deberá configurar una interfaz adicional en los servidores para proporcionar conectividad desde el sistema operativo host a la red de datos para el despliegue del SO y las actualizaciones de controlador de dispositivo de SO, de ser necesario.

En la tabla siguiente se muestran las configuraciones que se pueden realizar para las interfaces de red de XClarity Administrator según el tipo de topología de red que se haya implementado en su entorno. Utilice esta tabla para determinar cómo definir cada interfaz de red.

Tabla 1. Rol de cada interfaz de red según la topología de red

Topología de red	**Rol de la interfaz 1 (eth0)**	**Rol de la interfaz 2 (eth1)**
Red convergente (red de gestión y datos con soporte para el despliegue del SO y actualizaciones del controlador de dispositivo del SO)	Red de gestión • Detección y gestión • Configuración del servidor • Actualizaciones de firmware • Recopilación de datos de servicio • Notificación automática de problemas (como Llamar a casa y la herramienta de actualización de Lenovo) • Recuperación de datos de garantía • Implementación de SO • Actualizaciones de controladores de dispositivos de SO	Ninguno
Red de gestión separada con soporte para el despliegue del SO y actualizaciones del controlador de dispositivo del SO y red de datos	Red de gestión • Detección y gestión • Configuración del servidor • Actualizaciones de firmware • Recopilación de datos de servicio • Notificación automática de problemas (como Llamar a casa y la herramienta de actualización de Lenovo) • Recuperación de datos de garantía • Implementación de SO • Actualizaciones de controladores de dispositivos de SO	Red de datos • Ninguno
Red de gestión separada y red de datos con soporte para el despliegue del SO y actualizaciones del controlador de dispositivo del SO	Red de gestión • Detección y gestión • Configuración del servidor • Actualizaciones de firmware • Recopilación de datos de servicio • Notificación automática de problemas (como Llamar a casa y la herramienta de actualización de Lenovo) • Recuperación de datos de garantía	Red de datos • Implementación de SO • Actualizaciones de controladores de dispositivos de SO

Tabla 1. Rol de cada interfaz de red según la topología de red (continuación)

Topología de red	Rol de la interfaz 1 (eth0)	Rol de la interfaz 2 (eth1)
Red de gestión separada y red de datos sin soporte para el despliegue del SO y actualizaciones del controlador de dispositivo del SO	Red de gestión • Detección y gestión • Configuración del servidor • Actualizaciones de firmware • Recopilación de datos de servicio • Notificación automática de problemas (como Llamar a casa y la herramienta de actualización de Lenovo) • Recuperación de datos de garantía	Red de datos • Ninguno
Solo red de gestión (no se admiten el despliegue del SO y las actualizaciones de controladores de dispositivos del SO)	Red de gestión • Detección y gestión • Configuración del servidor • Actualizaciones de firmware • Recopilación de datos de servicio • Notificación automática de problemas (como Llamar a casa y la herramienta de actualización de Lenovo) • Recuperación de datos de garantía	Ninguno

Una sola red de datos y de gestión

En esta topología de red, las comunicaciones de gestión, las comunicaciones de datos y el despliegue de sistemas operativos se producen en la misma red. Esta topología recibe el nombre de red *convergida*.

Importante: Implementar una red de datos compartidos y de gestión puede provocar interrupciones en el tráfico, como paquetes que se caen o problemas de conectividad de red de gestión, según su configuración de red (por ejemplo, si el tráfico de los servidores tiene una prioridad alta y el tráfico de los controladores de gestión tiene una prioridad baja). La red de gestión utiliza el tráfico UDP, además de TCP. El tráfico UDP puede tener una prioridad más baja cuando el tráfico de red es alto.

Al instalar Lenovo XClarity Administrator, debe definir la interfaz de red eth0 usando las siguientes consideraciones:

- La interfaz debe estar configurada para admitir la detección de dispositivos y de gestión (como la configuración del servidor y las actualizaciones de firmware). Debe poder comunicarse con los CMM y los conmutadores Flex en cada chasis gestionado, el controlador de gestión de la placa base en cada servidor gestionado y cada conmutador RackSwitch.
- Si tiene pensado adquirir actualizaciones de firmware y de controlador de dispositivo de SO usando XClarity Administrator, al menos una de las interfaces de red también debe estar conectada con Internet, preferentemente a través de un firewall. Si no es así, tiene que importar las actualizaciones al repositorio.
- Si desea recopilar datos del servicio o bien notificación automática de problemas (incluido Llamar a casa y la herramienta de carga de Lenovo), al menos una de las interfaces de red debe estar conectada a Internet, preferentemente a través de un firewall.
- Si desea desplegar imágenes del sistema operativo y actualizar controladores de dispositivos de SO, la interfaz debe tener conectividad de red IP a la interfaz de red del servidor que se utiliza para acceder al sistema operativo del host.

  Nota: Si implementó una red aparte para desplegar SO y actualizar controladores de dispositivos de SO, puede configurar la segunda interfaz de red para conectarse a esa red en lugar de hacerlo a la red de datos. Sin embargo, si el sistema operativo de cada servidor no tiene acceso a la red de datos, deberá

configurar una interfaz adicional en los servidores para proporcionar conectividad desde el sistema operativo host a la red de datos para el despliegue del SO y las actualizaciones de controlador de dispositivo de SO, de ser necesario.

- Puede configurar XClarity Administrator en cualquier sistema que cumpla con los requisitos de XClarity Administrator, incluido un servidor gestionado solamente cuando implemente una topología de una sola red de datos y de gestión o una topología de redes de datos y de gestión separadas virtualmente; no obstante, no puede utilizar XClarity Administrator para aplicar actualizaciones de firmware a ese servidor gestionado. Incluso en ese caso, solo se aplica determinado firmware con la activación inmediata y XClarity Administrator fuerza el reinicio del servidor de destino, lo que reinicia también XClarity Administrator. Cuando se aplica con la activación aplazada, solo se aplica determinado firmware cuando se reinicia el host de XClarity Administrator.

También puede configurar una segunda interfaz de red para que se conecte a la misma red que XClarity Administrator a fin de que se admita la redundancia.

En la figura siguiente se muestra un ejemplo de implementación de una topología de red convergida.

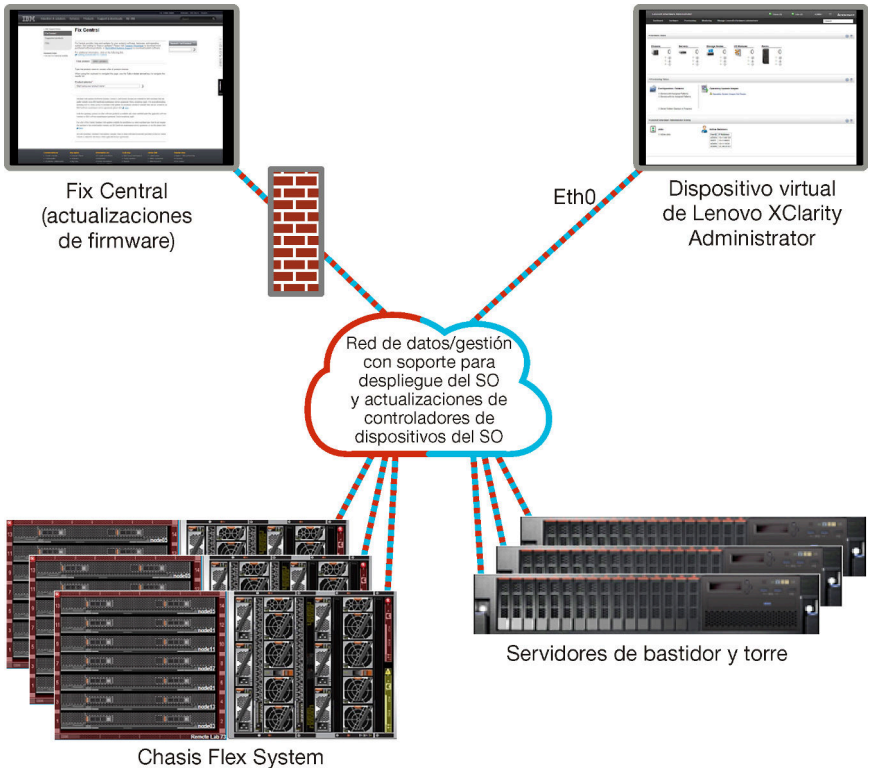


Figura 1. Ejemplo de implementación de una sola red de gestión, datos y despliegue del sistema operativo

Redes de datos y de gestión separadas físicamente

En esta topología de red, la red de gestión y la red de datos son redes separadas físicamente, mientras que la red de despliegue del sistema operativo está configurada como parte de la red de gestión o de la red de datos.

Al instalar Lenovo XClarity Administrator, debe definir los valores de red teniendo en cuenta estas consideraciones:

- La primera interfaz de red (normalmente, la interfaz Eth0) debe estar conectada a la red de gestión y configurada para que admita la detección de dispositivos y gestión (incluidas las actualizaciones de firmware y configuración del servidor. Debe poder comunicarse con los CMM y los conmutadores Flex en

cada chasis gestionado, el controlador de gestión en cada servidor gestionado y cada conmutador RackSwitch.

- La segunda interfaz de red (normalmente la interfaz eth1) se puede configurar para comunicarse con una red de datos interna, con una red de datos pública o ambas.
- Si tiene pensado adquirir actualizaciones de firmware y de controlador de dispositivo de SO usando XClarity Administrator, al menos una de las interfaces de red también debe estar conectada con Internet, preferentemente a través de un firewall. Si no es así, tiene que importar las actualizaciones al repositorio.
- Si desea recopilar datos del servicio o bien notificación automática de problemas (incluido Llamar a casa y la herramienta de carga de Lenovo), al menos una de las interfaces de red debe estar conectada a Internet, preferentemente a través de un firewall.
- Si tiene pensado desplegar imágenes del sistema operativo y actualizar los controladores de dispositivo del SO, puede elegir utilizar la interfaz eth1 o eth0. Sin embargo, la interfaz que use debe tener la conectividad de red IP hacia la interfaz de red del servidor que se usa para acceder al sistema operativo host.

  Nota: Si implementó una red aparte para desplegar SO y actualizar controladores de dispositivos de SO, puede configurar la segunda interfaz de red para conectarse a esa red en lugar de hacerlo a la red de datos. Sin embargo, si el sistema operativo de cada servidor no tiene acceso a la red de datos, deberá configurar una interfaz adicional en los servidores para proporcionar conectividad desde el sistema operativo host a la red de datos para el despliegue del SO y las actualizaciones de controlador de dispositivo de SO, de ser necesario.

En la Figura 2 “Ejemplo de implementación de redes de datos y de gestión separadas físicamente con la red del sistema operativo como parte de la red de datos” en la página 25 se muestra un ejemplo de implementación de redes de gestión y de datos separadas en las que la red de despliegue del sistema operativo está configurada como parte de la red de datos.

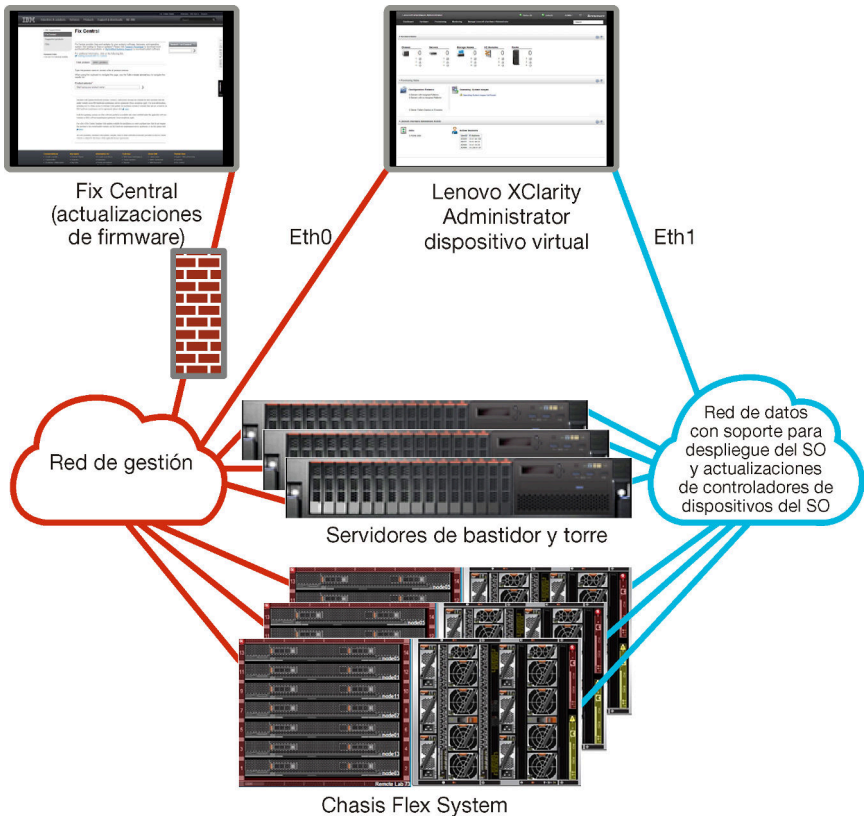


Figura 2. Ejemplo de implementación de redes de datos y de gestión separadas físicamente con la red del sistema operativo como parte de la red de datos

En la Figura 3 “Ejemplo de implementación de redes de datos y de gestión separadas físicamente con la red del sistema operativo como parte de la red de gestión” en la página 26 se muestra otro ejemplo de implementación de redes de gestión y de datos separadas en las que la red de despliegue del sistema operativo está configurada como parte de la red de gestión. En esta implementación, XClarity Administrator no necesita conectividad a la red de datos.

Nota: Si la red de despliegue del sistema operativo no tiene acceso a la red de datos, deberá configurar una interfaz adicional en los servidores para proporcionar conectividad desde el sistema operativo host del servidor a la red de datos, en caso necesario.

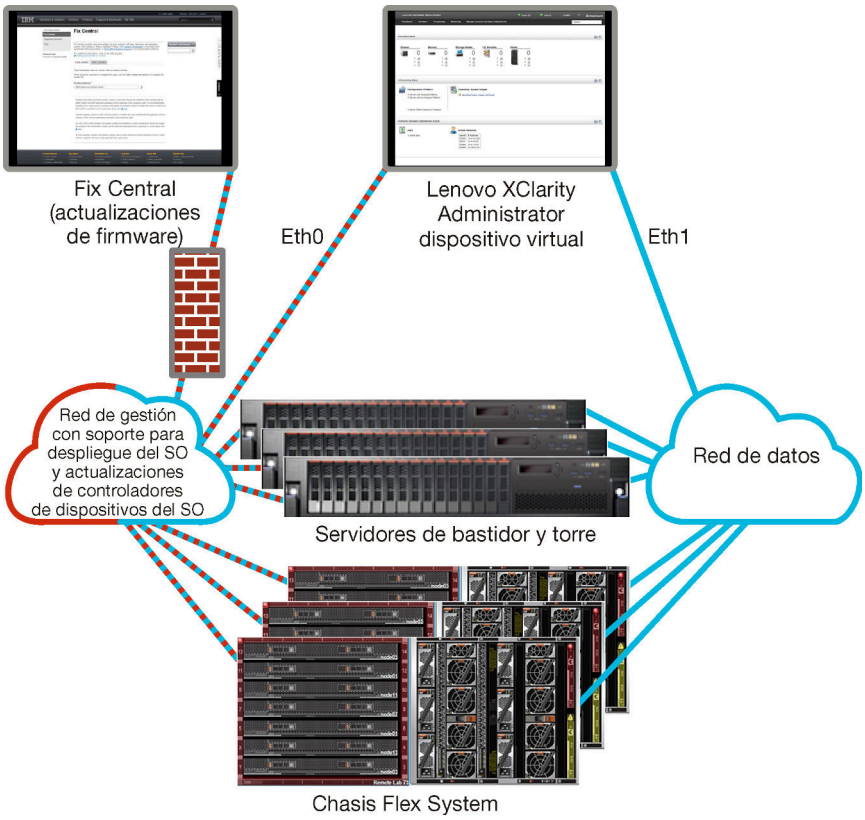


Figura 3. Ejemplo de implementación de redes de datos y de gestión separadas físicamente con la red del sistema operativo como parte de la red de gestión

Redes de datos y de gestión separadas virtualmente

En esta topología, la red de datos y la red de gestión están separadas virtualmente. Los paquetes de la red de datos y de la red de gestión se envían mediante la misma conexión física. El etiquetado de VLAN se utiliza en todos los paquetes de datos de la red de gestión para mantener el tráfico entre las dos redes separadas.

Nota: Si Lenovo XClarity Administrator está instalado en un host que se encuentra en ejecución en un servidor de cálculo gestionado de un chasis, no puede utilizar XClarity Administrator para aplicar actualizaciones de firmware a todo el chasis al mismo tiempo. Cuando se apliquen actualizaciones de firmware, el sistema host deberá reiniciarse.

Al instalar XClarity Administrator, debe definir los valores de red teniendo en cuenta estas consideraciones:

- La primera interfaz de red (normalmente, la interfaz Eth0) debe estar conectada a la red de gestión y configurada para que admita la detección de dispositivos y gestión (incluidas las actualizaciones de firmware y configuración del servidor. Debe poder comunicarse con los CMM y los conmutadores Flex en cada chasis gestionado, el controlador de gestión en cada servidor gestionado y cada conmutador RackSwitch.
- La segunda interfaz de red (normalmente la interfaz eth1) se puede configurar para comunicarse con una red de datos interna, con una red de datos pública o ambas.
- Si tiene pensado adquirir actualizaciones de firmware y de controlador de dispositivo de SO usando XClarity Administrator, al menos una de las interfaces de red también debe estar conectada con Internet, preferentemente a través de un firewall. Si no es así, tiene que importar las actualizaciones al repositorio.
- Si desea recopilar datos del servicio o bien notificación automática de problemas (incluido Llamar a casa y la herramienta de carga de Lenovo), al menos una de las interfaces de red debe estar conectada a Internet, preferentemente a través de un firewall.

- Si tiene pensado desplegar imágenes del sistema operativo y actualizar los controladores de dispositivo del SO, puede elegir utilizar la interfaz eth1 o eth0. Sin embargo, la interfaz que use debe tener la conectividad de red IP hacia la interfaz de red del servidor que se usa para acceder al sistema operativo host.

  Nota: Si implementó una red aparte para desplegar SO y actualizar controladores de dispositivos de SO, puede configurar la segunda interfaz de red para conectarse a esa red en lugar de hacerlo a la red de datos. Sin embargo, si el sistema operativo de cada servidor no tiene acceso a la red de datos, deberá configurar una interfaz adicional en los servidores para proporcionar conectividad desde el sistema operativo host a la red de datos para el despliegue del SO y las actualizaciones de controlador de dispositivo de SO, de ser necesario.

- Puede configurar XClarity Administrator en cualquier sistema que cumpla con los requisitos de XClarity Administrator, incluido un servidor gestionado solamente cuando implemente una topología de una sola red de datos y de gestión o una topología de redes de datos y de gestión separadas virtualmente; no obstante, no puede utilizar XClarity Administrator para aplicar actualizaciones de firmware a ese servidor gestionado. Incluso en ese caso, solo se aplica determinado firmware con la activación inmediata y XClarity Administrator fuerza el reinicio del servidor de destino, lo que reinicia también XClarity Administrator. Cuando se aplica con la activación aplazada, solo se aplica determinado firmware cuando se reinicia el host de XClarity Administrator.

En la Figura 4 “Ejemplo de implementación de redes de datos y de gestión separadas virtualmente con la red del sistema operativo como parte de la red de datos” en la página 27 se muestra un ejemplo de implementación de redes de gestión y de datos separadas virtualmente en las que la red de despliegue del sistema operativo está configurada como parte de la red de datos. En este ejemplo, XClarity Administrator está instalado en un servidor gestionado en un chasis.

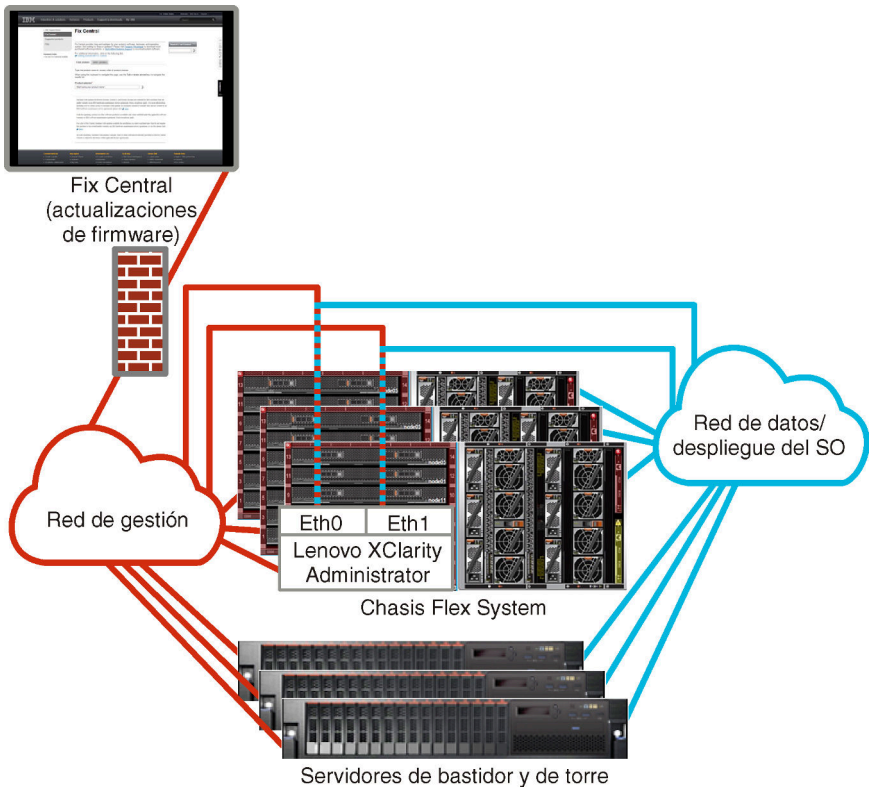


Figura 4. Ejemplo de implementación de redes de datos y de gestión separadas virtualmente con la red del sistema operativo como parte de la red de datos

En la Figura 5 “Ejemplo de implementación de redes de gestión y de datos separadas virtualmente con la red del sistema operativo como parte de la red de gestión” en la página 28 se muestra un ejemplo de implementación de redes de gestión y de datos separadas virtualmente en las que la red de despliegue del sistema operativo está configurada como parte de la red de gestión y XClarity Administrator está instalado en un servidor gestionado en un chasis. En esta implementación, XClarity Administrator no necesita conectividad a la red de datos.

Nota: Si la red de despliegue del sistema operativo no tiene acceso a la red de datos, deberá configurar una interfaz adicional en los servidores para proporcionar conectividad desde el sistema operativo host del servidor a la red de datos, en caso necesario.

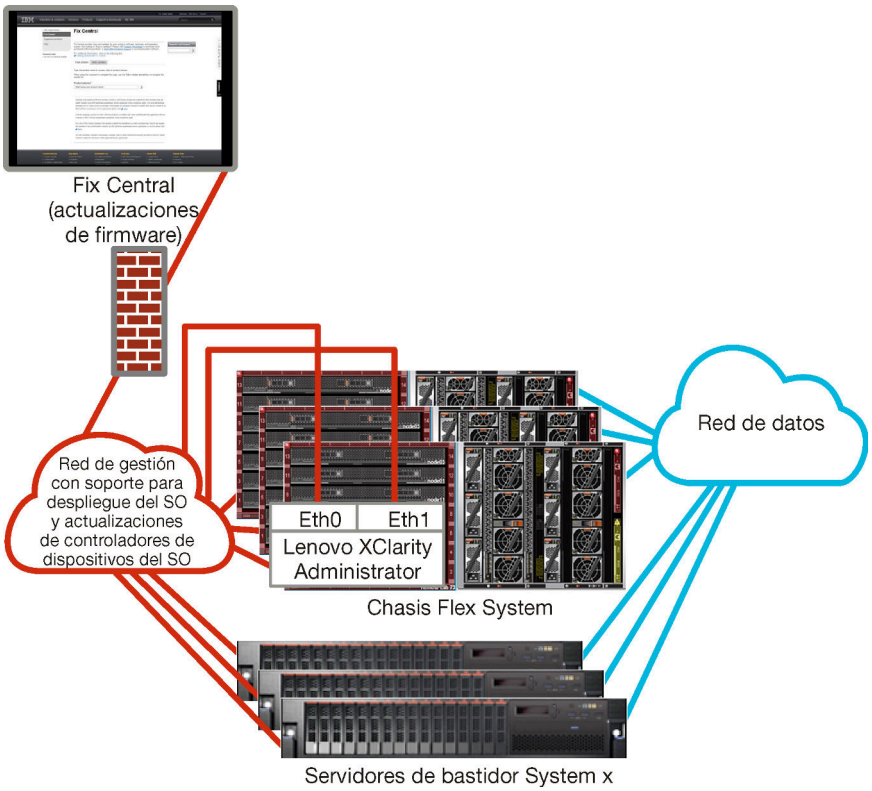


Figura 5. Ejemplo de implementación de redes de gestión y de datos separadas virtualmente con la red del sistema operativo como parte de la red de gestión

Red de solo gestión

En esta topología, Lenovo XClarity Administrator solamente tiene acceso a la red de gestión. No tiene acceso a la red de datos. Sin embargo, es necesario que XClarity Administrator tenga acceso a la red de despliegue del sistema operativo en el caso de que tenga pensado desplegar imágenes de sistemas operativos desde XClarity Administrator en servidores gestionados.

Al instalar XClarity Administrator y definir los valores de red, la interfaz de red Eth0 se debe configurar de modo que:

- La interfaz debe estar configurada para admitir la detección de dispositivos y de gestión (como la configuración del servidor y las actualizaciones de firmware). Debe poder comunicarse con los CMM y los conmutadores Flex en cada chasis gestionado, el controlador de gestión de la placa base en cada servidor gestionado y cada conmutador RackSwitch.
- Si tiene pensado adquirir actualizaciones de firmware y de controlador de dispositivo de SO usando XClarity Administrator, al menos una de las interfaces de red también debe estar conectada con Internet, preferentemente a través de un firewall. Si no es así, tiene que importar las actualizaciones al repositorio.

- Si desea recopilar datos del servicio o bien notificación automática de problemas (incluido Llamar a casa y la herramienta de carga de Lenovo), al menos una de las interfaces de red debe estar conectada a Internet, preferentemente a través de un firewall.
- Si desea desplegar imágenes del sistema operativo y actualizar controladores de dispositivos de SO, la interfaz debe tener conectividad de red IP a la interfaz de red del servidor que se utiliza para acceder al sistema operativo del host.

  Nota: Si implementó una red aparte para desplegar SO y actualizar controladores de dispositivos de SO, puede configurar la segunda interfaz de red para conectarse a esa red en lugar de hacerlo a la red de datos. Sin embargo, si el sistema operativo de cada servidor no tiene acceso a la red de datos, deberá configurar una interfaz adicional en los servidores para proporcionar conectividad desde el sistema operativo host a la red de datos para el despliegue del SO y las actualizaciones de controlador de dispositivo de SO, de ser necesario.

También puede configurar una segunda interfaz de red para que se conecte a la misma red que XClarity Administrator a fin de que se admita la redundancia.

En la Figura 6 “Ejemplo de implementación de una red de solo gestión; no se permite el despliegue del sistema operativo” en la página 29 se muestra un ejemplo de implementación para una red de solo gestión en la que no se admite el despliegue del sistema operativo desde XClarity Administrator.

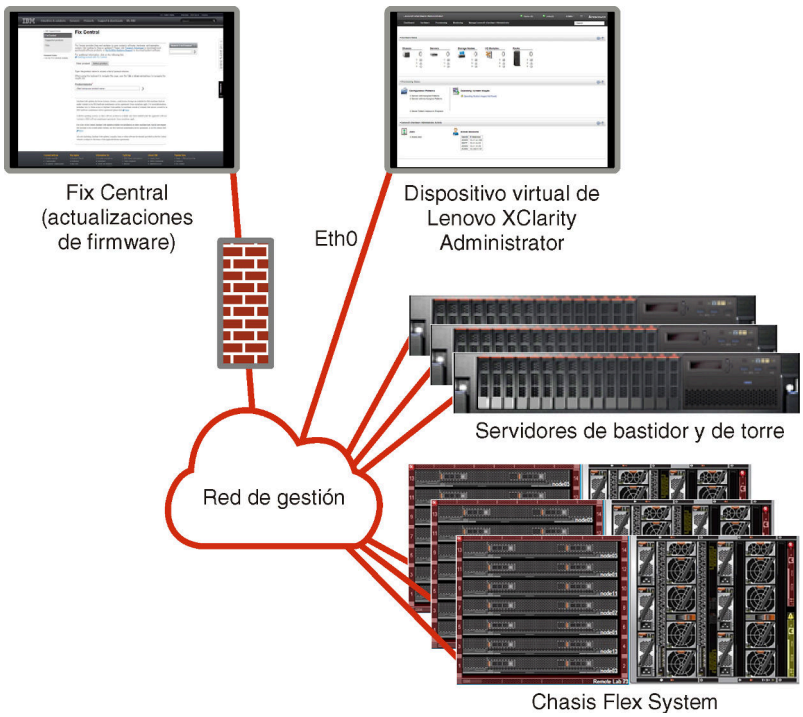


Figura 6. Ejemplo de implementación de una red de solo gestión; no se permite el despliegue del sistema operativo

En la Figura 6 “Ejemplo de implementación de una red de solo gestión; no se permite el despliegue del sistema operativo” en la página 29 se muestra un ejemplo de implementación para una red de solo gestión en la que se admite el despliegue del sistema operativo desde XClarity Administrator.

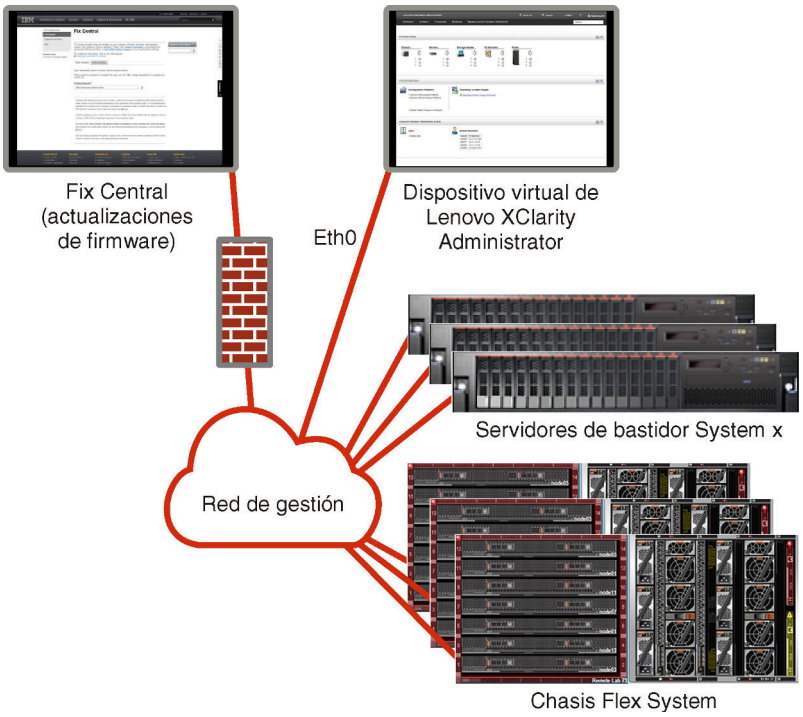


Figura 7. Ejemplo de implementación de una red de solo gestión; se permite el despliegue del sistema operativo

Consideraciones de seguridad

Planifique la seguridad de Lenovo XClarity Administrator y de todos los dispositivos gestionados.

Gestión de encapsulación

Cuando gestiona chasis y servidores Lenovo en Lenovo XClarity Administrator, puede configurar Lenovo XClarity Administrator para cambiar las reglas de firewall de los dispositivos para que solo se acepten las solicitudes entrantes de Lenovo XClarity Administrator. Esto se conoce como *encapsulación*. También puede habilitar o deshabilitar la encapsulación en chasis y servidores que ya se estén gestionando mediante Lenovo XClarity Administrator.

Cuando se habilita la encapsulación en dispositivos que admiten la encapsulación, Lenovo XClarity Administrator cambia el modo de encapsulación del dispositivo a “encapsulationLite” y cambia las reglas de firewall en el dispositivo para limitar las solicitudes entrantes a únicamente las que se reciben de este Lenovo XClarity Administrator.

Cuando está deshabilitado, el modo de encapsulación se establece como “normal”. Si la encapsulación se habilitó previamente en los dispositivos, se quitan las reglas de firewall de encapsulación.

Atención: Si se habilita la encapsulación y XClarity Administrator no está disponible antes de que se elimine la gestión de un dispositivo, se deben realizar algunos pasos para deshabilitar la encapsulación y establecer comunicación con el dispositivo. Para los procedimientos de recuperación, consulte el Recuperación de la gestión de chasis con un CMM después de un error en el servidor de gestión y Recuperación de la gestión de un servidor de bastidor o de torre después de un error de servidor de gestión en la documentación en línea de XClarity Administrator.

Notas:

- La encapsulación no es compatible en conmutadores, dispositivos de almacenamiento y chasis y servidores que no son de Lenovo.

- La gestión de un servidor de bastidor puede tardar bastante tiempo cuando la interfaz de red de gestión está configurada para utilizar el protocolo de configuración dinámica de host (DHCP) y cuando la encapsulación está habilitada.

Para obtener más información sobre la encapsulación, consulte Habilitar encapsulación en la XClarity Administrator documentación en línea.

Gestión criptográfica

La gestión criptográfica se compone de modos y protocolos de comunicación que controlan la forma en la que se manejan comunicaciones seguras entre Lenovo XClarity Administrator y los dispositivos gestionados (tales como chasis, servidores y conmutadores Flex).

Algoritmos criptográficos

XClarity Administrator 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. Los sistemas operativos del cliente y los navegadores web deben ser compatibles con una de las siguientes suites de cifrado.

- SSH-ED25519
- SSH-ED25519-CERT-V01@OPENSSH.COM
- ECDSA-SHA2-NISTP256
- ECDSA-SHA2-NISTP256-CERT-V01@OPENSSH.COM
- ECDSA-SHA2-NISTP384
- ECDSA-SHA2-NISTP384-CERT-V01@OPENSSH.COM
- ECDSA-SHA2-NISTP521
- ECDSA-SHA2-NISTP521-CERT-V01@OPENSSH.COM
- RSA-SHA2-512
- RSA-SHA2-256
- RSA-SHA2-384

Modos criptográficos para el servidor de gestión

Este valor determina el modo que utilizará para las comunicaciones seguras en el servidor de gestión.

- **Compatibilidad**. Este es el modo predeterminado. Es compatible con versiones de firmware más antiguas, navegadores y otros clientes de red que no implementan los estrictos estándares de seguridad que se necesitan para la conformidad con NIST SP 800-131A.
- **NIST SP 800-131A**. Este modo está diseñado para cumplir con el estándar NIST SP 800-131A. XClarity Administrator está diseñado para utilizar siempre una criptografía compleja internamente y, donde proceda, utilizar conexiones de red basadas en criptografías complejas. Sin embargo, con este modo, no se permiten las conexiones de red que utilizan una criptografía que no está aprobada por NIST SP 800-131A, incluido el rechazo de certificados de seguridad de la capa de transporte (TLS) firmados con un hash SHA-1 o más débil.

  Si selecciona este modo:

  – Para todos los puertos que no sean el puerto 8443, se desactivan todos los cifrados TLS CBC y todos los cifrados que no admiten Perfect Forward Secrecy.

  – Las notificaciones de sucesos no se pueden enviar correctamente a algunas suscripciones de dispositivos móviles (consulte Reenviar sucesos a dispositivos móviles en la documentación en línea de XClarity Administrator). Los servicios externos, tales como Android e iOS, presentan certificados que están firmados con SHA-1, que es un algoritmo que no se ajusta a los requisitos más estrictos del modo NIST SP 800-131A. Como resultado, cualquier conexión a estos servicios puede fallar con una excepción del certificado o una falla del protocolo de enlace.

Para obtener más información acerca de la conformidad con NIST SP 800-131A, consulte Implementación de la conformidad con NIST 800-131A en la documentación en línea de XClarity Administrator.

Para obtener más información sobre cómo configurar los modos de seguridad en el servidor de gestión, consulte Configuración del modo criptográfico y los protocolos de comunicación en la documentación en línea de XClarity Administrator.

Modos de seguridad para los servidores gestionados

Este valor determina el modo que se utilizará para las comunicaciones seguras en los servidores gestionados.

- **Seguridad de compatibilidad**. Seleccione este modo cuando los servicios y los clientes requieran una criptografía que no sea compatible con CNSA/FIPS. Este modo admite una amplia gama de algoritmos criptográficos y permite habilitar todos los servicios.
- **NIST SP 800-131A**. Seleccione este modo para garantizar el cumplimiento del estándar NIST SP 800-131A. Esto incluye restringir las claves RSA a 2048 bits o más, restringir los hash utilizados para las firmas digitales a SHA-256 o superior, y garantizar que solo se utilicen algoritmos de cifrado simétricos aprobados por NIST. Este modo requiere configurar el modo SSL/TLS en **Servidor y cliente de TLS 1.2**.

  Este modo es compatible con los servidores ThinkSystem V1 y V2.
- **Seguridad estándar**. Este es el modo de seguridad predeterminado para los servidores ThinkSystem V3 y V4. Seleccione este modo para garantizar el cumplimiento del estándar FIPS 140-3. Para que XCC funcione en el modo validado con FIPS 140-3, solo se pueden habilitar los servicios que admiten la criptografía de nivel FIPS 140-3. Los servicios que no admiten la criptografía de nivel FIPS 140-2/140-3 están deshabilitados de manera predeterminada, pero se pueden habilitar si es necesario. Si se habilita cualquier servicio que utilice criptografía de nivel FIPS 140-3, XCC no puede operar en el modo validado con FIPS 140-3. Este modo requiere certificados de nivel FIP.
- **Seguridad estricta empresarial**. Este es el modo más seguro para los servidores ThinkSystem V3 y V4. Seleccione este modo para garantizar el cumplimiento del estándar CNSA. Solo se permiten los servicios que admiten criptografía de nivel CNSA. Los servicios no seguros están deshabilitados de forma predeterminada y no se pueden habilitar. Este modo requiere certificados de nivel CNSA.

  XClarity Administrator utiliza firmas de certificado RSA 3072-bit/SHA-384 para servidores en el modo de **Seguridad estricta empresarial**.

  Importante:

  - La clave de característica bajo demanda de XCC se debe instalar en cada uno de los Servidores ThinkSystem V3 y V4 (con XCC2 o XCC3) seleccionados para utilizar este modo.
  - En este modo, si XClarity Administrator utiliza un certificado autofirmado, XClarity Administrator debe utilizar un certificado raíz y un certificado de servidor basados en RSA 3072-bit/SHA-384. Si XClarity Administrator utiliza un certificado externo firmado, XClarity Administrator debe generar una CSR basada en RSA 3072-bit/SHA-384 y ponerse en contacto con la CA externa para firmar un nuevo certificado de servidor basado en RSA 3072-bit/SHA-384.
  - Cuando XClarity Administrator utiliza un certificado basado en RSA 3072-bit/SHA-384, XClarity Administrator puede desconectar dispositivos que no sean servidores y chasis de Flex System (CMMS), servidores ThinkSystem, servidores ThinkServer, servidores System x M4 y M5, conmutadores de la serie Lenovo ThinkSystem DB, Lenovo RackSwitch, conmutadores Flex System, conmutadores Mellanox, dispositivos de almacenamiento ThinkSystem DE/DM, almacenamiento de biblioteca de cintas de IBM y servidores ThinkSystem SR635/SR655 actualizados con firmware anterior a 22C. Para continuar gestionando los dispositivos desconectados, configure otra instancia de XClarity Administrator con un certificado basado en 2048-bit/SHA-256.
- **Alta seguridad**. Este es el modo más seguro para los servidores ThinkSystem V1 y V2. Seleccione este modo para garantizar el cumplimiento de los estándares NIST y PFS (Perfect Forward Secrecy).

Este modo solo es compatible con los servidores ThinkSystem V1 y V2. Se requiere la versión de firmware de XCC publicada durante el segundo trimestre de 2023 o posterior.

Debe tener en cuenta las implicaciones siguientes que supone cambiar el modo criptográfico.

- Para XClarity Administrator v4.2 y versiones anteriores:
  - Para utilizar la autenticación gestionada para gestionar un servidor ThinkSystem o ThinkAgile cuando la versión de TLS en XCC está establecida en v1.3, la **Versión mínima de TLS del servidor** en XClarity Administrator también debe estar configurada en TLS v1.3 (consulte Configuración del modo criptográfico y los protocolos de comunicación en la documentación en línea).
- Para XClarity Administrator v4.0 y versiones anteriores:
  - No puede utilizar la *autenticación gestionada* para gestionar un servidor ThinkSystem o ThinkAgile cuando el modo de seguridad de XCC está establecido en **TLS v1.3**.
  - En el caso de servidores ThinkSystem o ThinkAgile gestionados mediante *autenticación gestionada*, el cambio del modo de seguridad de XCC a **TLS v1.3** mediante XClarity Administrator o XCC provocará que el servidor esté fuera de línea.
- No se admite el cambio de los modos de **Seguridad de compatibilidad** o **Seguridad estándar** al modo de **Seguridad estricta empresarial**.
- Si se actualiza del modo de **Seguridad de compatibilidad** al modo de **Seguridad estándar**, recibirá una advertencia si los certificados importados o las claves públicas SSH son no conformes. Sin embargo, aún podrá realizar la actualización al modo de **Seguridad estándar**.
- Si se realiza una degradación del modo de **Seguridad estricta empresarial** al modo de **Seguridad de compatibilidad** o **Seguridad estándar**:
  - El servidor se reinicia automáticamente para que entre en vigor el modo de seguridad.
  - Para servidores ThinkSystem V3 y V4: Si falta o caduca la clave FoD del modo estricto en XCC, y si XCC utiliza un certificado TLS autofirmado, XCC vuelve a generar el certificado TLS autofirmado en función del algoritmo de cumplimiento estricto estándar. XClarity Administrator muestra un error de conexión debido a un error de certificado. Para resolver el error de certificado no fiable, consulte Resolución de un certificado de servidor no fiable en la documentación en línea de XClarity Administrator. Si XCC utiliza un certificado TLS personalizado, XCC permite la degradación y le advierte que debe importar un certificado de servidor basado en la criptografía del modo de **Seguridad estándar**.

Puede cambiar los valores de seguridad para los siguientes dispositivos.
- Servidores Lenovo ThinkSystem con procesadores Intel o AMD (excepto SR635/SR655)
- Servidores Lenovo ThinkSystem V2
- Servidores Lenovo ThinkSystem V3 con procesadores Intel o AMD
- Servidores Lenovo ThinkSystem V4
- Servidores Lenovo ThinkEdge SE350 y SE450
- Servidores Lenovo System x

Para obtener más información sobre cómo configurar los modos de seguridad en el servidor gestionado, consulte Configuración de los valores de seguridad para un servidor en la documentación en línea de XClarity Administrator.

Certificados de seguridad

Lenovo XClarity Administrator utiliza certificados SSL para establecer comunicaciones seguras y de confianza entre XClarity Administrator y sus dispositivos gestionados (como los chasis y los procesadores de servicios en servidores System x), así como comunicaciones con XClarity Administrator por los usuarios con o con diferentes dispositivos. De forma predeterminada, XClarity Administrator, los CMM y los controladores de gestión de la placa base utilizan certificados generados por XClarity Administrator que están autofirmados y han sido emitidos por una entidad de certificación interna.

El certificado autofirmado de servidor predeterminado, que se genera de manera exclusiva en cada instancia de XClarity Administrator, proporciona suficiente seguridad para muchos entornos. Puede elegir permitir gestionar los certificados mediante XClarity Administrator o puede adoptar un papel más activo y personalizar o sustituir los certificados de servidor. XClarity Administrator 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.
- Generar una solicitud de firma de un certificado (CSR) que pueda enviarse a la entidad de certificación de su elección firmar un certificado personalizado que se pueda cargar después en XClarity Administrator para su uso como un certificado de servidor 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 Trabajo con certificados de seguridad en la XClarity Administrator documentación en línea.

Autenticación

Servidores de autenticación admitidos

El *servidor de autenticación* es un registro de usuario que se usa para autenticar las credenciales de los usuarios. Lenovo XClarity Administrator admite los siguientes tipos de servidores de autenticación.

- **Servidor de autenticación local**. De manera predeterminada, XClarity Administrator está configurado para utilizar el servidor del Protocolo ligero de acceso a directorios (LDAP) que se encuentra en el servidor de gestión.
- **Servidor LDAP externo**. Actualmente, se admiten Microsoft Active Directory y OpenLDAP. Este servidor debe residir en un servidor de Microsoft Windows externo conectado a la red de gestión. Cuando se utiliza un servidor LDAP externo, el servidor de autenticación local se deshabilita.

  Atención: Para configurar el método de vinculación de Active Directory para utilizar las credenciales de inicio de sesión, el controlador de gestión de la placa base para cada servidor gestionado debe estar ejecutando firmware a partir de septiembre de 2016 o con posterioridad.
- **Sistema de gestión de identidades externo**. Actualmente, solo se admite CyberArk.

  Si las cuentas de usuario de un servidor ThinkSystem o ThinkAgile están integradas en CyberArk, puede elegir que XClarity Administrator recupere las credenciales de CyberArk para iniciar sesión en el servidor cuando configure inicialmente los servidores para la gestión (con autenticación gestionada o local). Antes de que las credenciales se puedan recuperar de CyberArk, las rutas cyberark deben definirse en XClarity Administrator y se debe establecer confianza mutua entre CyberArk y XClarity Administrator mediante la autenticación mutua TLS a través de certificados de cliente.
- **SAML externo proveedor de identidad**. Actualmente, se admite Microsoft Active Directory Federation Services (AD FS). Además de ingresar un nombre de usuario y contraseña, se puede configurar una autenticación de varios factores para habilitar una seguridad adicional al solicitar un código PIN, la lectura de una tarjeta inteligente y un certificado de cliente. Cuando se utiliza un proveedor de identidad SAML, el servidor de autenticación local no se deshabilita. Se requieren cuentas de usuarios locales para iniciar sesión directamente en un chasis o servidor gestionado (a menos que se habilite la Encapsulación en ese dispositivo) para la autenticación de PowerShell y REST API y para la recuperación, si la autenticación externa no está disponible.

  Puede elegir usar un servidor LDAP externo y un proveedor de identidad externo. Si ambos están habilitados, el servidor LDAP externo se utiliza para iniciar sesión directamente en los dispositivos gestionados y el proveedor de identidad se utiliza para iniciar sesión en el servidor de gestión.

Para obtener más información sobre los servidores de autenticación, consulte Gestión del servidor de autenticación en la XClarity Administrator documentación en línea.

Autenticación de dispositivo

De forma predeterminada, los dispositivos se gestionan utilizando autenticación gestionada de XClarity Administrator para iniciar sesión en los dispositivos. Cuando se gestionan servidores de bastidor y chasis de Lenovo, puede optar por utilizar autenticación local o gestionada para iniciar sesión en los dispositivos.

- Cuando se utiliza la *autenticación local* para los servidores de bastidor, chasis de Lenovo y conmutadores de bastidor de Lenovo, XClarity Administrator usa una credencial almacenada para autenticar el dispositivo. La *credencial almacenada* puede corresponder con una cuenta de usuario activa en el dispositivo o con una cuenta de usuario en un servidor de Active Directory.

  Debe crear una credencial almacenada en XClarity Administrator que coincida con una cuenta de usuario activa en el dispositivo o una cuenta de usuario en un servidor de Active Directory antes de gestionar el dispositivo utilizando la autenticación local (consulte Gestión de credenciales almacenadas en la documentación en línea de XClarity Administrator).

  Notas:

  – Cuando se habilita la autenticación local para un dispositivo, no puede editar las credenciales almacenadas para dicho dispositivo utilizando XClarity Administrator.

  – Los dispositivos RackSwitch solo admiten credenciales almacenadas para la autenticación. Las credenciales de usuario de XClarity Administrator no se admiten.

- Usar la *autenticación gestionada* le permite gestionar y supervisar varios dispositivos utilizando las credenciales en el servidor de autenticación de XClarity Administrator en lugar las credenciales locales. Cuando un dispositivo se gestiona mediante autenticación gestionada (fuera de los servidores ThinkServer, System x M4 y conmutadores), XClarity Administrator configura el dispositivo gestionado y sus componentes instalados para utilizar el servidor autenticación de XClarity Administrator para la gestión centralizada de usuarios de todos los dispositivos.

  – Cuando se habilita la autenticación gestionada, puede gestionar dispositivos utilizando las credenciales ingresadas manualmente o almacenadas (consulte Gestión de cuentas de usuario y en la documentación en línea de XClarity Administrator).La credencial almacenada solo se utilizará hasta que XClarity Administrator configure los valores de LDAP en el dispositivo. Después de eso, cualquier cambio de la credencial almacenada no tiene efecto la gestión o la supervisión de dicho dispositivo.

  – Si se utiliza un servidor LDAP local o externo como el servidor de autenticación de XClarity Administrator, las cuentas de usuario que están definidas en el servidor de autenticación se utilizan para iniciar sesión en XClarity Administrator, en los CMM y en los controladores de gestión de la placa base del dominio de XClarity Administrator. Las cuentas de usuario del CMM local y del controlador de gestión están deshabilitadas.

    Nota: Para los servidores Think Edge SE450, SE350 V2 y SE360 V2, la cuenta de usuario local predeterminada permanece habilitada y el resto de las cuentas locales están deshabilitadas.

  – Si se utiliza un proveedor de identidad SAML 2.0 como el servidor de autenticación de XClarity Administrator, los dispositivos gestionados no pueden acceder a las cuentas SAML. No obstante, cuando se utiliza un proveedor de identidad SAML y un servidor LDAP juntos, si el proveedor de identidad utiliza cuentas que existen en el servidor LDAP, las cuentas de usuario LDAP pueden utilizarse para iniciar sesión en los dispositivos gestionados, mientras que los métodos de autenticación más avanzados proporcionados por SAML 2.0 (como la autenticación de varios factores y el inicio de sesión único) pueden utilizarse para iniciar sesión en XClarity Administrator.

  – El inicio de sesión único permite a un usuario que ya inició sesión en XClarity Administrator iniciar sesión automáticamente en el control de gestión de la placa base. El inicio de sesión único está habilitado de forma predeterminada cuando un servidor ThinkSystem o ThinkAgile se incluye en la gestión por XClarity Administrator (a menos que el servidor se esté gestionando con contraseñas de

CyberArk). Puede configurar el valor global para habilitar o deshabilitar el inicio de sesión único en todos los servidores ThinkSystem y ThinkAgile gestionados. Habilitar el inicio de sesión único para un servidor ThinkSystem y ThinkAgile específico sustituye el valor global de todos los servidores ThinkSystem y ThinkAgile (consulte Gestión de servidores en la documentación en línea de XClarity Administrator).

Nota: El inicio de sesión único se deshabilita automáticamente cuando se utiliza el sistema de gestión de identidades CyberArk para la autenticación.

- Cuando se habilita la autenticación gestionada para los servidores ThinkSystem SR635 y SR655:
  - El firmware del controlador de gestión de la placa base admite hasta cinco roles de usuario LDAP. XClarity Administrator añade estos roles de usuario LDAP a los servidores durante la gestión: **lxc-supervisor**, **lxc-sysmgr**, **lxc-admin**, **lxc-fw-admin** y **lxc-os-admin**.Los usuarios deben tener asignado al menos uno de los roles de usuario LDAP especificados para comunicarse con servidores ThinkSystem SR635 y SR655.
  - El firmware del controlador de gestión no admite usuarios LDAP que tengan el mismo nombre de usuario que el usuario local del servidor.
- Para servidores ThinkServer y System x M4, no se usa el servidor de autenticación de XClarity Administrator. Por el contrario, se crea una cuenta IPMI en el dispositivo con el prefijo “LXCA_” seguido de una cadena aleatoria. (Las cuentas de usuario de IPM local no se deshabilitan). Cuando anula la gestión de un servidor ThinkServer, se deshabilita la cuenta de usuario “LXCA_” y se sustituye el prefijo “LXCA_” con el prefijo “DISABLED_”. Para determinar si un servidor ThinkServer está gestionado por otra instancia, XClarity Administrator comprueba la existencia de cuentas IPMI con el prefijo “LXCA_”. Si elige forzar la gestión de un servidor ThinkServer gestionado, se deshabilitan todas las cuentas IPMI en el dispositivo con el prefijo “LXCA_” y cambian de nombre. Considere la posibilidad de borrar manualmente las cuentas IPMI que ya no se utilizan.

  Si usa credenciales ingresadas manualmente, XClarity Administrator crea automáticamente una credencial almacenada y usa esa credencial almacenada para gestionar el dispositivo.

  Notas: Cuando se habilita la autenticación gestionada para un dispositivo, no puede editar las credenciales almacenadas para dicho dispositivo utilizando XClarity Administrator.

  - Cada vez que gestiona un dispositivo mediante las credenciales ingresadas manualmente, se crea una nueva credencial almacenad para ese dispositivo, incluso si se han creado otras credenciales almacenadas para ese dispositivo durante un proceso de gestión anterior.
  - Cuando se anula la gestión de un dispositivo, XClarity Administrator no elimina las credenciales almacenadas que se crearon automáticamente para ese dispositivo durante el proceso de gestión.

Cuenta de usuario de recuperación

Si se especifica una contraseña de recuperación, XClarity Administrator deshabilita la cuenta de usuario CMM local o de controlador de gestión local y crea una nueva cuenta de usuario de recuperación (`RECOVERY_ID`) en el dispositivo para autenticaciones futuras. Si el servidor de gestión presenta un error, puede utilizar la cuenta `RECOVERY_ID` para iniciar sesión en el dispositivo a fin de llevar a cabo las acciones de recuperación necesarias para restaurar las funciones de gestión de la cuenta en el dispositivo hasta que el nodo de gestión se restaure o se sustituya.

Si anula la gestión de un dispositivo que tiene una cuenta de usuario de `RECOVERY_ID`, se habilitarán todas las cuentas de usuario local y la cuenta de `RECOVERY_ID` se eliminará.

- Si cambia las cuentas de usuario locales deshabilitadas (por ejemplo, si cambia una contraseña), estos cambios no afectarán a la cuenta de `RECOVERY_ID`. En el modo de autenticación gestionada, la cuenta de `RECOVERY_ID` es la única cuenta de usuario que está activa y operativa.

- Utilice la cuenta de `RECOVERY_ID` solo en caso de emergencia, como, por ejemplo, si el servidor de gestión falla o si hay un problema de red que impide las comunicaciones del dispositivo con XClarity Administrator para autenticar usuarios.
- La contraseña de `RECOVERY_ID` se especifica al detectar el dispositivo. Asegúrese de que registra la contraseña para utilizarla posteriormente.
- Los dispositivos RackSwitch solo admiten credenciales almacenadas para la autenticación. Las credenciales de usuario de XClarity Administrator no se admiten.

Para obtener información acerca de la recuperación de dispositivos gestionados, consulte Recuperación de la gestión de chasis con un CMM después de un error en el servidor de gestión y Recuperación de la gestión de un servidor de bastidor o de torre después de un error de servidor de gestión en la documentación en línea de XClarity Administrator.

Cuentas de usuarios y grupos de roles

Las *cuentas de usuario* se utilizan para iniciar sesión y gestionar Lenovo XClarity Administrator y todos los chasis y servidores gestionados. Las cuentas de usuario de XClarity Administrator están sujetas a dos procesos interdependientes: autenticación y autorización.

La *autenticación* es el mecanismo de seguridad con el que se verifican las credenciales de un usuario. En el proceso de autenticación se utilizan las credenciales del usuario que están almacenadas en el servidor de autenticación configurado. También impide que los servidores de gestión o aplicaciones de sistemas no autorizados accedan a los recursos. Después de la autenticación, el usuario puede acceder a XClarity Administrator. No obstante, para acceder a un recurso específico o para llevar a cabo una tarea determinada, el usuario también debe contar con la autorización adecuada.

En la *autorización* se comprueban los permisos del usuario autenticado y se controla el acceso a los recursos según la calidad de miembro del usuario concreto en un grupo de roles. Los *grupos de roles* se utilizan para asignar roles específicos a un conjunto de cuentas de usuario que se definen y gestionan en el servidor de autenticación. Por ejemplo, si un usuario es miembro de un grupo de roles con permisos de supervisor, dicho usuario puede crear, editar y eliminar cuentas de usuarios de XClarity Administrator. Si un usuario tiene permisos de operador, solo puede ver la información de la cuenta de usuario.

Para obtener más información sobre las cuentas de usuario y los grupos de roles, consulte Gestión de cuentas de usuario en la XClarity Administrator documentación en línea.

Seguridad de la cuenta de usuario

Los valores de la cuenta de usuario controlan la complejidad de la contraseña, el bloqueo de la cuenta y el tiempo de espera por inactividad de la sesión web. Puede cambiar los valores de seguridad de la cuenta.

Para obtener más información acerca de los valores de seguridad de la cuenta, consulte Cambio de los valores de seguridad de una cuenta de usuario en la documentación en línea de Lenovo XClarity Administrator.

Consideraciones de alta disponibilidad

Si desea configurar la alta disponibilidad para Lenovo XClarity Administrator, use las funciones de alta disponibilidad que forman parte del sistema operativo del host o el entorno de contenedor.

Docker

Puede usar Docker Datacenter para configurar un entorno de alta disponibilidad para contenedores de XClarity Administrator que se ejecutan en Docker Engine. Para obtener más información sobre la alta disponibilidad de Docker Datacenter, consulte Página web de Arquitectura de alta disponibilidad aplicaciones con Docker Datacenter.

Citrix

Utilice la función de alta disponibilidad que se proporciona con el entorno Citrix. Para obtener más información, consulte Implementación de alta disponibilidad (Citrix) en la documentación en línea de XClarity Administrator..

KVM (CentOS, RedHat, Rocky y Ubuntu)

Puede usar OpenStack, o si ya tiene un entorno de alta disponibilidad, continuar utilizando los procesos internos. Para obtener más información sobre la alta disponibilidad de OpenStack, consulte Implementación de alta disponibilidad (KVM) en la documentación en línea de XClarity Administrator..

Microsoft Hyper-V

Utilice la función de alta disponibilidad que se proporciona con el entorno ESXi. Para obtener información, consulte Implementación de la alta disponibilidad (Microsoft Hyper-V) en la documentación en línea de XClarity Administrator..

Nutanix AHV

Utilice la función de alta disponibilidad de máquina virtual proporcionada para el entorno Nutanix AHV. Para obtener más información, consulte Implementación de alta disponibilidad (Nutanix) en la documentación en línea de XClarity Administrator..

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:

- Un mínimo de dos hosts 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 puede instalarse en uno de los hosts que se usan en el clúster. Sin embargo, si ese host se apaga o no es utilizable, también se 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).

Para obtener información detallada sobre la configuración de un clúster de VMware High Availability, consulte Implementación de alta disponibilidad (VMware ESXi) en la documentación en línea de XClarity Administrator..

Características bajo demanda

Características bajo demanda activa características sin necesidad de instalar hardware o adquirir equipos nuevos. Esta activación se realiza adquiriendo e instalando las Características bajo demanda correspondientes.

Para utilizar las operaciones de control remoto y de despliegue del sistema operativo en Lenovo XClarity Administrator, debe habilitar la actualización avanzada de XClarity Controller empresarial o MM para

servidores que no se entregan de forma predeterminada con estas características ya activadas. Estas operaciones también requieren que se haya instalado una clave de Características bajo demanda de presencia remota en los servidores ThinkSystem, convergentes y System x. Puede determinar si la presencia remota está habilitada, deshabilitada o no instalada en un servidor desde la página Servidores (consulte Visualización del estado de un servidor gestionado en la documentación en línea de XClarity Administrator).

Algunas funciones avanzadas del servidor se activan utilizando las claves de Características bajo demanda. Si las características tienen valores configurables que aparecen durante la configuración de la UEFI, puede configurar los valores utilizando Patrones de configuración; no obstante, la configuración resultante no se activa hasta que se instala la clave de Características bajo demanda correspondiente.

Nota: No puede instalar ni gestionar claves de Características bajo demanda desde XClarity Administrator; no obstante, puede ver la lista de claves de Características bajo demanda que están instaladas en la actualidad en los servidores gestionados. Para obtener más información sobre cómo ver las claves de Características bajo demanda instaladas, consulte Visualización de las claves de característica bajo demanda en la documentación en línea de XClarity Administrator.

Para adquirir e instalar claves de Características bajo demanda, siga estos pasos:

1. Adquiera la actualización de Características bajo demanda utilizando el número de referencia adecuado.

   Puede adquirir claves desde Características del portal web on Demand. Una vez finalizada la compra, recibirá un código de autorización por correo electrónico.
2. En la Características del portal web on Demand, introduzca el código de autorización que ha recibido, junto con el identificador exclusivo de sistema del servidor que desea actualizar.
3. Descargue la clave de activación en formato de archivo .KEY.
4. Cargue la clave de activación en el controlador de gestión del servidor.
5. Reinicie el servidor. La característica se activa cuando finaliza el reinicio.

Para obtener más información acerca de las claves de Características bajo demanda, consulte el Uso de Lenovo Features on Demand.

Capítulo 3. Instalación de Lenovo XClarity Administrator

Existen varias formas de conectar los dispositivos gestionables a la red y configurar el dispositivo virtual Lenovo XClarity Administrator para gestionar estos dispositivos. Utilice la información de esta sección como guía para configurar los dispositivos gestionables e instalar el XClarity Administrator

En esta sección se describe cómo configurar diversas topologías comunes. Esta sección no cubre todas las topologías de red posibles.

Atención: Para gestionar dispositivos, XClarity Administrator debe tener acceso a la red de gestión.

Más información:

- Instalación de Lenovo XClarity Administrator en VMware vCenter
- Instalación de Lenovo XClarity Administrator en VMware vSphere
- Instalación de Lenovo XClarity Administrator en Windows Hyper-V
- Instalación de Lenovo XClarity Administrator en Red Hat KVM

Datos únicos y red de gestión

En esta topología de red, tanto la red de datos como la red de gestión son la misma red.

Antes de empezar

Asegúrese de que estén habilitados todos los puertos apropiados, incluidos los puertos que XClarity Administrator necesita (consulte Disponibilidad de puertos).

Asegúrese de que el firmware mínimo necesario esté instalado en cada dispositivo que desee gestionar mediante XClarity Administrator. Encontrará los niveles de firmware mínimos requeridos del Soporte de XClarity Administrator: página web de compatibilidad haciendo clic en la pestaña **Compatibilidad** y, a continuación, pulsando el enlace de los tipos de dispositivo correspondientes.

Importante: configure los componentes de los dispositivos de forma que minimicen los cambios de dirección IP. Plantéese la posibilidad de utilizar direcciones IP estáticas en lugar del protocolo de configuración dinámica de host (DHCP). Si se utiliza DHCP, asegúrese de que los cambios de dirección IP se minimizan.

Acerca de esta tarea

Para los dispositivos virtuales, todas las comunicaciones entre XClarity Administrator y la red se producen a través de la interfaz de red eth0 en el host. Para la información sobre el consumo, puede utilizar un nombre personalizado; sin embargo, este escenario utiliza eth0.

Importante: Implementar una red de datos compartidos y de gestión puede provocar interrupciones en el tráfico, como paquetes que se caen o problemas de conectividad de red de gestión, según su configuración de red (por ejemplo, si el tráfico de los servidores tiene una prioridad alta y el tráfico de los controladores de gestión tiene una prioridad baja). La red de gestión utiliza el tráfico UDP, además de TCP. El tráfico UDP puede tener una prioridad más baja cuando el tráfico de red es alto.

En la figura siguiente se muestra una forma de configurar el entorno cuando la red de datos y la red de gestión son la misma. Los números de la figura corresponden a los pasos numerados de las secciones siguientes.

Nota: Esta figura no representa todas las opciones de cableado que podrían ser necesarias para su entorno. En cambio, esta figura muestra únicamente los requisitos de la opción de cableado para los servidores de bastidor, conmutadores de bastidor, conmutadores Flex y CMM, en la medida en que están relacionados con la configuración de una sola red de datos y de gestión.

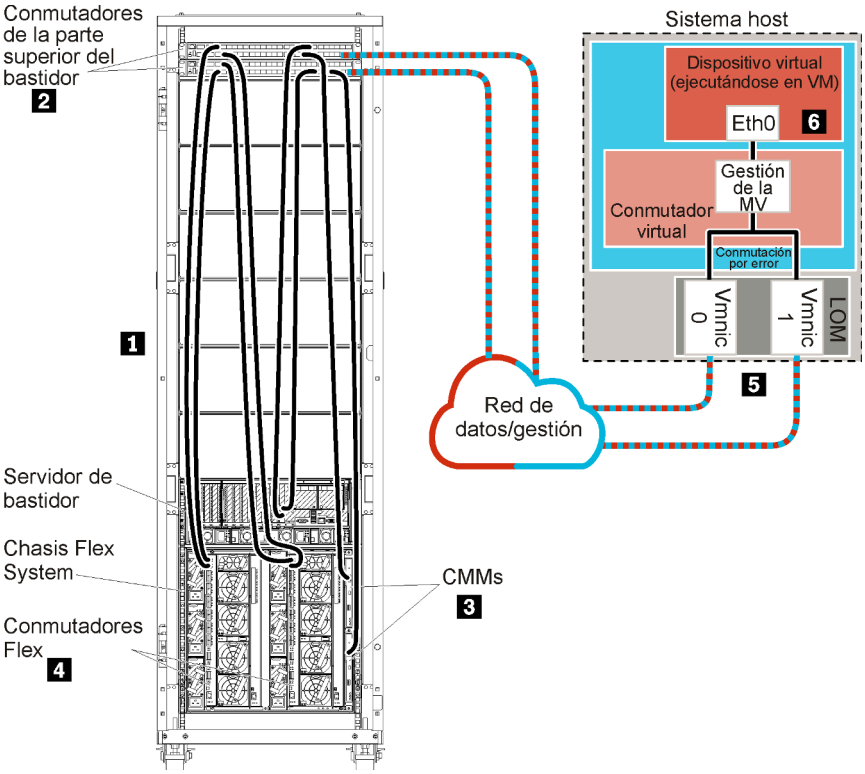


Figura 8. Ejemplo de topología de una sola red de datos y gestión para un dispositivo virtual

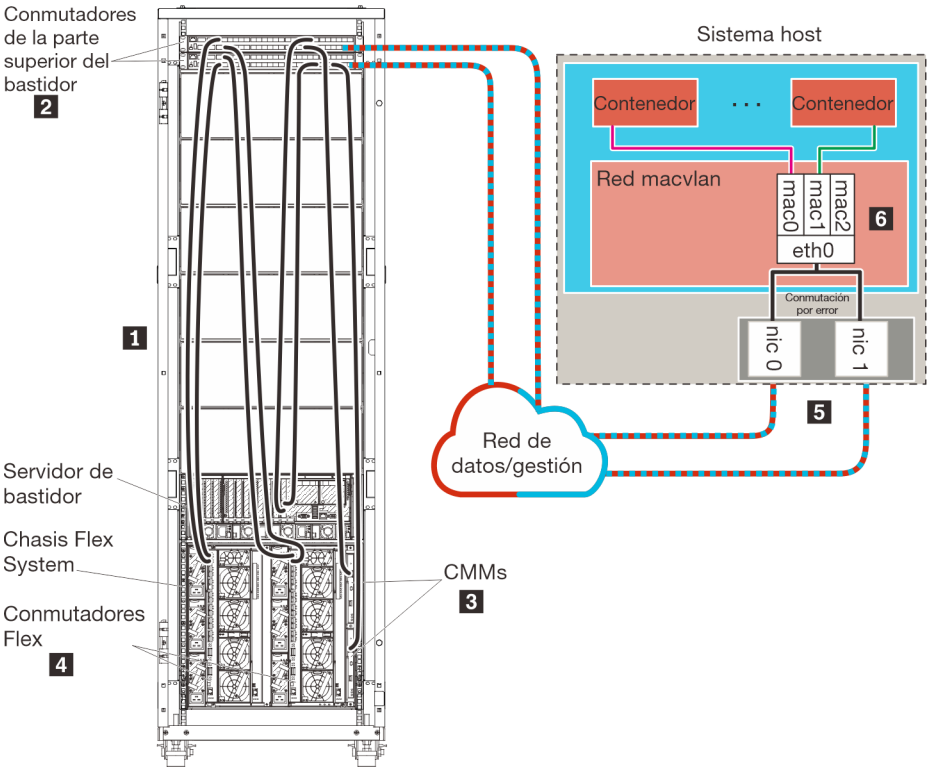


Figura 9. Ejemplo de topología de una sola red de datos y gestión para contenedores

Importante: Puede configurar XClarity Administrator en cualquier sistema que cumpla los requisitos de XClarity Administrator, incluido servidor gestionado. Si utiliza un servidor gestionado para el host XClarity Administrator:

- Debe implementar una topología de redes de datos y de gestión separadas virtualmente o bien una topología de una sola red de datos y gestión.
- No puede utilizar XClarity Administrator para aplicar actualizaciones de firmware a ese servidor gestionado. Aunque solo se aplique parte del firmware con la activación inmediata, XClarity Administrator fuerza el reinicio del servidor de destino, lo que reinicia también XClarity Administrator. Cuando se aplica con la activación diferida, solo se aplica determinado firmware cuando se reinicia el host de XClarity Administrator.
- Si utiliza un servidor en un chasis de Flex System, asegúrese de que el servidor esté configurado para encenderse automáticamente. Puede configurar esta opción en la interfaz web del CMM al hacer clic en **Gestión de chasis → Nodos de cálculo** y después al seleccionar el servidor y seleccionar **Encendido automático** para el **Modo de encendido automático**.

Si tiene intención de instalarXClarity Administrator para gestionar chasis y servidores de bastidor existentes que ya se han configurado, continúe con el Paso 5: Instale y configure el host.

Para obtener información adicional sobre cómo planificar esta topología, incluida información sobre los valores de red y la configuración de Eth1 y Eth0, consulte Una sola red de datos y de gestión.

Paso 1: Cableado del chasis, los servidores de bastidor y el host Lenovo XClarity Administrator a los conmutadores de la parte superior del bastidor

Conecte el chasis, los servidores de bastidor y el host XClarity Administrator a los conmutadores de la parte superior del bastidor para habilitar las comunicaciones entre los dispositivos y la red.

Procedimiento

Conecte cada conmutador Flex y CMM de cada chasis, de cada servidor de bastidor y del host XClarity Administrator a los dos conmutadores de la parte superior del bastidor. Puede elegir cualquier puerto de los conmutadores de la parte superior del bastidor.

La figura siguiente es un ejemplo que muestra el cableado del chasis (Conmutadores Flex y CMM), los servidores de bastidor y el host XClarity Administrator a los conmutadores de la parte superior del bastidor.

Nota: Esta figura no representa todas las opciones de cableado que podrían ser necesarias para su entorno. En cambio, esta figura muestra únicamente los requisitos de la opción de cableado para los servidores de bastidor, conmutadores de bastidor, conmutadores Flex y CMM, en la medida en que están relacionados con la configuración de una sola red de datos y de gestión.

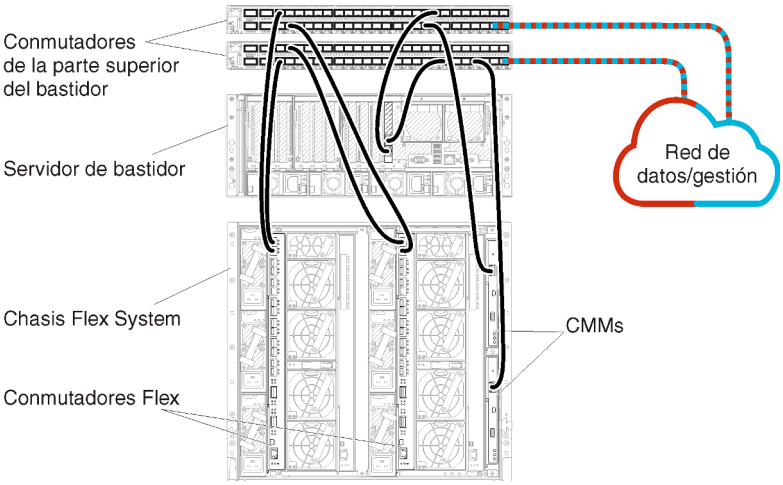


Figura 10. Ejemplo de cableado para una sola red de datos y gestión

Paso 2: Configuración de los conmutadores de la parte superior del bastidor

Configure los conmutadores de la parte superior del bastidor.

Antes de empezar

Además de los requisitos de configuración normales para los conmutadores de la parte superior del bastidor, asegúrese de que estén habilitados todos los puertos apropiados, incluidos los puertos externos a los Conmutadores Flex, a los servidores de bastidor y a la red, así como los puertos internos al CMM, a los servidores de bastidor y a la red.

Procedimiento

Los pasos de configuración pueden variar en función del tipo de los RackSwitch instalados.

Para obtener información acerca de cómo configurar los conmutadores de la parte superior del bastidor de Lenovo, consulte la Documentación en línea de RackSwitch en System x. Si se instala otro conmutador de la parte superior del bastidor, consulte la documentación que se proporciona con ese conmutador.

Paso 3: Configuración de los Chassis Management Module (CMM)

Configure el Chassis Management Module (CMM) principal de su chasis para gestionar todos los dispositivos de este último.

Acerca de esta tarea

Para obtener información detallada acerca de cómo configurar un CMM, consulte Configuración de los componentes del chasis en la documentación en línea de Flex System.

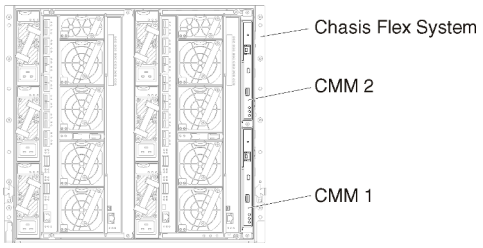
Además, consulte los pasos 4.1 a 4.5 del póster de instrucciones proporcionado con el chasis.

Procedimiento

Lleve a cabo los pasos siguientes para configurar el CMM.

Si se han instalado dos CMM, configure solo el *principal*, lo que sincroniza automáticamente la configuración con el CMM en espera.

Paso 1. Conecte un cable Ethernet desde el CMM de la bahía 1 a una estación de trabajo cliente para crear una conexión directa.



Para conectar el CMM por primera vez, es posible que tenga que cambiar las propiedades del Protocolo de Internet en la estación de trabajo cliente.

Importante: Asegúrese de que la subred de la estación de trabajo cliente sea la misma que la subred del CMM. (La subred del CMM predeterminada es 255.255.255.0.) La dirección IP elegida para la estación de trabajo cliente debe estar en la misma red que el CMM (por ejemplo, 192.168.70.0 - 192.168.70.24).

Paso 2. Para iniciar la interfaz de gestión del CMM, abra un navegador web en la estación de trabajo cliente y diríjalo a la dirección IP del CMM.

Notas:

- Asegúrese de utilizar una conexión segura y de incluir **https** en la URL (por ejemplo, https://192.168.70.100). Si no incluye https, recibirá un error de página no encontrada.
- Si utiliza la dirección IP predeterminada (192.168.70.100), puede que transcurran unos minutos hasta que la interfaz de gestión del CMM esté disponible. Este retraso se produce porque el CMM trata de obtener una dirección DHCP durante dos minutos antes de volver a la dirección estática predeterminada.

Paso 3. Inicie sesión en la interfaz de gestión del CMM utilizando el Id. de usuario predeterminado `USERID` y la contraseña `PASSWORD`. Una vez que haya iniciado sesión, deberá cambiar la contraseña predeterminada.

Paso 4. Complete el Asistente de configuración inicial del CMM para especificar los detalles de su entorno. El Asistente de configuración inicial incluye las siguientes opciones:

- Consulte el inventario del chasis y el estado.
- Importar la configuración desde un archivo de configuración existente.
- Configure los valores generales del CMM.
- Configure la fecha y hora del CMM.

  Consejo: cuando instale XClarity Administrator, configure XClarity Administrator y todos los chasis gestionados por XClarity Administrator para que utilicen un servidor NTP.
- Configure la información IP del CMM.
- Configure la política de seguridad del CMM.
- Configure el sistema de nombres de dominio (DNS).
- Configure los despachadores de sucesos.

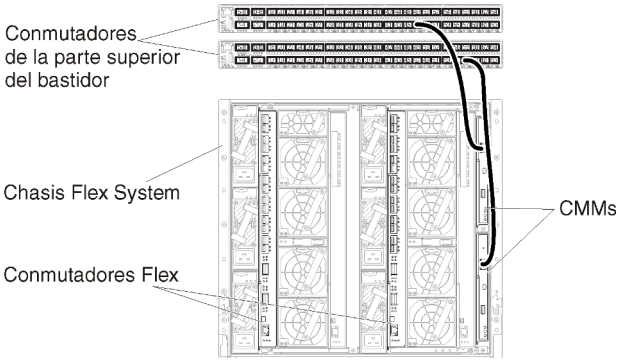
Paso 5. Después de guardar los valores del asistente de configuración y aplicar los cambios, configure las direcciones IP de todos los componentes del chasis.

Consulte el paso 4.6 del poster de instrucciones proporcionado con el chasis.

Nota: Debe restablecer el procesador de gestión del sistema de cada nodo de cálculo y reiniciar los conmutadores Flex para mostrar las nuevas direcciones IP.

Paso 6. Reinicie el CMM mediante la interfaz de gestión del CMM.

Paso 7. Cuando el CMM se esté reiniciando, conecte un cable desde el puerto Ethernet del CMM a su red.



Paso 8. Inicie sesión en la interfaz de gestión del CMM utilizando la nueva dirección IP.

Después de finalizar

También puede configurar el CMM para que admita redundancia. Utilice el sistema de ayuda del CMM para obtener más información acerca de los campos que están disponibles en cada una de las páginas siguientes.

- Configure la conmutación por error para el CMM en caso de que se produzca un fallo de hardware en el CMM principal. En la interfaz de gestión del CMM, haga clic en **Gestión del módulo de gestión → Propiedades → Conmutación por error avanzada**.
- Configure la conmutación por error avanzada como resultado de un problema de red (enlace ascendente). En la interfaz de gestión del CMM, haga clic en **Gestión del módulo de gestión → Red**, haga clic en la pestaña **Ethernet** y, a continuación, haga clic en **Ethernet avanzada**. Como mínimo, asegúrese de seleccionar la casilla **Conmutación por error si hay pérdida de vínculo de red física**.

Paso 4: Configuración de Conmutadores Flex

Configure Conmutadores Flex (módulos de E/S) en cada chasis.

Antes de empezar

Asegúrese de que están habilitados todos los puertos apropiados, incluidos los puertos externos que van desde el conmutador Flex al conmutador de la parte superior del bastidor y los puertos internos al CMM.

Si los conmutadores Flex se configuran para obtener valores de red dinámicos (dirección IP, máscara de red, puerta de enlace y dirección DNS) a través de DHCP, asegúrese de que dichos conmutadores tienen unos valores coherentes (por ejemplo, compruebe que las direcciones IP se encuentran en la misma red que el CMM).

Importante: Para cada chasis de Flex System, asegúrese de que el tipo de entramado de la tarjeta de expansión de cada servidor en el chasis sea compatible con el tipo de entramado de todos los conmutadores Flex del mismo chasis. Por ejemplo, si instala conmutadores Ethernet en un chasis, todos los servidores de dicho chasis deben tener conectividad Ethernet a través del conector LAN en la placa madre o de una tarjeta de expansión Ethernet. Para obtener más información acerca de cómo configurar los conmutadores Flex, consulte la Configuración de los módulos de E/S en la documentación en línea de Flex System.

Procedimiento

Los pasos de configuración pueden variar en función del tipo de Conmutadores Flex instalado. Para obtener más información acerca de cada uno de los Conmutadores Flex compatibles, consulte Conmutadores de red Flex System en la documentación en línea de Flex System.

Normalmente, tendrá que configurar los conmutadores Flex en las bahías 1 y 2 de conmutadores Flex.

Consejo: la bahía 2 del conmutador Flex es la tercera bahía de los módulos si se mira a la parte posterior del chasis.

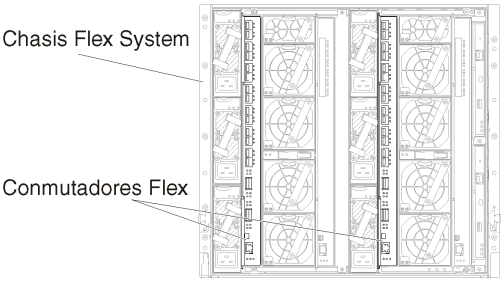


Figura 11. Ubicaciones de los Conmutador Flex en un chasis

Paso 5: Instale y configure el host

Puede instalar Docker en cualquier servidor que cumpla los requisitos para Lenovo XClarity Administrator.

Antes de empezar

Puede usar Docker Datacenter para configurar un entorno de alta disponibilidad para contenedores de XClarity Administrator que se ejecutan en Docker Engine. Para obtener más información sobre la alta disponibilidad de Docker Datacenter, consulte Página web de Arquitectura de alta disponibilidad aplicaciones con Docker Datacenter.

Asegúrese de que el host cumple los requisitos previos definidos en Requisitos previos de hardware y software.

Asegúrese de que el sistema host esté en la misma red que los dispositivos que desea gestionar.

Importante: Puede configurar XClarity Administrator en cualquier sistema que cumpla los requisitos de XClarity Administrator, incluido servidor gestionado. Si utiliza un servidor gestionado para el host XClarity Administrator:

- Debe implementar una topología de redes de datos y de gestión separadas virtualmente o bien una topología de una sola red de datos y gestión.
- No puede utilizar XClarity Administrator para aplicar actualizaciones de firmware a ese servidor gestionado. Aunque solo se aplique parte del firmware con la activación inmediata, XClarity Administrator fuerza el reinicio del servidor de destino, lo que reinicia también XClarity Administrator. Cuando se aplica con la activación diferida, solo se aplica determinado firmware cuando se reinicia el host de XClarity Administrator.
- Si utiliza un servidor en un chasis de Flex System, asegúrese de que el servidor esté configurado para encenderse automáticamente. Puede configurar esta opción en la interfaz web del CMM al hacer clic en **Gestión de chasis → Nodos de cálculo** y después al seleccionar el servidor y seleccionar **Encendido automático** para el **Modo de encendido automático**.

Procedimiento

Instale y configure Docker en el host siguiendo las instrucciones proporcionadas con su distribución de Docker.

Paso 6. Instalación y configuración de un XClarity Administrator

Instale y configure el contenedor Lenovo XClarity Administrator en el host Docker recién instalado.

Antes de empezar

Asegúrese de que el sistema host cumpla los requisitos de hardware y software (consulte Requisitos previos de hardware y software).

Asegúrese de que estén habilitados todos los puertos apropiados, incluidos los puertos que XClarity Administrator necesita (consulte Disponibilidad de puertos).

Asegúrese de que el sistema host esté en la misma red que los dispositivos que desea gestionar.

Asegúrese de que el SO host y el XClarity Administrator usan el mismo servidor NTP.

XClarity Administrator permite utilizar un nombre personalizado para la red para la gestión de datos, la gestión del hardware y el despliegue del SO (consulte Configuraciones de red). En estos ejemplos del siguiente procedimiento se utiliza eth0.

Asegúrese de que la red macvlan esté cargada en el kernel en el sistema host. Para comprobar si está cargado, utilice el comando **lsmod | grep macvlan**. Para cargar macvlan en el kernel, ejecute el comando **modprobe macvlan**.

Asegúrese de utilizar un nombre y una dirección IP únicos para cada contenedor cuando ejecute varios contenedores de XClarity Administrator en el mismo host.

Si tiene pensado gestionar ThinkServer y otros dispositivos heredados, asegúrese de que Docker esté habilitado para admitir IPv6.

1. Edite el archivo /etc/docker/daemon.json, establezca la clave **ipv6** en verdadero y establezca la clave **fixed-cidr-v6** en la subred IPv6. A continuación, se muestra un archivo daemon de ejemplo.
```
{
   "ipv6": true,
   "fixed-cidr-v6": "2001:db8:1::/64",
   "experimental": true,
   "ip6tables": true
}
```
2. Ejecute el siguiente comando para volver a cargar el archivo de configuración de Docker.
```
systemctl reload docker
```

Nota: XClarity Administrator *no* se ejecuta como un contenedor con privilegios.

Las reglas de firewall no están configuradas en el contenedor XClarity Administrator. Para agregar reglas de firewall para el contenedor en el sistema host, siga estos pasos.

1. Ejecute el siguiente comando para obtener la ID de proceso Docker, identificada por “NSPID”.
```
docker inspect --format='{{ .State.Pid }}' "$CONTAINER_NAME"
```
2. Ejecute el siguiente comando para crear un enlace simbólico.
```
LINKFILE="/var/run/netns/$NSPID"
mkdir -p /var/run/netns
/bin/rm -f "$LINKFILE"
ln -s "/proc/$NSPID/ns/net" "$LINKFILE"
```
3. Ejecute el siguiente comando para configurar las reglas iptables adecuadas.
```
ip netns exec $NSPID iptables -I OUTPUT -j DROP
```
4. Ejecute el siguiente comando para asegurarse de que se eliminen todos los enlaces.
```
/bin/rm -f "$LINKFILE"
```

Procedimiento

Para instalar un contenedor XClarity Administrator utilizando el método Docker compose, realice los pasos siguientes.

Paso 1. Descargue la imagen del dispositivo virtual de XClarity Administrator, el archivo de entorno y el archivo YAML desde el Página web de descarga de XClarity Administrator hasta una estación de trabajo cliente. Inicie sesión en el sitio web y utilice la clave de acceso que se le facilitó para descargar la imagen.

Paso 2. Importe la imagen del contenedor de XClarity Administrator a su host y ejecute el siguiente comando.
```
docker load -i lnvgy_sw_lxca_<ver>_anyos_noarch.tar.gz
```

Paso 3. Edite el archivo `docker_compose.env` y actualice las variables de entorno siguientes.

- **CONTAINER_NAME**. Nombre de contenedor único, que se utiliza para crear volúmenes de docker para cada instancia de XClarity Administrator (por ejemplo, `CONTAINER_NAME=LXCA-203`)
- **ADDRESS**. Dirección IPv4 estática para el contenedor (por ejemplo, `ADDRESS=192.0.2.0`)
- **BACKUP_MOUNT**. (Opcional) Ruta para el recurso compartido remoto que se puede utilizar para almacenar las copias de seguridad de XClarity Administrator. Debe ser `/mnt/backup_share`.
- **FIRMWARE_MOUNT**. (Opcional) Ruta de acceso para la unidad compartida remota que se puede utilizar como repositorio remoto para las actualizaciones de firmware. Debe ser `/mnt/fw_share`.

A continuación hay un archivo de entorno de muestra.
```
CONTAINER_NAME="LXCA-203"
ADDRESS="192.0.2.0"
BACKUP_MOUNT="/mnt/backup_share"
FIRMWARE_MOUNT="/mnt/fw_share"
```

Paso 4. Edite el archivo `docker_compose.yml` y actualice las propiedades siguientes.

- Establezca la propiedad **image** con el nombre del archivo de imagen de instalación utilizado en el paso 2.

  Nota: Puede cambiar el nombre de archivo de la imagen (por ejemplo, a “más reciente”) mediante el comando `docker tag`.
- Si desea utilizar recursos compartidos remotos como repositorio de firmware remoto y almacenar copias de seguridad de XClarity Administrator, establecer el punto de montaje del host para cada unidad compartida remota en la propiedad **volumes**.
- Establezca la propiedad **DNS** en la dirección IP de los servidores DNS.
- El contenedor comparte el grupo de recursos de procesador y de memoria que están disponibles para el host. Opcionalmente, defina los límites del uso de recursos estableciendo las **cpus** y las propiedades de **memoria**.
- Establezca la propiedad **primaria** al nombre de la interfaz de red del sistema host que se va a utilizar como interfaz primaria para la interfaz macvlan en el contenedor. Esta interfaz debe tener acceso directo a la subred asignada al contenedor.
- Establezca la **subred** y la **puerta de enlace** de acuerdo con la topología de su red. Normalmente, la subred y la puerta de enlace son para la red de gestión a la que pertenece ${ADDRESS}.
- Si desea admitir IPv6, establezca la propiedad **enable_ipv6** en verdadero, establezca la propiedad **ipv6_address** en la dirección IPv6 y añada otro conjunto de propiedades de **subred** y **puerta de enlace** de acuerdo con la topología de su red (normalmente para la red de gestión a la que pertenece la dirección IPv6).

Nota: XClarity Administrator utiliza macvlan para configurar la red de contenedores. Para obtener más información, consulte el tema Página web de Uso de redes macvlan

A continuación, se muestra un archivo YML de ejemplo, con IPv6 habilitado.

```
version: '3.8'

services:

  lxca:
    image: lenovo/lxca:4.1.0-124
    container_name: ${CONTAINER_NAME}
    tty: true
    stop_grace_period: 60s
    volumes:
      #bind mount example
      - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
      - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
      #docker volume mount
      - data:/opt/lenovo/lxca/data
      - postgresql:/var/lib/postgresql
      - log:/var/log
      - confluent-etc:/etc/confluent
      - confluent-log:/var/log/confluent
      - confluent:/var/lib/confluent
      - propconf:/opt/lenovo/lxca/bin/conf
      - ssh:/etc/ssh
      - xcat:/etc/xcat
    networks:
      lan:
        ipv4_address: ${ADDRESS}
```

```
          ipv6_address: "2001:8003:7d51:2003::2"
      dns:
        - 192.0.2.10
        - 192.0.2.11
      deploy:
        resources:
          limits:
            cpus: "2.0"
            memory: "8g"

volumes:
  data:
    name: ${CONTAINER_NAME}-data
  postgresql:
    name: ${CONTAINER_NAME}-postgresql
  log:
    name: ${CONTAINER_NAME}-log
  confluent-etc:
    name: ${CONTAINER_NAME}-confluent-etc
  confluent-log:
    name: ${CONTAINER_NAME}-confluent-log
  confluent:
    name: ${CONTAINER_NAME}-confluent
  propconf:
    name: ${CONTAINER_NAME}-propconf
  ssh:
    name: ${CONTAINER_NAME}-ssh
  xcat:
    name: ${CONTAINER_NAME}-xcat

networks:
  lan:
    name: lan
    driver: macvlan
    enable_ipv6: true
    driver_opts:
      parent: eth0
    ipam:
      config:
        - subnet: 192.0.0.0/19
          gateway: 192.0.30.1
        - subnet: "2001:8003:7d51:2000::/80"
          gateway: "2001:8003:7d51:2000::1"
```

Paso 5. Despliegue la imagen en docker al ejecutar el siguiente comando, donde <*ENV_FILENAME*> es el nombre del archivo de variables ambientales que creó en el paso 2.

```
COMPOSE_HTTP_TIMEOUT=300 docker-compose -p ${CONTAINER_NAME} --env-file <ENV_FILENAME> up -d
```

Después de finalizar

Inicie sesión en XClarity Administrator y realice la configuración correspondiente (consulte el Acceso a la interfaz web de Lenovo XClarity Administrator por primera vez y el Configuración de Lenovo XClarity Administrator).

Datos separados físicamente y redes de gestión

En esta topología, la red de datos y la red de gestión son redes separadas físicamente. Las comunicaciones de gestión entre Lenovo XClarity Administrator y la red se producen a través de la interfaz de red Eth0 en el host. Las comunicaciones de datos se producen a través de la interfaz de red Eth1.

Antes de empezar

Asegúrese de que estén habilitados todos los puertos apropiados, incluidos los puertos que XClarity Administrator necesita (consulte Disponibilidad de puertos).

Asegúrese de que el firmware mínimo necesario esté instalado en cada dispositivo que desee gestionar mediante XClarity Administrator. Encontrará los niveles de firmware mínimos requeridos del Soporte de XClarity Administrator: página web de compatibilidad haciendo clic en la pestaña **Compatibilidad** y, a continuación, pulsando el enlace de los tipos de dispositivo correspondientes.

Importante: configure los componentes de los dispositivos de forma que minimicen los cambios de dirección IP. Plantéese la posibilidad de utilizar direcciones IP estáticas en lugar del protocolo de configuración dinámica de host (DHCP). Si se utiliza DHCP, asegúrese de que los cambios de dirección IP se minimizan.

Acerca de esta tarea

En la figura siguiente se muestra una forma de configurar el entorno cuando la red de datos y la red de gestión son redes físicamente distintas. Los números de la figura corresponden a los pasos numerados de las secciones siguientes.

Nota: Esta figura no representa todas las opciones de cableado que podrían ser necesarias para su entorno. En cambio, esta figura muestra únicamente los requisitos de la opción de cableado para los conmutadores Flex, los CMM y los servidores de bastidor, en la medida en que están relacionados con la configuración de redes de datos y de gestión separadas físicamente.

Consejo: en vez de configurar que se conecten dos conmutadores físicos a cada red para tener redundancia (lo que hace un total de cuatro conmutadores), puede establecer que solo se conecte un conmutador físico a cada red (lo que hace un total de dos conmutadores). En ese caso, cada conmutador estaría conectado a dos redes y se podrían implementar dos VLAN: una para la red de datos y otra para la red de gestión, con el fin de segregar el tráfico de datos.

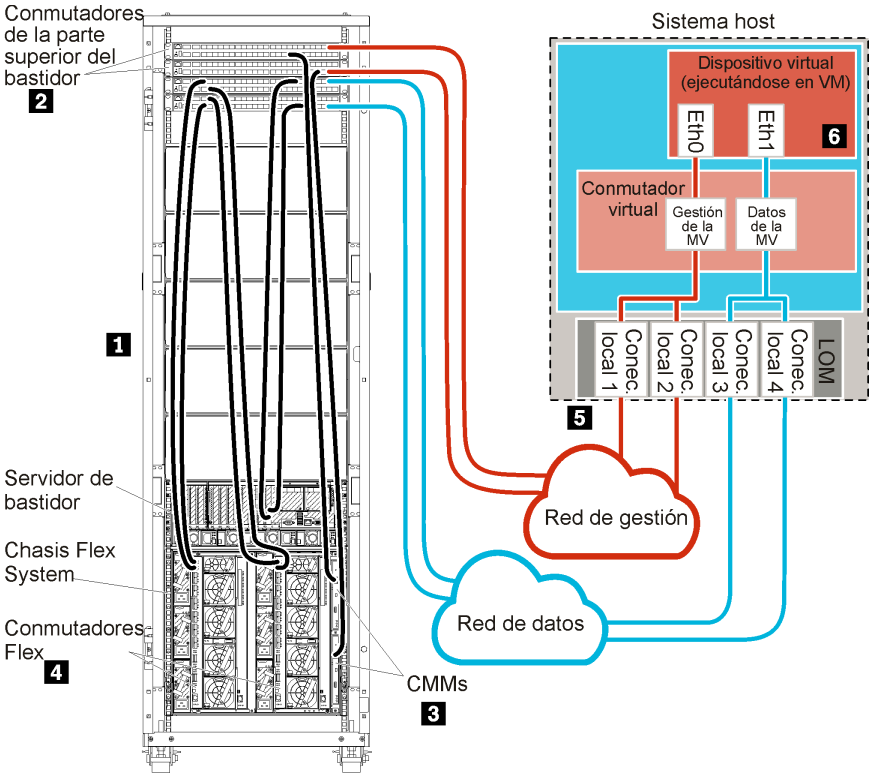


Figura 12. Ejemplo de datos separados físicamente y topología de red de administración para un dispositivo virtual

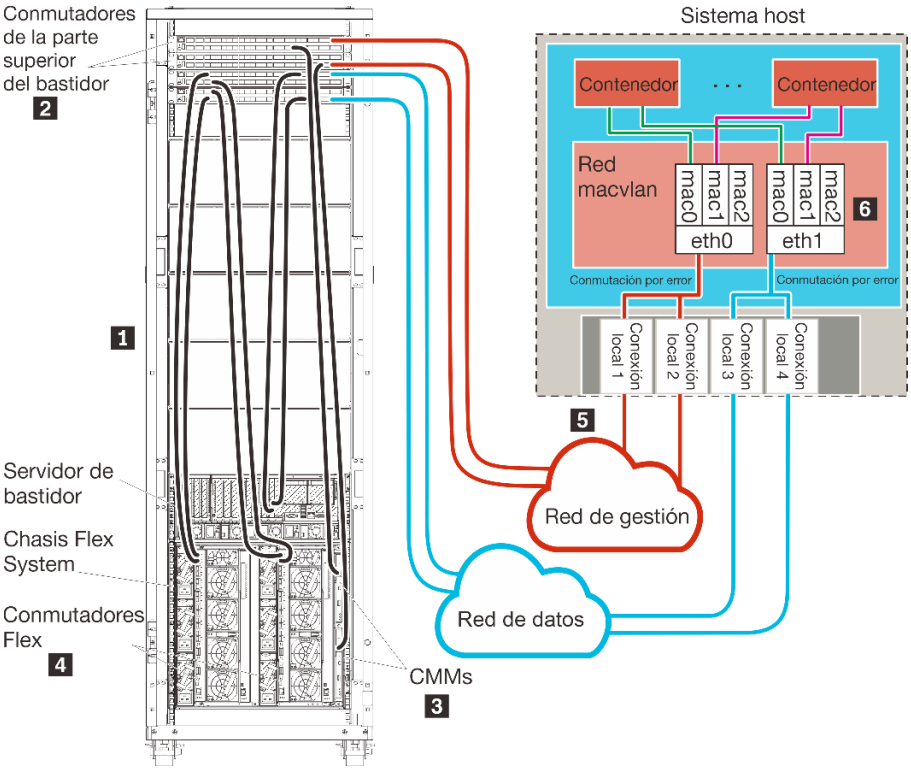


Figura 13. Ejemplo de datos separados físicamente y topología de red de administración para contenedores

Si tiene intención de instalarXClarity Administrator para gestionar chasis y servidores de bastidor existentes que ya se han configurado, continúe con el Paso 5: Instale y configure el host.

Para obtener información adicional sobre cómo planificar esta topología, incluida información sobre los valores de red y la configuración de Eth1 y Eth0, consulte Redes de datos y de gestión separadas físicamente.

Paso 1: Cableado del chasis, los servidores de bastidor y el host Lenovo XClarity Administrator a los conmutadores de la parte superior del bastidor

Conecte el chasis, los servidores de bastidor y el host XClarity Administrator a los conmutadores de la parte superior del bastidor para habilitar las comunicaciones entre los dispositivos y las redes.

Procedimiento

Conecte cada conmutador Flex y CMM de cada chasis, de cada servidor de bastidor y del host XClarity Administrator a los dos conmutadores de la parte superior del bastidor. Puede elegir cualquier puerto de los conmutadores de la parte superior del bastidor.

La figura siguiente es un ejemplo que muestra el cableado del chasis (Conmutadores Flex y CMM), los servidores de bastidor y el host XClarity Administrator a los conmutadores de la parte superior del bastidor.

Nota: Esta figura no representa todas las opciones de cableado que podrían ser necesarias para su entorno. En cambio, esta figura muestra únicamente los requisitos de la opción de cableado para los conmutadores Flex, los CMM y los servidores de bastidor, en la medida en que están relacionados con la configuración de redes de datos y de gestión separadas físicamente.

Consejo: en vez de configurar que se conecten dos conmutadores físicos a cada red para tener redundancia (lo que hace un total de cuatro conmutadores), puede establecer que solo se conecte un conmutador físico a cada red (lo que hace un total de dos conmutadores). En ese caso, cada conmutador estaría conectado a dos redes y se podrían implementar dos VLAN: una para la red de datos y otra para la red de gestión, con el fin de segregar el tráfico de datos.

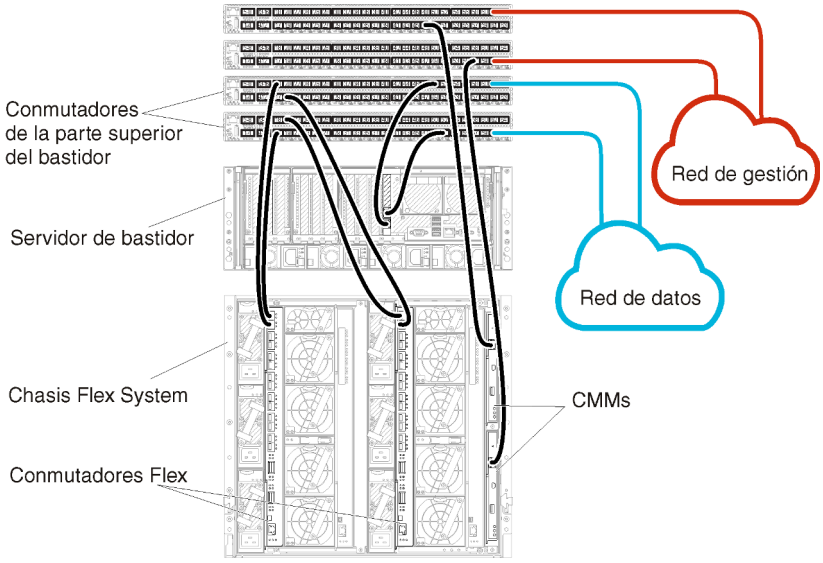


Figura 14. Ejemplo de cableado para redes de datos y de gestión separadas físicamente

Paso 2: Configuración de los conmutadores de la parte superior del bastidor

Configure los conmutadores de la parte superior del bastidor.

Antes de empezar

Además de los requisitos de configuración normales para los conmutadores de la parte superior del bastidor, asegúrese de que estén habilitados todos los puertos apropiados, incluidos los puertos externos a los Conmutadores Flex, a los servidores de bastidor y a la red, así como los puertos internos al CMM, a los servidores de bastidor y a la red.

Procedimiento

Los pasos de configuración pueden variar en función del tipo de los RackSwitch instalados.

Para obtener información acerca de cómo configurar los conmutadores de la parte superior del bastidor de Lenovo, consulte la Documentación en línea de RackSwitch en System x. Si se instala otro conmutador de la parte superior del bastidor, consulte la documentación que se proporciona con ese conmutador.

Paso 3: Configuración de los Chassis Management Module (CMM)

Configure el Chassis Management Module (CMM) principal de su chasis para gestionar todos los dispositivos de este último.

Acerca de esta tarea

Para obtener información detallada acerca de cómo configurar un CMM, consulte Configuración de los componentes del chasis en la documentación en línea de Flex System.

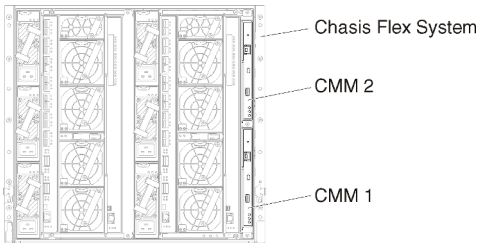
Además, consulte los pasos 4.1 a 4.5 del póster de instrucciones proporcionado con el chasis.

Procedimiento

Lleve a cabo los pasos siguientes para configurar el CMM.

Si se han instalado dos CMM, configure solo el *principal*, lo que sincroniza automáticamente la configuración con el CMM en espera.

Paso 1. Conecte un cable Ethernet desde el CMM de la bahía 1 a una estación de trabajo cliente para crear una conexión directa.



Para conectar el CMM por primera vez, es posible que tenga que cambiar las propiedades del Protocolo de Internet en la estación de trabajo cliente.

Importante: Asegúrese de que la subred de la estación de trabajo cliente sea la misma que la subred del CMM. (La subred del CMM predeterminada es 255.255.255.0.) La dirección IP elegida

para la estación de trabajo cliente debe estar en la misma red que el CMM (por ejemplo, 192.168.70.0 - 192.168.70.24).

Paso 2. Para iniciar la interfaz de gestión del CMM, abra un navegador web en la estación de trabajo cliente y diríjalo a la dirección IP del CMM.

Notas:

- Asegúrese de utilizar una conexión segura y de incluir **https** en la URL (por ejemplo, https://192.168.70.100). Si no incluye https, recibirá un error de página no encontrada.
- Si utiliza la dirección IP predeterminada (192.168.70.100), puede que transcurran unos minutos hasta que la interfaz de gestión del CMM esté disponible. Este retraso se produce porque el CMM trata de obtener una dirección DHCP durante dos minutos antes de volver a la dirección estática predeterminada.

Paso 3. Inicie sesión en la interfaz de gestión del CMM utilizando el Id. de usuario predeterminado `USERID` y la contraseña `PASSWORD`. Una vez que haya iniciado sesión, deberá cambiar la contraseña predeterminada.

Paso 4. Complete el Asistente de configuración inicial del CMM para especificar los detalles de su entorno. El Asistente de configuración inicial incluye las siguientes opciones:

- Consulte el inventario del chasis y el estado.
- Importar la configuración desde un archivo de configuración existente.
- Configure los valores generales del CMM.
- Configure la fecha y hora del CMM.

  Consejo: cuando instale XClarity Administrator, configure XClarity Administrator y todos los chasis gestionados por XClarity Administrator para que utilicen un servidor NTP.
- Configure la información IP del CMM.
- Configure la política de seguridad del CMM.
- Configure el sistema de nombres de dominio (DNS).
- Configure los despachadores de sucesos.

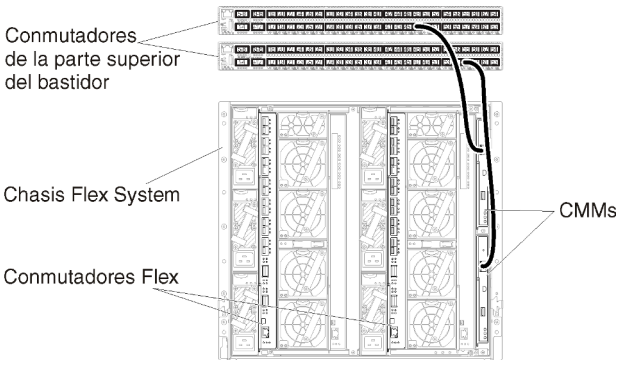
Paso 5. Después de guardar los valores del asistente de configuración y aplicar los cambios, configure las direcciones IP de todos los componentes del chasis.

Consulte el paso 4.6 del poster de instrucciones proporcionado con el chasis.

Nota: Debe restablecer el procesador de gestión del sistema de cada nodo de cálculo y reiniciar los conmutadores Flex para mostrar las nuevas direcciones IP.

Paso 6. Reinicie el CMM mediante la interfaz de gestión del CMM.

Paso 7. Cuando el CMM se esté reiniciando, conecte un cable desde el puerto Ethernet del CMM a su red.



Paso 8. Inicie sesión en la interfaz de gestión del CMM utilizando la nueva dirección IP.

Después de finalizar

También puede configurar el CMM para que admita redundancia. Utilice el sistema de ayuda del CMM para obtener más información acerca de los campos que están disponibles en cada una de las páginas siguientes.

- Configure la conmutación por error para el CMM en caso de que se produzca un fallo de hardware en el CMM principal. En la interfaz de gestión del CMM, haga clic en **Gestión del módulo de gestión → Propiedades → Conmutación por error avanzada**.
- Configure la conmutación por error avanzada como resultado de un problema de red (enlace ascendente). En la interfaz de gestión del CMM, haga clic en **Gestión del módulo de gestión → Red**, haga clic en la pestaña **Ethernet** y, a continuación, haga clic en **Ethernet avanzada**. Como mínimo, asegúrese de seleccionar la casilla **Conmutación por error si hay pérdida de vínculo de red física**.

Paso 4: Configuración de Conmutadores Flex

Configure los Conmutadores Flex en cada chasis.

Antes de empezar

Asegúrese de que están habilitados todos los puertos apropiados, incluidos los puertos externos que van desde el conmutador Flex al conmutador de la parte superior del bastidor y los puertos internos al CMM.

Si los conmutadores Flex se configuran para obtener valores de red dinámicos (dirección IP, máscara de red, puerta de enlace y dirección DNS) a través de DHCP, asegúrese de que dichos conmutadores tienen unos valores coherentes (por ejemplo, compruebe que las direcciones IP se encuentran en la misma red que el CMM).

Importante: Para cada chasis de Flex System, asegúrese de que el tipo de entramado de la tarjeta de expansión de cada servidor en el chasis sea compatible con el tipo de entramado de todos los conmutadores Flex del mismo chasis. Por ejemplo, si instala conmutadores Ethernet en un chasis, todos los servidores de dicho chasis deben tener conectividad Ethernet a través del conector LAN en la placa madre o de una tarjeta de expansión Ethernet. Para obtener más información acerca de cómo configurar los conmutadores Flex, consulte la Configuración de los módulos de E/S en la documentación en línea de Flex System.

Procedimiento

Los pasos de configuración pueden variar en función del tipo de Conmutadores Flex instalado. Para obtener más información acerca de cada uno de los Conmutadores Flex compatibles, consulte Conmutadores de red Flex System en la documentación en línea de Flex System.

Normalmente, tendrá que configurar los conmutadores Flex en las bahías 1 y 2 de conmutadores Flex.

Consejo: la bahía 2 del conmutador Flex es la tercera bahía de los módulos si se mira a la parte posterior del chasis.

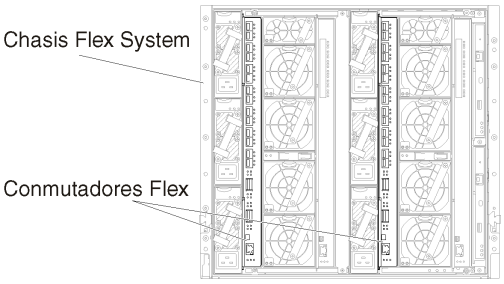


Figura 15. Ubicaciones de los Conmutador Flex en un chasis

Paso 5: Instale y configure el host

Puede instalar Docker en cualquier servidor que cumpla los requisitos para Lenovo XClarity Administrator

Antes de empezar

Puede usar Docker Datacenter para configurar un entorno de alta disponibilidad para contenedores de XClarity Administrator que se ejecutan en Docker Engine. Para obtener más información sobre la alta disponibilidad de Docker Datacenter, consulte Página web de Arquitectura de alta disponibilidad aplicaciones con Docker Datacenter.

Asegúrese de que el host cumple los requisitos previos definidos en Requisitos previos de hardware y software.

Asegúrese de que el sistema host esté en la misma red que los dispositivos que desea gestionar.

Importante: Puede configurar XClarity Administrator en cualquier sistema que cumpla los requisitos de XClarity Administrator, incluido servidor gestionado. Si utiliza un servidor gestionado para el host XClarity Administrator:

- Debe implementar una topología de redes de datos y de gestión separadas virtualmente o bien una topología de una sola red de datos y gestión.
- No puede utilizar XClarity Administrator para aplicar actualizaciones de firmware a ese servidor gestionado. Aunque solo se aplique parte del firmware con la activación inmediata, XClarity Administrator fuerza el reinicio del servidor de destino, lo que reinicia también XClarity Administrator. Cuando se aplica con la activación diferida, solo se aplica determinado firmware cuando se reinicia el host de XClarity Administrator.
- Si utiliza un servidor en un chasis de Flex System, asegúrese de que el servidor esté configurado para encenderse automáticamente. Puede configurar esta opción en la interfaz web del CMM al hacer clic en **Gestión de chasis → Nodos de cálculo** y después al seleccionar el servidor y seleccionar **Encendido automático** para el **Modo de encendido automático**.

Procedimiento

Instale y configure Docker en el host siguiendo las instrucciones proporcionadas con su distribución de Docker.

Paso 6: Instalación y configuración del XClarity Administrator

Instale y configure el contenedor Lenovo XClarity Administrator en el host Docker recién instalado.

Antes de empezar

Asegúrese de que el sistema host cumpla los requisitos de hardware y software (consulte Requisitos previos de hardware y software).

Asegúrese de que estén habilitados todos los puertos apropiados, incluidos los puertos que XClarity Administrator necesita (consulte Disponibilidad de puertos).

Asegúrese de que el sistema host esté en la misma red que los dispositivos que desea gestionar.

Asegúrese de que el SO host y el XClarity Administrator usan el mismo servidor NTP.

XClarity Administrator permite utilizar un nombre personalizado para la red para la gestión de datos, la gestión del hardware y el despliegue del SO (consulte Configuraciones de red). En estos ejemplos del siguiente procedimiento se utiliza eth0.

XClarity Administrator permite utilizar un nombre personalizado para la red para la gestión de datos y de hardware y la red utilizada para el despliegue del SO (consulte Configuraciones de red). Estos ejemplos en el siguiente procedimiento utilizan eth0 y eth1 respectivamente

Asegúrese de que la red macvlan esté cargada en el kernel en el sistema host. Para comprobar si está cargado, utilice el comando **lsmod | grep macvlan**. Para cargar macvlan en el kernel, ejecute el comando **modprobe macvlan**.

Asegúrese de utilizar un nombre y una dirección IP únicos para cada contenedor cuando ejecute varios contenedores de XClarity Administrator en el mismo host.

Si tiene pensado gestionar ThinkServer y otros dispositivos heredados, asegúrese de que Docker esté habilitado para admitir IPv6.

1. Edite el archivo /etc/docker/daemon.json, establezca la clave **ipv6** en verdadero y establezca la clave **fixed-cidr-v6** en la subred IPv6. A continuación, se muestra un archivo daemon de ejemplo.
```
{
   "ipv6": true,
   "fixed-cidr-v6": "2001:db8:1::/64",
   "experimental": true,
   "ip6tables": true
}
```
2. Ejecute el siguiente comando para volver a cargar el archivo de configuración de Docker.
```
systemctl reload docker
```

Nota: XClarity Administrator *no* se ejecuta como un contenedor con privilegios.

Las reglas de firewall no están configuradas en el contenedor XClarity Administrator. Para agregar reglas de firewall para el contenedor en el sistema host, siga estos pasos.

1. Ejecute el siguiente comando para obtener la ID de proceso Docker, identificada por “NSPID”.
```
docker inspect --format='{{ .State.Pid }}' "$CONTAINER_NAME"
```
2. Ejecute el siguiente comando para crear un enlace simbólico.
```
LINKFILE="/var/run/netns/$NSPID"
mkdir -p /var/run/netns
/bin/rm -f "$LINKFILE"
ln -s "/proc/$NSPID/ns/net" "$LINKFILE"
```
3. Ejecute el siguiente comando para configurar las reglas iptables adecuadas.
```
ip netns exec $NSPID iptables -I OUTPUT -j DROP
```
4. Ejecute el siguiente comando para asegurarse de que se eliminen todos los enlaces.
```
/bin/rm -f "$LINKFILE"
```

Procedimiento

Para instalar un contenedor XClarity Administrator utilizando el método Docker compose, realice los pasos siguientes.

Paso 1. Descargue la imagen del dispositivo virtual de XClarity Administrator, el archivo de entorno y el archivo YAML desde el Página web de descarga de XClarity Administrator hasta una estación de trabajo cliente. Inicie sesión en el sitio web y utilice la clave de acceso que se le facilitó para descargar la imagen.

Paso 2. Importe la imagen del contenedor de XClarity Administrator a su host y ejecute el siguiente comando.
```
docker load -i lnvgy_sw_lxca_<ver>_anyos_noarch.tar.gz
```

Paso 3. Edite el archivo `docker_compose.env` y actualice las variables de entorno siguientes.

- **CONTAINER_NAME**. Nombre de contenedor único, que se utiliza para crear volúmenes de docker para cada instancia de XClarity Administrator (por ejemplo, `CONTAINER_NAME=LXCA-203`)
- **ADDRESS**. Dirección IPv4 estática para el contenedor (por ejemplo, `ADDRESS=192.0.2.0`)
- **BACKUP_MOUNT**. (Opcional) Ruta para el recurso compartido remoto que se puede utilizar para almacenar las copias de seguridad de XClarity Administrator. Debe ser `/mnt/backup_share`.
- **FIRMWARE_MOUNT**. (Opcional) Ruta de acceso para la unidad compartida remota que se puede utilizar como repositorio remoto para las actualizaciones de firmware. Debe ser `/mnt/fw_share`.

A continuación hay un archivo de entorno de muestra.
```
CONTAINER_NAME="LXCA-203"
ADDRESS="192.0.2.0"
BACKUP_MOUNT="/mnt/backup_share"
FIRMWARE_MOUNT="/mnt/fw_share"
```

Paso 4. Edite el archivo `docker_compose.yml` y actualice las propiedades siguientes.

- Establezca la propiedad **image** con el nombre del archivo de imagen de instalación utilizado en el paso 2.

  Nota: Puede cambiar el nombre de archivo de la imagen (por ejemplo, a “más reciente”) mediante el comando `docker tag`.
- Si desea utilizar recursos compartidos remotos como repositorio de firmware remoto y almacenar copias de seguridad de XClarity Administrator, establecer el punto de montaje del host para cada unidad compartida remota en la propiedad **volumes**.
- Establezca la propiedad **DNS** en la dirección IP de los servidores DNS.
- El contenedor comparte el grupo de recursos de procesador y de memoria que están disponibles para el host. Opcionalmente, defina los límites del uso de recursos estableciendo las **cpus** y las propiedades de **memoria**.
- Establezca la propiedad **primaria** al nombre de la interfaz de red del sistema host que se va a utilizar como interfaz primaria para la interfaz macvlan en el contenedor. Esta interfaz debe tener acceso directo a la subred asignada al contenedor.
- Establezca la **subred** y la **puerta de enlace** de acuerdo con la topología de su red. Normalmente, la subred y la puerta de enlace son para la red de gestión a la que pertenece ${ADDRESS}.
- Si desea admitir IPv6, establezca la propiedad **enable_ipv6** en verdadero, establezca la propiedad **ipv6_address** en la dirección IPv6 y añada otro conjunto de propiedades de **subred** y **puerta de enlace** de acuerdo con la topología de su red (normalmente para la red de gestión a la que pertenece la dirección IPv6).

A continuación, se muestra un archivo YML de ejemplo, con IPv6 habilitado.

```
version: '3.8'

services:

  lxca:
    image: lenovo/lxca:4.1.0-124
    container_name: ${CONTAINER_NAME}
    tty: true
    stop_grace_period: 60s
    volumes:
      #bind mount example
      - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
      - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
      #docker volume mount
      - data:/opt/lenovo/lxca/data
      - postgresql:/var/lib/postgresql
      - log:/var/log
      - confluent-etc:/etc/confluent
      - confluent-log:/var/log/confluent
      - confluent:/var/lib/confluent
      - propconf:/opt/lenovo/lxca/bin/conf
      - ssh:/etc/ssh
      - xcat:/etc/xcat
    networks:
      lan1:
        ipv4_address: ${ADDRESS}
        ipv6_address: "2001:8003:7d51:2000::2"
      lan2:
        ipv4_address: 192.0.1.3
        ipv6_address: "2001:8003:7d51:2003::2"
    dns:
      - 192.0.40.10
      - 192.0.50.11
    deploy:
      resources:
        limits:
          cpus: "2.0"
          memory: "8g"

volumes:
  data:
    name: ${CONTAINER_NAME}-data
  postgresql:
    name: ${CONTAINER_NAME}-postgresql
  log:
    name: ${CONTAINER_NAME}-log
  confluent-etc:
    name: ${CONTAINER_NAME}-confluent-etc
  confluent-log:
    name: ${CONTAINER_NAME}-confluent-log
  confluent:
    name: ${CONTAINER_NAME}-confluent
  propconf:
    name: ${CONTAINER_NAME}-propconf
  ssh:
    name: ${CONTAINER_NAME}-ssh
  xcat:
    name: ${CONTAINER_NAME}-xcat
```

```
networks:
  lan1:
    name: lan1
    driver: macvlan
    enable_ipv6: true
    driver_opts:
      parent: eno1
    ipam:
      config:
        - subnet: 192.0.0.0/19
          gateway: 192.0.30.1
        - subnet: "2001:8003:7d51:2000::/80"
          gateway: "2001:8003:7d51:2000::1"
  lan2:
    name: lan2
    driver: macvlan
    enable_ipv6: true
    driver_opts:
      parent: virbr0
    ipam:
      config:
        - subnet: 192.0.122.0/24
        - subnet: "2001:8003:7d51:2005::/80"
```

Paso 5. Despliegue la imagen en docker al ejecutar el siguiente comando, donde <*ENV_FILENAME*> es el nombre del archivo de variables ambientales que creó en el paso 2.

```
COMPOSE_HTTP_TIMEOUT=300 docker-compose -p ${CONTAINER_NAME} --env-file <ENV_FILENAME> up -d
```

Después de finalizar

Inicie sesión en XClarity Administrator y realice la configuración correspondiente (consulte el Acceso a la interfaz web de Lenovo XClarity Administrator por primera vez y el Configuración de Lenovo XClarity Administrator).

Datos separados virtualmente y topología de red de gestión

En esta topología, la red de datos y la red de gestión están separadas virtualmente. Los paquetes de la red de datos y de la red de gestión se envían mediante la misma conexión física. El etiquetado de VLAN en todos los paquetes de datos de la red de gestión se utiliza para mantener el tráfico entre las dos redes separadas.

Antes de empezar

Asegúrese de que estén habilitados todos los puertos apropiados, incluidos los puertos que XClarity Administrator necesita (consulte Disponibilidad de puertos).

Asegúrese de que el firmware mínimo necesario esté instalado en cada dispositivo que desee gestionar mediante XClarity Administrator. Encontrará los niveles de firmware mínimos requeridos del Soporte de XClarity Administrator: página web de compatibilidad haciendo clic en la pestaña **Compatibilidad** y, a continuación, pulsando el enlace de los tipos de dispositivo correspondientes.

Asegúrese de que los identificadores de VLAN están configurados para la red de datos y la red de gestión. De forma opcional, habilite el etiquetado VLAN desde el Conmutadores Flex si implementa el etiquetado desde el Conmutadores Flex o habilítelo desde los conmutadores de la parte superior del bastidor si implementa el etiquetado desde estos últimos.

Asegúrese de definir los puertos a los que se conectan los CMM como pertenecientes a la VLAN de gestión.

Importante: configure los componentes de los dispositivos de forma que minimicen los cambios de dirección IP. Plantéese la posibilidad de utilizar direcciones IP estáticas en lugar del protocolo de configuración dinámica de host (DHCP). Si se utiliza DHCP, asegúrese de que los cambios de dirección IP se minimizan.

Acerca de esta tarea

En la figura siguiente se ilustra una forma de configurar el entorno de manera que la red de gestión esté separada de la red virtual. Los números de la figura corresponden a los pasos numerados de las secciones siguientes.

Nota: Esta figura no representa todas las opciones de cableado que podrían ser necesarias para su entorno. En cambio, esta figura muestra únicamente los requisitos de la opción de cableado para los conmutadores Flex, los CMM y los servidores de bastidor, en la medida en que están relacionados con la configuración de redes de datos y de gestión separadas virtualmente.

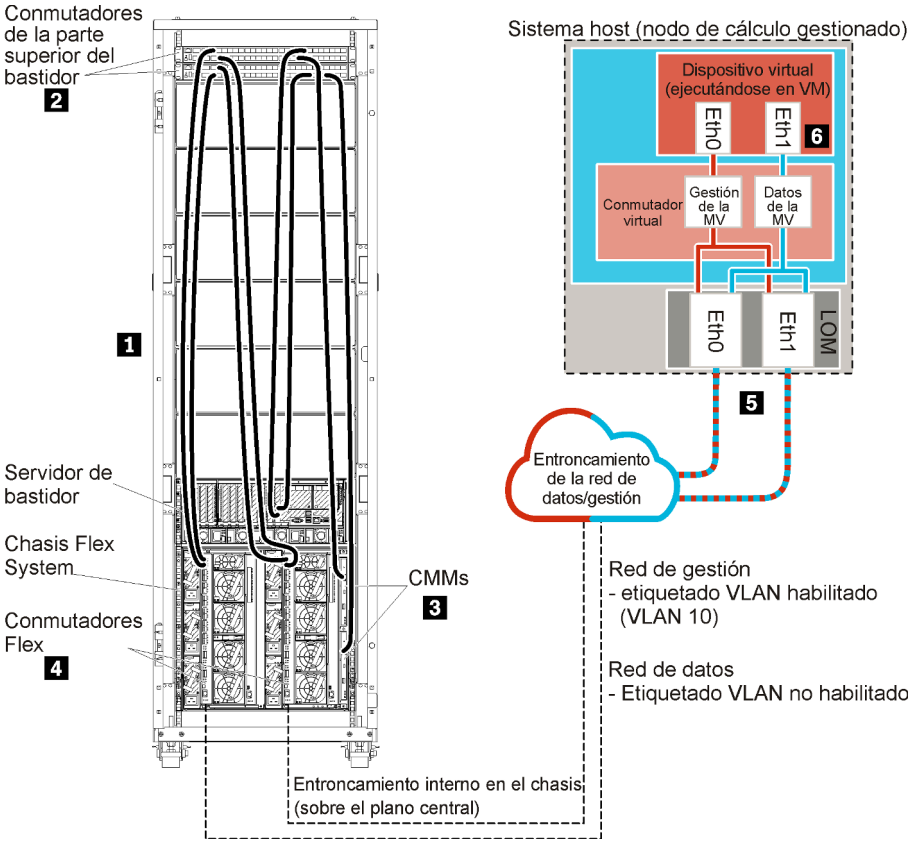


Figura 16. Ejemplo de datos separados virtualmente y topología de red de administración para un dispositivo virtual

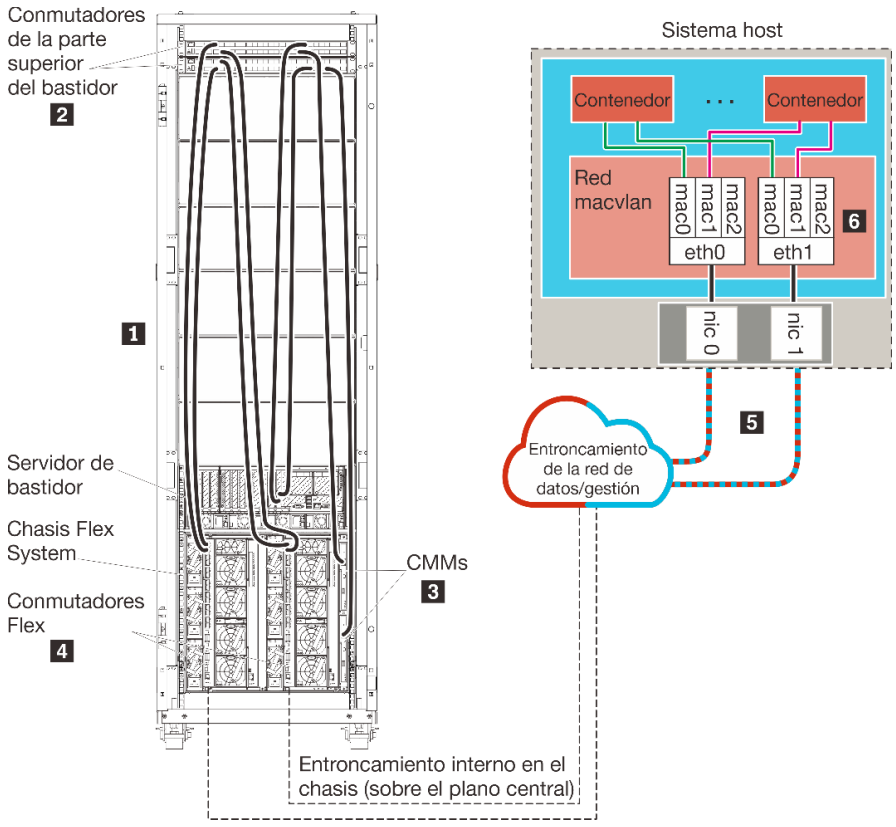


Figura 17. Ejemplo de datos separados virtualmente y topología de red de administración para contenedores

En este caso, XClarity Administrator está instalado en un servidor de un chasis de Flex System gestionado mediante XClarity Administrator.

Importante: Puede configurar XClarity Administrator en cualquier sistema que cumpla los requisitos de XClarity Administrator, incluido servidor gestionado. Si utiliza un servidor gestionado para el host XClarity Administrator:

- Debe implementar una topología de redes de datos y de gestión separadas virtualmente o bien una topología de una sola red de datos y gestión.
- No puede utilizar XClarity Administrator para aplicar actualizaciones de firmware a ese servidor gestionado. Aunque solo se aplique parte del firmware con la activación inmediata, XClarity Administrator fuerza el reinicio del servidor de destino, lo que reinicia también XClarity Administrator. Cuando se aplica con la activación diferida, solo se aplica determinado firmware cuando se reinicia el host de XClarity Administrator.
- Si utiliza un servidor en un chasis de Flex System, asegúrese de que el servidor esté configurado para encenderse automáticamente. Puede configurar esta opción en la interfaz web del CMM al hacer clic en **Gestión de chasis → Nodos de cálculo** y después al seleccionar el servidor y seleccionar **Encendido automático** para el **Modo de encendido automático**.

Además, en este caso, todos los datos se envían a través de las mismas conexiones físicas. La separación entre las redes de gestión y de datos se lleva a cabo mediante el etiquetado VLAN, en virtud del cual se adjuntan etiquetas específicas correspondientes a la red de gestión a los paquetes de datos entrantes, a fin de asegurarse de que se direccionen a las interfaces apropiadas. Las etiquetas se quitan de los paquetes de datos salientes.

El etiquetado VLAN puede habilitarse en uno de los dispositivos siguientes:

- **Conmutadores de la parte superior del bastidor**. Las etiquetas VLAN correspondientes a la red de gestión se agregan a los paquetes a medida que entran en el conmutador de la parte superior del bastidor y después pasan a través de los Conmutadores Flex hasta los servidores en el chasis de Flex System. En la ruta de regreso, las etiquetas VLAN se quitan a medida que se envían desde el conmutador de la parte superior del bastidor a los controladores de gestión.
- **Conmutadores Flex**. Las etiquetas VLAN correspondientes a la red de gestión se agregan a los paquetes a medida que entran en el Conmutadores Flex y se pasan a los servidores en un chasis de Flex System. En la ruta de regreso, los servidores agregan etiquetas VLAN y estas se pasan a los Conmutadores Flex, que las quitan antes de efectuar el reenvío a los controladores de gestión.

La decisión de implementar el etiquetado VLAN o no dependerá de las necesidades y la complejidad de su entorno.

Si tiene intención de instalarXClarity Administrator para gestionar chasis y servidores de bastidor existentes que ya se han configurado, continúe con el Paso 5: Instale y configure el host.

Para obtener información adicional sobre cómo planificar esta topología, incluida información sobre los valores de red y la configuración de Eth1 y Eth0, consulte Redes de datos y de gestión separadas virtualmente.

Paso 1: Cableado del chasis y los servidores de bastidor a los conmutadores de la parte superior del bastidor

Conecte el chasis y los servidores de bastidor al mismo conmutador de la parte superior del bastidor para habilitar las comunicaciones entre los dispositivos.

Procedimiento

Conecte cada conmutador Flex y CMM de cada chasis y cada servidor de bastidor a los dos conmutadores de la parte superior del bastidor. Puede elegir cualquier puerto del conmutador de la parte superior del bastidor.

La figura siguiente es un ejemplo que muestra el cableado del chasis (conmutadores Flex y CMM) y los servidores de bastidor a los conmutadores de la parte superior del bastidor cuando Lenovo XClarity Administrator está instalado en un servidor de un chasis que se gestionará mediante XClarity Administrator.

Nota: Esta figura no representa todas las opciones de cableado que podrían ser necesarias para su entorno. En cambio, esta figura muestra únicamente los requisitos de la opción de cableado para los conmutadores Flex, los CMM y los servidores de bastidor, en la medida en que están relacionados con la configuración de redes de datos y de gestión separadas virtualmente.

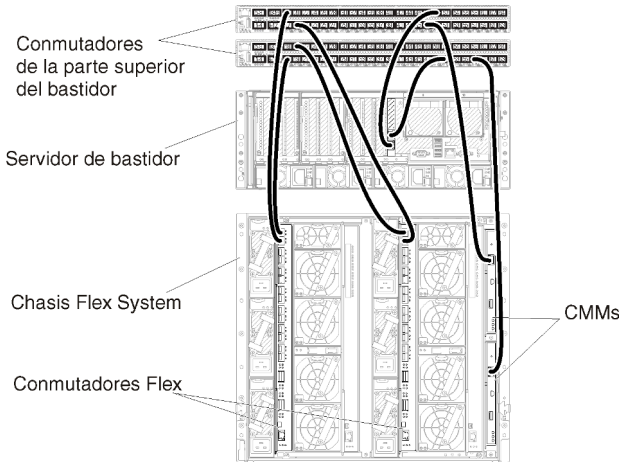


Figura 18. Ejemplo de cableado para redes de datos y de gestión separadas virtualmente

Paso 2: Configuración de los conmutadores de la parte superior del bastidor

Configure los conmutadores de la parte superior del bastidor.

Antes de empezar

Además de los requisitos de configuración normales para los conmutadores de la parte superior del bastidor, asegúrese de que estén habilitados todos los puertos apropiados, incluidos los puertos externos a los Conmutadores Flex, a los servidores de bastidor y a la red, así como los puertos internos al CMM, a los servidores de bastidor y a la red.

Puede implementar el etiquetado VLAN en los conmutadores Flex o conmutadores de la parte superior del bastidor, según las necesidades y la complejidad de su entorno. Si implementa el etiquetado en los conmutadores de la parte superior del bastidor, debe habilitar el etiquetado VLAN desde ellos.

Asegúrese de que los identificadores de VLAN están configurados para las redes de gestión y de datos.

Procedimiento

Los pasos de configuración pueden variar en función del tipo de los RackSwitch instalados.

En la figura siguiente se muestra un ejemplo de un caso de etiquetado VLAN implementado en los conmutadores de la parte superior del bastidor que solamente se ha habilitado en la red de gestión. La VLAN de gestión se ha configurado como VLAN 10.

En este caso, es preciso definir los puertos a los que se conectan los CMM como pertenecientes a la VLAN de gestión.

Nota: También se puede habilitar el etiquetado VLAN en la red de datos, para configurar una VLAN de datos.

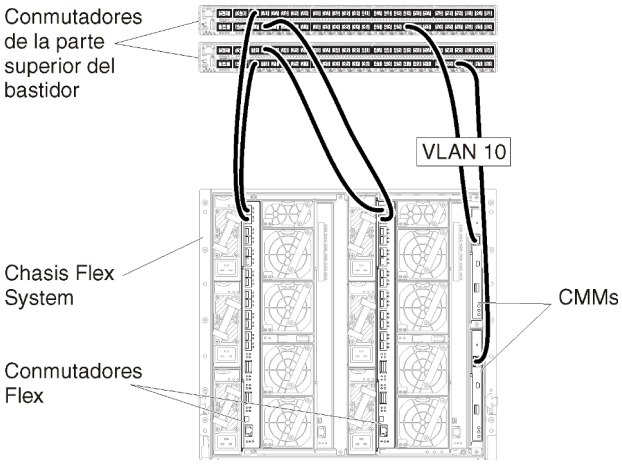


Figura 19. Ejemplo de configuración para Conmutadores Flex en redes de datos y gestión separadas virtualmente (VMware ESXi) en las que el etiquetado VLAN está habilitado solo en la red de gestión

Para obtener información acerca de cómo configurar los conmutadores de la parte superior del bastidor de Lenovo, consulte la Documentación en línea de RackSwitch en System x. Si se instala otro conmutador de la parte superior del bastidor, consulte la documentación que se proporciona con ese conmutador.

Paso 3: Configuración de los Chassis Management Module (CMM)

Configure el Chassis Management Module (CMM) principal de su chasis para gestionar todos los dispositivos de este último.

Acerca de esta tarea

Para obtener información detallada acerca de cómo configurar un CMM, consulte Configuración de los componentes del chasis en la documentación en línea de Flex System.

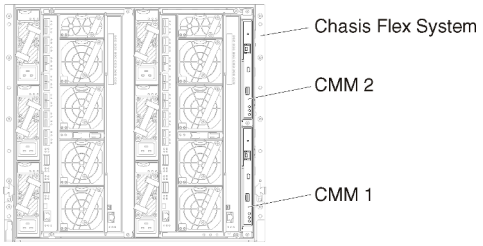
Además, consulte los pasos 4.1 a 4.5 del póster de instrucciones proporcionado con el chasis.

Procedimiento

Lleve a cabo los pasos siguientes para configurar el CMM.

Si se han instalado dos CMM, configure solo el *principal*, lo que sincroniza automáticamente la configuración con el CMM en espera.

Paso 1. Conecte un cable Ethernet desde el CMM de la bahía 1 a una estación de trabajo cliente para crear una conexión directa.



Para conectar el CMM por primera vez, es posible que tenga que cambiar las propiedades del Protocolo de Internet en la estación de trabajo cliente.

Importante: Asegúrese de que la subred de la estación de trabajo cliente sea la misma que la subred del CMM. (La subred del CMM predeterminada es 255.255.255.0.) La dirección IP elegida para la estación de trabajo cliente debe estar en la misma red que el CMM (por ejemplo, 192.168.70.0 - 192.168.70.24).

Paso 2. Para iniciar la interfaz de gestión del CMM, abra un navegador web en la estación de trabajo cliente y diríjalo a la dirección IP del CMM.

Notas:

- Asegúrese de utilizar una conexión segura y de incluir **https** en la URL (por ejemplo, https://192.168.70.100). Si no incluye https, recibirá un error de página no encontrada.
- Si utiliza la dirección IP predeterminada (192.168.70.100), puede que transcurran unos minutos hasta que la interfaz de gestión del CMM esté disponible. Este retraso se produce porque el CMM trata de obtener una dirección DHCP durante dos minutos antes de volver a la dirección estática predeterminada.

Paso 3. Inicie sesión en la interfaz de gestión del CMM utilizando el Id. de usuario predeterminado `USERID` y la contraseña `PASSWORD`. Una vez que haya iniciado sesión, deberá cambiar la contraseña predeterminada.

Paso 4. Complete el Asistente de configuración inicial del CMM para especificar los detalles de su entorno. El Asistente de configuración inicial incluye las siguientes opciones:

- Consulte el inventario del chasis y el estado.
- Importar la configuración desde un archivo de configuración existente.
- Configure los valores generales del CMM.
- Configure la fecha y hora del CMM.

  Consejo: cuando instale XClarity Administrator, configure XClarity Administrator y todos los chasis gestionados por XClarity Administrator para que utilicen un servidor NTP.
- Configure la información IP del CMM.
- Configure la política de seguridad del CMM.
- Configure el sistema de nombres de dominio (DNS).
- Configure los despachadores de sucesos.

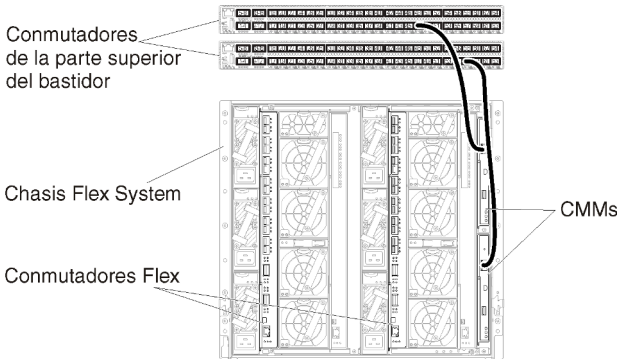
Paso 5. Después de guardar los valores del asistente de configuración y aplicar los cambios, configure las direcciones IP de todos los componentes del chasis.

Consulte el paso 4.6 del poster de instrucciones proporcionado con el chasis.

Nota: Debe restablecer el procesador de gestión del sistema de cada nodo de cálculo y reiniciar los conmutadores Flex para mostrar las nuevas direcciones IP.

Paso 6. Reinicie el CMM mediante la interfaz de gestión del CMM.

Paso 7. Cuando el CMM se esté reiniciando, conecte un cable desde el puerto Ethernet del CMM a su red.



Paso 8. Inicie sesión en la interfaz de gestión del CMM utilizando la nueva dirección IP.

Después de finalizar

También puede configurar el CMM para que admita redundancia. Utilice el sistema de ayuda del CMM para obtener más información acerca de los campos que están disponibles en cada una de las páginas siguientes.

- Configure la conmutación por error para el CMM en caso de que se produzca un fallo de hardware en el CMM principal. En la interfaz de gestión del CMM, haga clic en **Gestión del módulo de gestión → Propiedades → Conmutación por error avanzada**.
- Configure la conmutación por error avanzada como resultado de un problema de red (enlace ascendente). En la interfaz de gestión del CMM, haga clic en **Gestión del módulo de gestión → Red**, haga clic en la pestaña **Ethernet** y, a continuación, haga clic en **Ethernet avanzada**. Como mínimo, asegúrese de seleccionar la casilla **Conmutación por error si hay pérdida de vínculo de red física**.

Paso 4: Configuración de Conmutadores Flex

Configure los Conmutadores Flex en cada chasis.

Antes de empezar

Asegúrese de que están habilitados todos los puertos apropiados, incluidos los puertos externos que van desde el conmutador Flex al conmutador de la parte superior del bastidor y los puertos internos al CMM.

Puede implementar el etiquetado VLAN en los conmutadores Flex o conmutadores de la parte superior del bastidor, según las necesidades y la complejidad de su entorno. Si implementa el etiquetado en los conmutadores Flex, debe habilitar el etiquetado VLAN desde ellos.

Asegúrese de que los identificadores de VLAN están configurados para las redes de gestión y de datos.

Importante: Para cada chasis de Flex System, asegúrese de que el tipo de entramado de la tarjeta de expansión de cada servidor en el chasis sea compatible con el tipo de entramado de todos los conmutadores Flex del mismo chasis. Por ejemplo, si instala conmutadores Ethernet en un chasis, todos los servidores de dicho chasis deben tener conectividad Ethernet a través del conector LAN en la placa madre o de una tarjeta de expansión Ethernet. Para obtener más información acerca de cómo configurar los conmutadores Flex, consulte la Configuración de los módulos de E/S en la documentación en línea de Flex System.

Procedimiento

Los pasos de configuración pueden variar en función del tipo de Conmutadores Flex instalado. Para obtener más información acerca de cada uno de los Conmutadores Flex compatibles, consulte Conmutadores de red Flex System en la documentación en línea de Flex System.

En la figura siguiente se muestra un ejemplo de un caso de etiquetado VLAN implementado en los conmutadores Flex que solamente se ha habilitado en la red de gestión. La VLAN de gestión se ha configurado como VLAN 10.

Nota: Puede configurar una VLAN de datos habilitando el etiquetado VLAN en la red de datos.

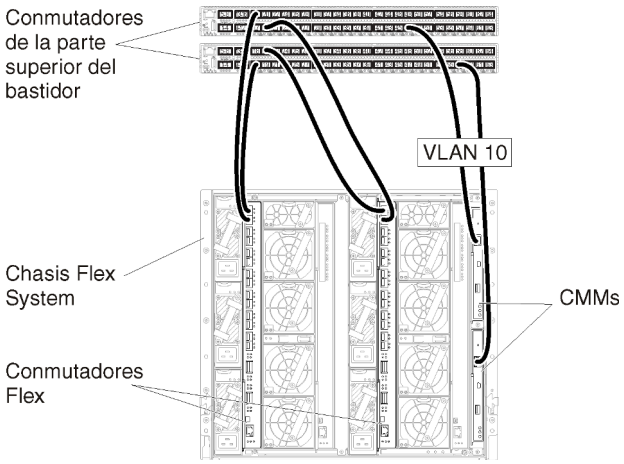


Figura 20. Ejemplo de configuración para Conmutadores Flex en redes de datos y gestión separadas virtualmente (VMware ESXi) en las que el etiquetado VLAN está habilitado solo en la red de gestión

Lleve a cabo los pasos siguientes para configurar los conmutadores Flex para este caso:

Paso 1. Configure los conmutadores Flex en la bahía 1 de conmutador Flex:

a. Defina la VLAN de gestión (en el ejemplo hemos elegido la VLAN 10) que va a contener el puerto externo desde donde el cable se dirige al conmutador de gestión de la parte superior del bastidor (Ext1).

b. Defina un puerto interno que será parte de la VLAN 10 (VLAN de gestión). Asegúrese de que el entroncamiento de VLAN esté habilitado en ese puerto.

Paso 2. Configure los conmutadores Flex en la bahía 2 de conmutador Flex:

Consejo: la bahía 2 del conmutador Flex es en realidad la tercera bahía de los módulos si se mira a la parte posterior del chasis:

a. Defina la VLAN de gestión (en el ejemplo hemos elegido la VLAN 10) que va a contener el puerto externo desde donde el cable se dirige al conmutador de gestión de la parte superior del bastidor.

b. Defina un puerto interno que será parte de la VLAN 10 (VLAN de gestión). Asegúrese de que el entroncamiento de VLAN esté habilitado en ese puerto.

Paso 5: Instale y configure el host

Puede instalar Docker en cualquier sistema que cumpla los requisitos para Lenovo XClarity Administrator.

Antes de empezar

Puede usar Docker Datacenter para configurar un entorno de alta disponibilidad para contenedores de XClarity Administrator que se ejecutan en Docker Engine. Para obtener más información sobre la alta disponibilidad de Docker Datacenter, consulte Página web de Arquitectura de alta disponibilidad aplicaciones con Docker Datacenter.

Asegúrese de que el host cumple los requisitos previos definidos en Requisitos previos de hardware y software.

Asegúrese de que el sistema host esté en la misma red que los dispositivos que desea gestionar.

Importante: Puede configurar XClarity Administrator en cualquier sistema que cumpla los requisitos de XClarity Administrator, incluido servidor gestionado. Si utiliza un servidor gestionado para el host XClarity Administrator:

- Debe implementar una topología de redes de datos y de gestión separadas virtualmente o bien una topología de una sola red de datos y gestión.
- No puede utilizar XClarity Administrator para aplicar actualizaciones de firmware a ese servidor gestionado. Aunque solo se aplique parte del firmware con la activación inmediata, XClarity Administrator fuerza el reinicio del servidor de destino, lo que reinicia también XClarity Administrator. Cuando se aplica con la activación diferida, solo se aplica determinado firmware cuando se reinicia el host de XClarity Administrator.
- Si utiliza un servidor en un chasis de Flex System, asegúrese de que el servidor esté configurado para encenderse automáticamente. Puede configurar esta opción en la interfaz web del CMM al hacer clic en **Gestión de chasis → Nodos de cálculo** y después al seleccionar el servidor y seleccionar **Encendido automático** para el **Modo de encendido automático**.

Procedimiento

Instale y configure Docker en el host siguiendo las instrucciones proporcionadas con su distribución de Docker.

Paso 6: Instalación y configuración del XClarity Administrator

Instale y configure el contenedor Lenovo XClarity Administrator en el host Docker recién instalado.

Antes de empezar

Asegúrese de que el sistema host cumpla los requisitos de hardware y software (consulte Requisitos previos de hardware y software).

Asegúrese de que estén habilitados todos los puertos apropiados, incluidos los puertos que XClarity Administrator necesita (consulte Disponibilidad de puertos).

Asegúrese de que el sistema host esté en la misma red que los dispositivos que desea gestionar.

Asegúrese de que el SO host y el XClarity Administrator usan el mismo servidor NTP.

XClarity Administrator permite utilizar un nombre personalizado para la red para la gestión de datos, la gestión del hardware y el despliegue del SO (consulte Configuraciones de red). En estos ejemplos del siguiente procedimiento se utiliza eth0.

XClarity Administrator permite utilizar un nombre personalizado para la red para la gestión de datos y de hardware y la red utilizada para el despliegue del SO (consulte Configuraciones de red). Estos ejemplos en el siguiente procedimiento utilizan eth0 y eth1 respectivamente.

Asegúrese de que la red macvlan esté cargada en el kernel en el sistema host. Para comprobar si está cargado, utilice el comando **lsmod | grep macvlan**. Para cargar macvlan en el kernel, ejecute el comando **modprobe macvlan**.

Asegúrese de utilizar un nombre y una dirección IP únicos para cada contenedor cuando ejecute varios contenedores de XClarity Administrator en el mismo host.

Si tiene pensado gestionar ThinkServer y otros dispositivos heredados, asegúrese de que Docker esté habilitado para admitir IPv6.

1. Edite el archivo /etc/docker/daemon.json, establezca la clave **ipv6** en verdadero y establezca la clave **fixed-cidr-v6** en la subred IPv6. A continuación, se muestra un archivo daemon de ejemplo.
```
{
   "ipv6": true,
   "fixed-cidr-v6": "2001:db8:1::/64",
   "experimental": true,
   "ip6tables": true
}
```
2. Ejecute el siguiente comando para volver a cargar el archivo de configuración de Docker.
```
systemctl reload docker
```

Nota: XClarity Administrator *no* se ejecuta como un contenedor con privilegios.

Las reglas de firewall no están configuradas en el contenedor XClarity Administrator. Para agregar reglas de firewall para el contenedor en el sistema host, siga estos pasos.

1. Ejecute el siguiente comando para obtener la ID de proceso Docker, identificada por “NSPID”.
```
docker inspect --format='{{ .State.Pid }}' "$CONTAINER_NAME"
```
2. Ejecute el siguiente comando para crear un enlace simbólico.
```
LINKFILE="/var/run/netns/$NSPID"
mkdir -p /var/run/netns
/bin/rm -f "$LINKFILE"
ln -s "/proc/$NSPID/ns/net" "$LINKFILE"
```
3. Ejecute el siguiente comando para configurar las reglas iptables adecuadas.
```
ip netns exec $NSPID iptables -I OUTPUT -j DROP
```
4. Ejecute el siguiente comando para asegurarse de que se eliminen todos los enlaces.
```
/bin/rm -f "$LINKFILE"
```

Procedimiento

Para instalar un contenedor XClarity Administrator utilizando el método Docker compose, realice los pasos siguientes.

Paso 1. Descargue la imagen del dispositivo virtual de XClarity Administrator, el archivo de entorno y el archivo YAML desde el Página web de descarga de XClarity Administrator hasta una estación de trabajo cliente. Inicie sesión en el sitio web y utilice la clave de acceso que se le facilitó para descargar la imagen.

Paso 2. Importe la imagen del contenedor de XClarity Administrator a su host y ejecute el siguiente comando.
```
docker load -i lnvgy_sw_lxca_<ver>_anyos_noarch.tar.gz
```

Paso 3. Edite el archivo `docker_compose.env` y actualice las variables de entorno siguientes.

- **CONTAINER_NAME**. Nombre de contenedor único, que se utiliza para crear volúmenes de docker para cada instancia de XClarity Administrator (por ejemplo, `CONTAINER_NAME=LXCA-203`)
- **ADDRESS**. Dirección IPv4 estática para el contenedor (por ejemplo, `ADDRESS=192.0.2.0`)
- **BACKUP_MOUNT**. (Opcional) Ruta para el recurso compartido remoto que se puede utilizar para almacenar las copias de seguridad de XClarity Administrator. Debe ser `/mnt/backup_share`.
- **FIRMWARE_MOUNT**. (Opcional) Ruta de acceso para la unidad compartida remota que se puede utilizar como repositorio remoto para las actualizaciones de firmware. Debe ser `/mnt/fw_share`.

A continuación hay un archivo de entorno de muestra.

```
CONTAINER_NAME="LXCA-203"
ADDRESS="192.0.2.0"
BACKUP_MOUNT="/mnt/backup_share"
FIRMWARE_MOUNT="/mnt/fw_share"
```

Paso 4. Edite el archivo `docker_compose.yml` y actualice las propiedades siguientes.

- Establezca la propiedad **image** con el nombre del archivo de imagen de instalación utilizado en el paso 2.

  Nota: Puede cambiar el nombre de archivo de la imagen (por ejemplo, a “más reciente”) mediante el comando `docker tag`.
- Si desea utilizar recursos compartidos remotos como repositorio de firmware remoto y almacenar copias de seguridad de XClarity Administrator, establecer el punto de montaje del host para cada unidad compartida remota en la propiedad **volumes**.
- Establezca la propiedad **DNS** en la dirección IP de los servidores DNS.
- El contenedor comparte el grupo de recursos de procesador y de memoria que están disponibles para el host. Opcionalmente, defina los límites del uso de recursos estableciendo las **cpus** y las propiedades de **memoria**.
- Establezca la propiedad **primaria** al nombre de la interfaz de red del sistema host que se va a utilizar como interfaz primaria para la interfaz macvlan en el contenedor. Esta interfaz debe tener acceso directo a la subred asignada al contenedor.
- Establezca la **subred** y la **puerta de enlace** de acuerdo con la topología de su red. Normalmente, la subred y la puerta de enlace son para la red de gestión a la que pertenece ${ADDRESS}.
- Si desea admitir IPv6, establezca la propiedad **enable_ipv6** en verdadero, establezca la propiedad **ipv6_address** en la dirección IPv6 y añada otro conjunto de propiedades de **subred** y **puerta de enlace** de acuerdo con la topología de su red (normalmente para la red de gestión a la que pertenece la dirección IPv6).

A continuación, se muestra un archivo YML de ejemplo, con IPv6 habilitado.

```
version: '3.8'

services:

  lxca:
    image: lenovo/lxca:4.1.0-124
    container_name: ${CONTAINER_NAME}
    tty: true
    stop_grace_period: 60s
    volumes:
      #bind mount example
      - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
      - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
      #docker volume mount
      - data:/opt/lenovo/lxca/data
      - postgresql:/var/lib/postgresql
      - log:/var/log
      - confluent-etc:/etc/confluent
      - confluent-log:/var/log/confluent
      - confluent:/var/lib/confluent
      - propconf:/opt/lenovo/lxca/bin/conf
      - ssh:/etc/ssh
      - xcat:/etc/xcat
    networks:
```

```
      lan1:
        ipv4_address: ${ADDRESS}
        ipv6_address: "2001:8003:7d51:2000::2"
      lan2:
        ipv4_address: 192.0.1.3
        ipv6_address: "2001:8003:7d51:2003::2"
    dns:
      - 192.0.40.10
      - 192.0.50.11
    deploy:
      resources:
        limits:
          cpus: "2.0"
          memory: "8g"

volumes:
  data:
    name: ${CONTAINER_NAME}-data
  postgresql:
    name: ${CONTAINER_NAME}-postgresql
  log:
    name: ${CONTAINER_NAME}-log
  confluent-etc:
    name: ${CONTAINER_NAME}-confluent-etc
  confluent-log:
    name: ${CONTAINER_NAME}-confluent-log
  confluent:
    name: ${CONTAINER_NAME}-confluent
  propconf:
    name: ${CONTAINER_NAME}-propconf
  ssh:
    name: ${CONTAINER_NAME}-ssh
  xcat:
    name: ${CONTAINER_NAME}-xcat

networks:
  lan1:
    name: lan1
    driver: macvlan
    enable_ipv6: true
    driver_opts:
      parent: eno1
    ipam:
      config:
        - subnet: 192.0.0.0/19
          gateway: 192.0.30.1
        - subnet: "2001:8003:7d51:2000::/80"
          gateway: "2001:8003:7d51:2000::1"
  lan2:
    name: lan2
    driver: macvlan
    enable_ipv6: true
    driver_opts:
      parent: virbr0
    ipam:
      config:
        - subnet: 192.0.122.0/24
          gateway: 192.0.122.1
        - subnet: "2001:8003:7d51:2003::/80"
          gateway: "2001:8003:7d51:2003::1"
```

Paso 5. Despliegue la imagen en docker al ejecutar el siguiente comando, donde <*ENV_FILENAME*> es el nombre del archivo de variables ambientales que creó en el paso 2.

```
COMPOSE_HTTP_TIMEOUT=300 docker-compose -p ${CONTAINER_NAME} --env-file <ENV_FILENAME> up -d
```

Después de finalizar

Inicie sesión en XClarity Administrator y realice la configuración correspondiente (consulte el Acceso a la interfaz web de Lenovo XClarity Administrator por primera vez y el Configuración de Lenovo XClarity Administrator).

Topología de red de solo gestión

En esta topología, Lenovo XClarity Administrator solamente tiene la red de gestión. No tiene la red de datos.

Antes de empezar

Asegúrese de que todos los puertos correctos estén habilitados, incluidos:
- Los puertos requeridos por XClarity Administrator (consulte Disponibilidad de puertos)
- Los puertos externos de la red
- Los puertos internos del CMM

Asegúrese de que el firmware mínimo necesario esté instalado en cada dispositivo que desee gestionar mediante XClarity Administrator. Encontrará los niveles de firmware mínimos requeridos del Soporte de XClarity Administrator: página web de compatibilidad haciendo clic en la pestaña **Compatibilidad** y, a continuación, pulsando el enlace de los tipos de dispositivo correspondientes.

Importante: configure los componentes de los dispositivos de forma que minimicen los cambios de dirección IP. Plantéese la posibilidad de utilizar direcciones IP estáticas en lugar del protocolo de configuración dinámica de host (DHCP). Si se utiliza DHCP, asegúrese de que los cambios de dirección IP se minimizan.

Acerca de esta tarea

En la figura siguiente se muestra una manera de configurar el entorno si Lenovo XClarity Administrator tiene solamente la red de gestión (y no la red de datos). Los números de la figura corresponden a los pasos numerados de las secciones siguientes.

Nota: Esta figura no representa todas las opciones de cableado que podrían ser necesarias para su entorno. En cambio, esta figura muestra únicamente los requisitos de la opción de cableado para los conmutadores Flex, los CMM y los servidores de bastidor, en la medida en que están relacionados con la configuración de una red de solo gestión.

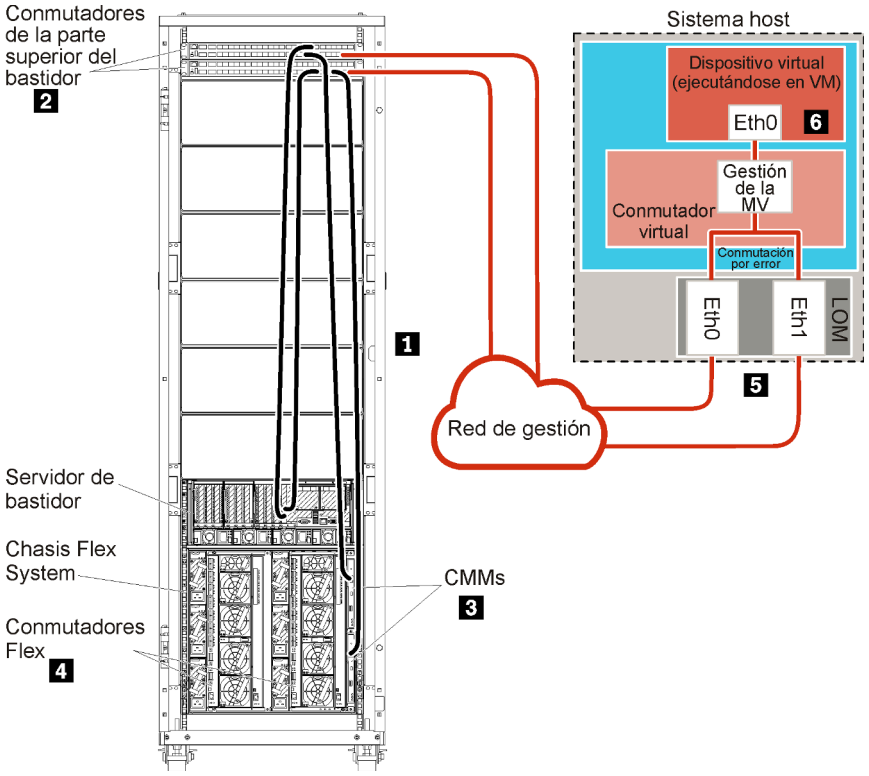


Figura 21. Ejemplo de topología de red de solo gestión para un dispositivo virtual

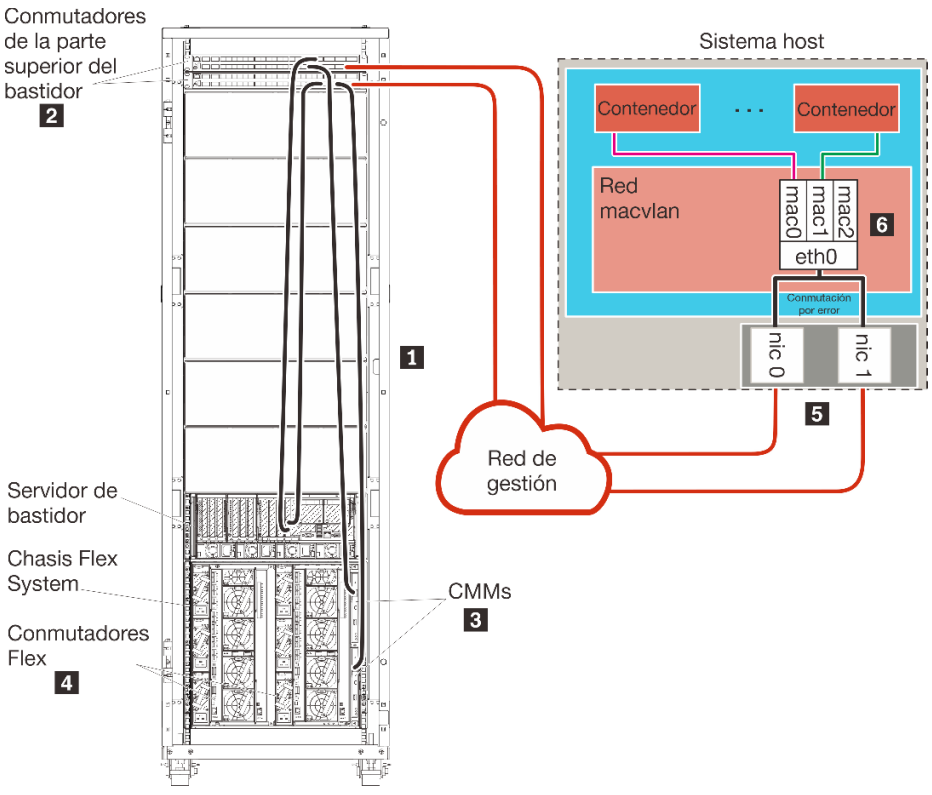


Figura 22. Ejemplo de topología de red de solo gestión para contenedores

Si tiene intención de instalarXClarity Administrator para gestionar chasis y servidores de bastidor existentes que ya se han configurado, continúe con el Paso 5: Instale y configure el host.

Para obtener información adicional sobre cómo planificar esta topología, incluida información sobre los valores de red y la configuración de Eth1 y Eth0, consulte Red de solo gestión.

Paso 1: Cableado del chasis, los servidores de bastidor y el host Lenovo XClarity Administrator a los conmutadores de la parte superior del bastidor

Conecte el chasis, los servidores de bastidor y el host XClarity Administrator a los conmutadores de la parte superior del bastidor para habilitar las comunicaciones entre los dispositivos y la red.

Procedimiento

Conecte cada conmutador Flex y CMM de cada chasis, de cada servidor de bastidor y del host XClarity Administrator a los dos conmutadores de la parte superior del bastidor. Puede elegir cualquier puerto de los conmutadores de la parte superior del bastidor.

La figura siguiente es un ejemplo que muestra el cableado del chasis (conmutadores Flex y CMM), los servidores de bastidor y el host XClarity Administrator a los conmutadores de la parte superior del bastidor.

Nota: Esta figura no representa todas las opciones de cableado que podrían ser necesarias para su entorno. En cambio, esta figura muestra únicamente los requisitos de la opción de cableado para los conmutadores Flex, los CMM y los servidores de bastidor, en la medida en que están relacionados con la configuración de una red de solo gestión.

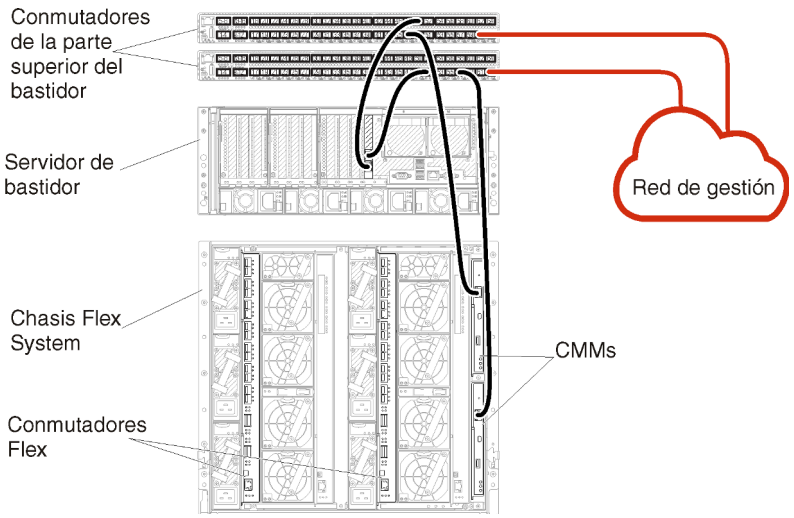


Figura 23. Ejemplo de cableado para una red de solo gestión

Paso 2: Configuración de los conmutadores de la parte superior del bastidor

Configure los conmutadores de la parte superior del bastidor.

Antes de empezar

Además de los requisitos de configuración normales para los conmutadores de la parte superior del bastidor, asegúrese de que estén habilitados todos los puertos apropiados, incluidos los puertos externos a los Conmutadores Flex, a los servidores de bastidor y a la red, así como los puertos internos al CMM, a los servidores de bastidor y a la red.

Procedimiento

Los pasos de configuración pueden variar en función del tipo de los RackSwitch instalados.

Para obtener información acerca de cómo configurar los conmutadores de la parte superior del bastidor de Lenovo, consulte la Documentación en línea de RackSwitch en System x. Si se instala otro conmutador de la parte superior del bastidor, consulte la documentación que se proporciona con ese conmutador.

Paso 3: Configuración de los Chassis Management Module (CMM)

Configure el Chassis Management Module (CMM) principal de su chasis para gestionar todos los dispositivos de este último.

Acerca de esta tarea

Para obtener información detallada acerca de cómo configurar un CMM, consulte Configuración de los componentes del chasis en la documentación en línea de Flex System.

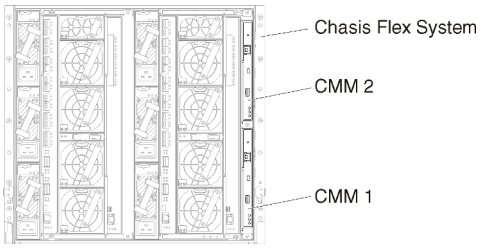
Además, consulte los pasos 4.1 a 4.5 del póster de instrucciones proporcionado con el chasis.

Procedimiento

Lleve a cabo los pasos siguientes para configurar el CMM.

Si se han instalado dos CMM, configure solo el *principal*, lo que sincroniza automáticamente la configuración con el CMM en espera.

Paso 1. Conecte un cable Ethernet desde el CMM de la bahía 1 a una estación de trabajo cliente para crear una conexión directa.



Para conectar el CMM por primera vez, es posible que tenga que cambiar las propiedades del Protocolo de Internet en la estación de trabajo cliente.

Importante: Asegúrese de que la subred de la estación de trabajo cliente sea la misma que la subred del CMM. (La subred del CMM predeterminada es 255.255.255.0.) La dirección IP elegida para la estación de trabajo cliente debe estar en la misma red que el CMM (por ejemplo, 192.168.70.0 - 192.168.70.24).

Paso 2. Para iniciar la interfaz de gestión del CMM, abra un navegador web en la estación de trabajo cliente y diríjalo a la dirección IP del CMM.

Notas:

- Asegúrese de utilizar una conexión segura y de incluir **https** en la URL (por ejemplo, https://192.168.70.100). Si no incluye https, recibirá un error de página no encontrada.
- Si utiliza la dirección IP predeterminada (192.168.70.100), puede que transcurran unos minutos hasta que la interfaz de gestión del CMM esté disponible. Este retraso se produce porque el CMM trata de obtener una dirección DHCP durante dos minutos antes de volver a la dirección estática predeterminada.

Paso 3. Inicie sesión en la interfaz de gestión del CMM utilizando el Id. de usuario predeterminado `USERID` y la contraseña `PASSWORD`. Una vez que haya iniciado sesión, deberá cambiar la contraseña predeterminada.

Paso 4. Complete el Asistente de configuración inicial del CMM para especificar los detalles de su entorno. El Asistente de configuración inicial incluye las siguientes opciones:

- Consulte el inventario del chasis y el estado.
- Importar la configuración desde un archivo de configuración existente.
- Configure los valores generales del CMM.
- Configure la fecha y hora del CMM.

  Consejo: cuando instale XClarity Administrator, configure XClarity Administrator y todos los chasis gestionados por XClarity Administrator para que utilicen un servidor NTP.
- Configure la información IP del CMM.
- Configure la política de seguridad del CMM.
- Configure el sistema de nombres de dominio (DNS).
- Configure los despachadores de sucesos.

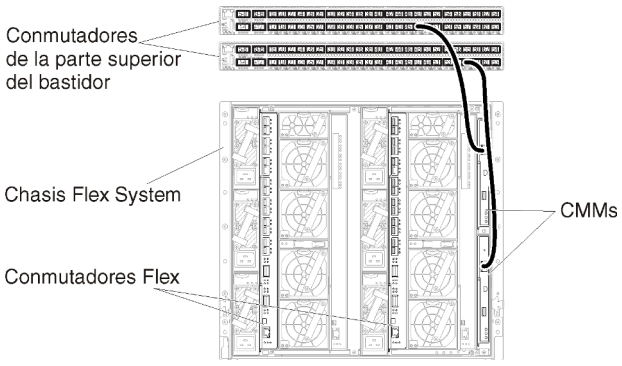
Paso 5. Después de guardar los valores del asistente de configuración y aplicar los cambios, configure las direcciones IP de todos los componentes del chasis.

Consulte el paso 4.6 del poster de instrucciones proporcionado con el chasis.

Nota: Debe restablecer el procesador de gestión del sistema de cada nodo de cálculo y reiniciar los conmutadores Flex para mostrar las nuevas direcciones IP.

Paso 6. Reinicie el CMM mediante la interfaz de gestión del CMM.

Paso 7. Cuando el CMM se esté reiniciando, conecte un cable desde el puerto Ethernet del CMM a su red.



Paso 8. Inicie sesión en la interfaz de gestión del CMM utilizando la nueva dirección IP.

Después de finalizar

También puede configurar el CMM para que admita redundancia. Utilice el sistema de ayuda del CMM para obtener más información acerca de los campos que están disponibles en cada una de las páginas siguientes.

- Configure la conmutación por error para el CMM en caso de que se produzca un fallo de hardware en el CMM principal. En la interfaz de gestión del CMM, haga clic en **Gestión del módulo de gestión → Propiedades → Conmutación por error avanzada**.
- Configure la conmutación por error avanzada como resultado de un problema de red (enlace ascendente). En la interfaz de gestión del CMM, haga clic en **Gestión del módulo de gestión → Red**, haga clic en la pestaña **Ethernet** y, a continuación, haga clic en **Ethernet avanzada**. Como mínimo, asegúrese de seleccionar la casilla **Conmutación por error si hay pérdida de vínculo de red física**.

Paso 4: Configuración de Conmutadores Flex

Configure los Conmutadores Flex en cada chasis.

Antes de empezar

Asegúrese de que están habilitados todos los puertos apropiados, incluidos los puertos externos que van desde el conmutador Flex al conmutador de la parte superior del bastidor y los puertos internos al CMM.

Si los conmutadores Flex se configuran para obtener valores de red dinámicos (dirección IP, máscara de red, puerta de enlace y dirección DNS) a través de DHCP, asegúrese de que dichos conmutadores tienen unos valores coherentes (por ejemplo, compruebe que las direcciones IP se encuentran en la misma red que el CMM).

Importante: Para cada chasis de Flex System, asegúrese de que el tipo de entramado de la tarjeta de expansión de cada servidor en el chasis sea compatible con el tipo de entramado de todos los conmutadores Flex del mismo chasis. Por ejemplo, si instala conmutadores Ethernet en un chasis, todos los servidores de dicho chasis deben tener conectividad Ethernet a través del conector LAN en la placa madre o de una tarjeta de expansión Ethernet. Para obtener más información acerca de cómo configurar los conmutadores Flex, consulte la Configuración de los módulos de E/S en la documentación en línea de Flex System.

Procedimiento

Los pasos de configuración pueden variar en función del tipo de Conmutadores Flex instalado. Para obtener más información acerca de cada uno de los Conmutadores Flex compatibles, consulte Conmutadores de red Flex System en la documentación en línea de Flex System.

Normalmente, tendrá que configurar los conmutadores Flex en las bahías 1 y 2 de conmutadores Flex.

Consejo: la bahía 2 del conmutador Flex es la tercera bahía de los módulos si se mira a la parte posterior del chasis.

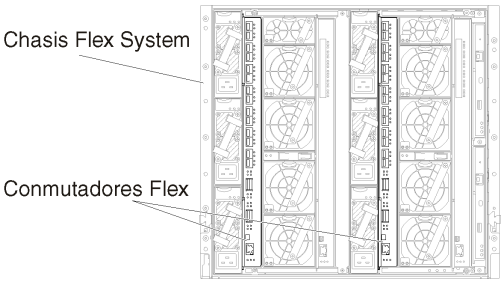


Figura 24. Ubicaciones de los Conmutador Flex en un chasis

Paso 5: Instale y configure el host

Puede instalar Docker en cualquier sistema que cumpla los requisitos para Lenovo XClarity Administrator.

Antes de empezar

Puede usar Docker Datacenter para configurar un entorno de alta disponibilidad para contenedores de XClarity Administrator que se ejecutan en Docker Engine. Para obtener más información sobre la alta disponibilidad de Docker Datacenter, consulte Página web de Arquitectura de alta disponibilidad aplicaciones con Docker Datacenter.

Asegúrese de que el host cumple los requisitos previos definidos en Requisitos previos de hardware y software.

Asegúrese de que el sistema host esté en la misma red que los dispositivos que desea gestionar.

Importante: Puede configurar XClarity Administrator en cualquier sistema que cumpla los requisitos de XClarity Administrator, incluido servidor gestionado. Si utiliza un servidor gestionado para el host XClarity Administrator:

- Debe implementar una topología de redes de datos y de gestión separadas virtualmente o bien una topología de una sola red de datos y gestión.
- No puede utilizar XClarity Administrator para aplicar actualizaciones de firmware a ese servidor gestionado. Aunque solo se aplique parte del firmware con la activación inmediata, XClarity Administrator fuerza el reinicio del servidor de destino, lo que reinicia también XClarity Administrator. Cuando se aplica con la activación diferida, solo se aplica determinado firmware cuando se reinicia el host de XClarity Administrator.
- Si utiliza un servidor en un chasis de Flex System, asegúrese de que el servidor esté configurado para encenderse automáticamente. Puede configurar esta opción en la interfaz web del CMM al hacer clic en **Gestión de chasis → Nodos de cálculo** y después al seleccionar el servidor y seleccionar **Encendido automático** para el **Modo de encendido automático**.

Procedimiento

Instale y configure Docker en el host siguiendo las instrucciones proporcionadas con su distribución de Docker.

Paso 6: Instalación y configuración del XClarity Administrator

Instale y configure el contenedor Lenovo XClarity Administrator en el host Docker recién instalado.

Antes de empezar

Asegúrese de que el sistema host cumpla los requisitos de hardware y software (consulte Requisitos previos de hardware y software).

Asegúrese de que estén habilitados todos los puertos apropiados, incluidos los puertos que XClarity Administrator necesita (consulte Disponibilidad de puertos).

Asegúrese de que el sistema host esté en la misma red que los dispositivos que desea gestionar.

Asegúrese de que el SO host y el XClarity Administrator usan el mismo servidor NTP.

XClarity Administrator permite utilizar un nombre personalizado para la red para la gestión de datos, la gestión del hardware y el despliegue del SO (consulte Configuraciones de red). En estos ejemplos del siguiente procedimiento se utiliza eth0.

XClarity Administrator permite utilizar un nombre personalizado para la red para la gestión de datos y de hardware (consulte Configuraciones de red). En estos ejemplos del siguiente procedimiento se utiliza eth0

Asegúrese de que la red macvlan esté cargada en el kernel en el sistema host. Para comprobar si está cargado, utilice el comando **lsmod | grep macvlan**. Para cargar macvlan en el kernel, ejecute el comando **modprobe macvlan**.

Asegúrese de utilizar un nombre y una dirección IP únicos para cada contenedor cuando ejecute varios contenedores de XClarity Administrator en el mismo host.

Si tiene pensado gestionar ThinkServer y otros dispositivos heredados, asegúrese de que Docker esté habilitado para admitir IPv6.

1. Edite el archivo /etc/docker/daemon.json, establezca la clave **ipv6** en verdadero y establezca la clave **fixed-cidr-v6** en la subred IPv6. A continuación, se muestra un archivo daemon de ejemplo.
```
{
   "ipv6": true,
   "fixed-cidr-v6": "2001:db8:1::/64",
   "experimental": true,
   "ip6tables": true
}
```
2. Ejecute el siguiente comando para volver a cargar el archivo de configuración de Docker.
```
systemctl reload docker
```

Nota: XClarity Administrator *no* se ejecuta como un contenedor con privilegios.

Las reglas de firewall no están configuradas en el contenedor XClarity Administrator. Para agregar reglas de firewall para el contenedor en el sistema host, siga estos pasos.

1. Ejecute el siguiente comando para obtener la ID de proceso Docker, identificada por “NSPID”.
```
docker inspect --format='{{ .State.Pid }}' "$CONTAINER_NAME"
```
2. Ejecute el siguiente comando para crear un enlace simbólico.
```
LINKFILE="/var/run/netns/$NSPID"
mkdir -p /var/run/netns
/bin/rm -f "$LINKFILE"
ln -s "/proc/$NSPID/ns/net" "$LINKFILE"
```
3. Ejecute el siguiente comando para configurar las reglas iptables adecuadas.
```
ip netns exec $NSPID iptables -I OUTPUT -j DROP
```
4. Ejecute el siguiente comando para asegurarse de que se eliminen todos los enlaces.
```
/bin/rm -f "$LINKFILE"
```

Procedimiento

Para instalar un contenedor XClarity Administrator utilizando el método Docker compose, realice los pasos siguientes.

Paso 1. Descargue la imagen del dispositivo virtual de XClarity Administrator, el archivo de entorno y el archivo YAML desde el Página web de descarga de XClarity Administrator hasta una estación de trabajo cliente. Inicie sesión en el sitio web y utilice la clave de acceso que se le facilitó para descargar la imagen.

Paso 2. Importe la imagen del contenedor de XClarity Administrator a su host y ejecute el siguiente comando.
```
docker load -i lnvgy_sw_lxca_<ver>_anyos_noarch.tar.gz
```

Paso 3. Edite el archivo `docker_compose.env` y actualice las variables de entorno siguientes.

- **CONTAINER_NAME**. Nombre de contenedor único, que se utiliza para crear volúmenes de docker para cada instancia de XClarity Administrator (por ejemplo, `CONTAINER_NAME=LXCA-203`)
- **ADDRESS**. Dirección IPv4 estática para el contenedor (por ejemplo, `ADDRESS=192.0.2.0`)
- **BACKUP_MOUNT**. (Opcional) Ruta para el recurso compartido remoto que se puede utilizar para almacenar las copias de seguridad de XClarity Administrator. Debe ser `/mnt/backup_share`.
- **FIRMWARE_MOUNT**. (Opcional) Ruta de acceso para la unidad compartida remota que se puede utilizar como repositorio remoto para las actualizaciones de firmware. Debe ser `/mnt/fw_share`.

A continuación hay un archivo de entorno de muestra.

```
CONTAINER_NAME="LXCA-203"
ADDRESS="192.0.2.0"
BACKUP_MOUNT="/mnt/backup_share"
FIRMWARE_MOUNT="/mnt/fw_share"
```

Paso 4. Edite el archivo `docker_compose.yml` y actualice las propiedades siguientes.

- Establezca la propiedad **image** con el nombre del archivo de imagen de instalación utilizado en el paso 2.

  Nota: Puede cambiar el nombre de archivo de la imagen (por ejemplo, a “más reciente”) mediante el comando `docker tag`.
- Si desea utilizar recursos compartidos remotos como repositorio de firmware remoto y almacenar copias de seguridad de XClarity Administrator, establecer el punto de montaje del host para cada unidad compartida remota en la propiedad **volumes**.
- Establezca la propiedad **DNS** en la dirección IP de los servidores DNS.
- El contenedor comparte el grupo de recursos de procesador y de memoria que están disponibles para el host. Opcionalmente, defina los límites del uso de recursos estableciendo las **cpus** y las propiedades de **memoria**.
- Establezca la propiedad **primaria** al nombre de la interfaz de red del sistema host que se va a utilizar como interfaz primaria para la interfaz macvlan en el contenedor. Esta interfaz debe tener acceso directo a la subred asignada al contenedor.
- Establezca la **subred** y la **puerta de enlace** de acuerdo con la topología de su red. Normalmente, la subred y la puerta de enlace son para la red de gestión a la que pertenece ${ADDRESS}.
- Si desea admitir IPv6, establezca la propiedad **enable_ipv6** en verdadero, establezca la propiedad **ipv6_address** en la dirección IPv6 y añada otro conjunto de propiedades de **subred** y **puerta de enlace** de acuerdo con la topología de su red (normalmente para la red de gestión a la que pertenece la dirección IPv6).

A continuación, se muestra un archivo YML de ejemplo, con IPv6 habilitado.

```
version: '3.8'

services:

  lxca:
    image: lenovo/lxca:4.1.0-124
    container_name: ${CONTAINER_NAME}
    tty: true
    stop_grace_period: 60s
    volumes:
      #bind mount example
```

```
      - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
      - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
      #docker volume mount
      - data:/opt/lenovo/lxca/data
      - postgresql:/var/lib/postgresql
      - log:/var/log
      - confluent-etc:/etc/confluent
      - confluent-log:/var/log/confluent
      - confluent:/var/lib/confluent
      - propconf:/opt/lenovo/lxca/bin/conf
      - ssh:/etc/ssh
      - xcat:/etc/xcat
    networks:
      lan:
        ipv4_address: ${ADDRESS}
        ipv6_address: "2001:8003:7d51:2003::2"
    dns:
      - 192.0.2.10
      - 192.0.2.11
    deploy:
      resources:
        limits:
          cpus: "2.0"
          memory: "8g"

volumes:
  data:
    name: ${CONTAINER_NAME}-data
  postgresql:
    name: ${CONTAINER_NAME}-postgresql
  log:
    name: ${CONTAINER_NAME}-log
  confluent-etc:
    name: ${CONTAINER_NAME}-confluent-etc
  confluent-log:
    name: ${CONTAINER_NAME}-confluent-log
  confluent:
    name: ${CONTAINER_NAME}-confluent
  propconf:
    name: ${CONTAINER_NAME}-propconf
  ssh:
    name: ${CONTAINER_NAME}-ssh
  xcat:
    name: ${CONTAINER_NAME}-xcat

networks:
  lan:
    name: lan
    driver: macvlan
    enable_ipv6: true
    driver_opts:
      parent: eth0
    ipam:
      config:
        - subnet: 192.0.0.0/19
          gateway: 192.0.30.1
        - subnet: "2001:8003:7d51:2000::/80"
          gateway: "2001:8003:7d51:2000::1"
```

Paso 5. Despliegue la imagen en docker al ejecutar el siguiente comando, donde <*ENV_FILENAME*> es el nombre del archivo de variables ambientales que creó en el paso 2.

```
COMPOSE_HTTP_TIMEOUT=300 docker-compose -p ${CONTAINER_NAME} --env-file <ENV_FILENAME> up -d
```

Después de finalizar

Inicie sesión en XClarity Administrator y realice la configuración correspondiente (consulte el Acceso a la interfaz web de Lenovo XClarity Administrator por primera vez y el Configuración de Lenovo XClarity Administrator).

Implementación de alta disponibilidad

Puede usar Docker Datacenter para configurar un entorno de alta disponibilidad para contenedores de Lenovo XClarity Administrator que se ejecutan en Docker Engine.

Para obtener más información sobre la alta disponibilidad de Docker Datacenter, consulte Página web de Arquitectura de alta disponibilidad aplicaciones con Docker Datacenter.

Capítulo 4. Configuración de Lenovo XClarity Administrator

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

Más información: XClarity Administrator: Configuración por primera vez

Procedimiento

Lleve a cabo los pasos siguientes para configurar XClarity Administrator por primera vez.

Paso 1. Acceso a la interfaz web de XClarity Administrator.

Paso 2. Lea y acepte el acuerdo de licencia.

Paso 3. Cree cuentas de usuario que tengan autoridad de supervisor.

Consejo: considere la necesidad de crear al menos dos cuentas de usuario con autoridad de supervisor para disponer de una copia de seguridad en caso necesario.

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

Paso 5. Configure la fecha y hora.

Paso 6. Configure los valores de servicio y soporte durante la configuración inicial, lo que incluye la declaración de privacidad, los datos de uso y de hardware, el soporte de Lenovo (llamar a casa), la herramienta de carga de Lenovo y la garantía de producto.

Paso 7. Configure los valores de seguridad, incluidos el servidor de autenticación, los grupos de usuarios, los certificados de servidor y el modo de criptografía.

Paso 8. Gestione el chasis, los servidores, los conmutadores y los dispositivos de almacenamiento.

Acceso a la interfaz web de Lenovo XClarity Administrator por primera vez

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

Antes de empezar

Asegúrese de utilizar uno de los siguientes navegadores web compatibles:
- Chrome™ 48.0 o posterior (55.0 o superior para Consola remota)
- Firefox® ESR 38.6.0 o posterior
- Microsoft® Internet Explorer® 11
- Microsoft Edge
- Safari® 9.0.2 o posterior (IOS7 o posterior y OS X)

Nota: El inicio de las interfaces del controlador de gestión desde XClarity Administrator mediante el navegador web Safari no se admite.

Asegúrese de que inicia sesión en la interfaz web de XClarity Administrator desde un sistema con conectividad de red al nodo de gestión de XClarity Administrator.

Procedimiento

Lleve a cabo los pasos siguientes para acceder a la interfaz web de XClarity Administrator por primera vez.

Paso 1. Dirija su navegador a la dirección IP de XClarity Administrator.

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

- **Para contenedores**. Use la dirección IPv4 especificada para la variable ${ADDRESS} para acceder a XClarity Administrator mediante la siguiente URL:
  `https://<IPv4_address>/ui/login.html`

  Por ejemplo:
  `https://192.0.2.10/ui/login.html`
- **Para dispositivos virtuales**. La dirección IP que utilice dependerá de cómo esté configurado su entorno.

  Si dispone de redes Eth0 y Eth1 en subredes independientes y utiliza DHCP en las dos subredes, utilice la dirección IP *Eth1* cuando acceda a la interfaz web para realizar la configuración inicial. Cuando XClarity Administrator se inicia por primera vez, tanto Eth0 como Eth1 obtienen una dirección IP asignada por DHCP, mientras que la puerta de enlace predeterminada de XClarity Administrator se establece en la puerta de enlace asignada por DHCP para *Eth1*.

  Uso de una dirección IPv4 estática
  Si ha especificado una dirección IPv4 en eth0_config, úsela para acceder a XClarity Administrator utilizando la siguiente URL:
  `https://<IPv4_address>/ui/login.html`

  Por ejemplo:
  `https://192.0.2.10/ui/login.html`

  Uso de un servidor DHCP en el mismo dominio de difusión que XClarity Administrator
  Si ha configurado un servidor DHCP en el mismo dominio de difusión que XClarity Administrator, utilice la dirección IPv4 que se muestra en la consola de la máquina virtual de XClarity Administrator para acceder a XClarity Administrator utilizando la siguiente URL:
  `https://<IPv4_address>/ui/login.html`

  Por ejemplo:
  `https://192.0.2.10/ui/login.html`

  Uso de un servidor DHCP en otro dominio de difusión que XClarity Administrator
  Si *no* se ha configurado un servidor DHCP en el mismo dominio de difusión, utilice la dirección de vínculo local (LLA) IPv6 que se muestra para eEth0 (la red de gestión) en la consola de la máquina virtual de XClarity Administrator para acceder a XClarity Administrator; por ejemplo:

```
------------------------------------------
Lenovo XClarity Administrator  Version x.x.x
------------------------------------------

eth0   flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  metric 1
         inet 192.0.2.10  netmask 255.255.255.0  broadcast 192.0.2.55
         inet6 2001:db8:56ff:fe80:bea3  prefixlen 64   scopeid 0x20<link>
         ether 00:15:5d:0c:d1:92    txqueuelen 1000 (Ethernet)
```

```
          RX errors 0  dropped 0  overruns 0  frame 0

eth1   flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  metric 1
          inet 192.0.2.20  netmask 255.255.255.0  broadcast 192.0.2.130
          inet6 2001:db8:56ff:fe80:bea3  prefixlen 64  scopeid 0x20<link>

================================================================================
================================================================================

You have 150 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
  x. To continue without changing IP settings
  … …
```

Consejo: la dirección de vínculo local (LLA) IPv6 se deriva de la dirección MAC de la interfaz.

Atención: Si está configurando XClarity Administrator 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 Administrator desde otra MV que tenga conectividad a XClarity Administrator. Por ejemplo, puede acceder a XClarity Administrator desde otra MV del host donde esté instado XClarity Administrator.

– **Firefox:**

  Para acceder a la interfaz web de XClarity Administrator desde un navegador de Firefox, inicie sesión utilizando la siguiente URL. Recuerde que se requieren corchetes al introducir direcciones IPv6.

  `https://[<IPv6_LLA>/ui/login.html]`

  Por ejemplo, según el ejemplo anterior mostrado para Eth0, introduzca la siguiente URL en el navegador web:

  `https://[fe80:21a:64ff:fe12:3456]/ui/login.html`

– **Internet Explorer:**

  Para acceder a la interfaz web de XClarity Administrator desde un navegador de Internet Explorer, inicie sesión utilizando la siguiente URL. Recuerde que se requieren corchetes al introducir direcciones IPv6.

  `https://[<IPv6_LLA>%25<zone_index>]/ui/login.html`

  donde *<zone_index>* es el identificador del adaptador Ethernet que está conectado a la red de gestión del equipo en el que ha iniciado el navegador web. Si está utilizando un navegador en Windows, utilice el comando `ipconfig` para buscar el índice de zona, que se muestra después del símbolo de porcentaje (%) en el campo **Dirección de vínculo local IPv6** del adaptador. En el ejemplo siguiente, el índice de zona es “30.”

```
PS C:> ipconfig
Windows IP Configuration

Ethernet adapter vEthernet (teamVirtualSwitch):

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : 2001:db8:56ff:fe80:bea3%30
   Autoconfiguration IPv4 Address. . : 192.0.2.30
   Default Gateway . . . . . :
```

  Si utiliza un navegador en Linux, utilice el mandato `ifconfig` para buscar el índice de zona. También puede utilizar el nombre del adaptador (normalmente Eth0) como índice de zona.

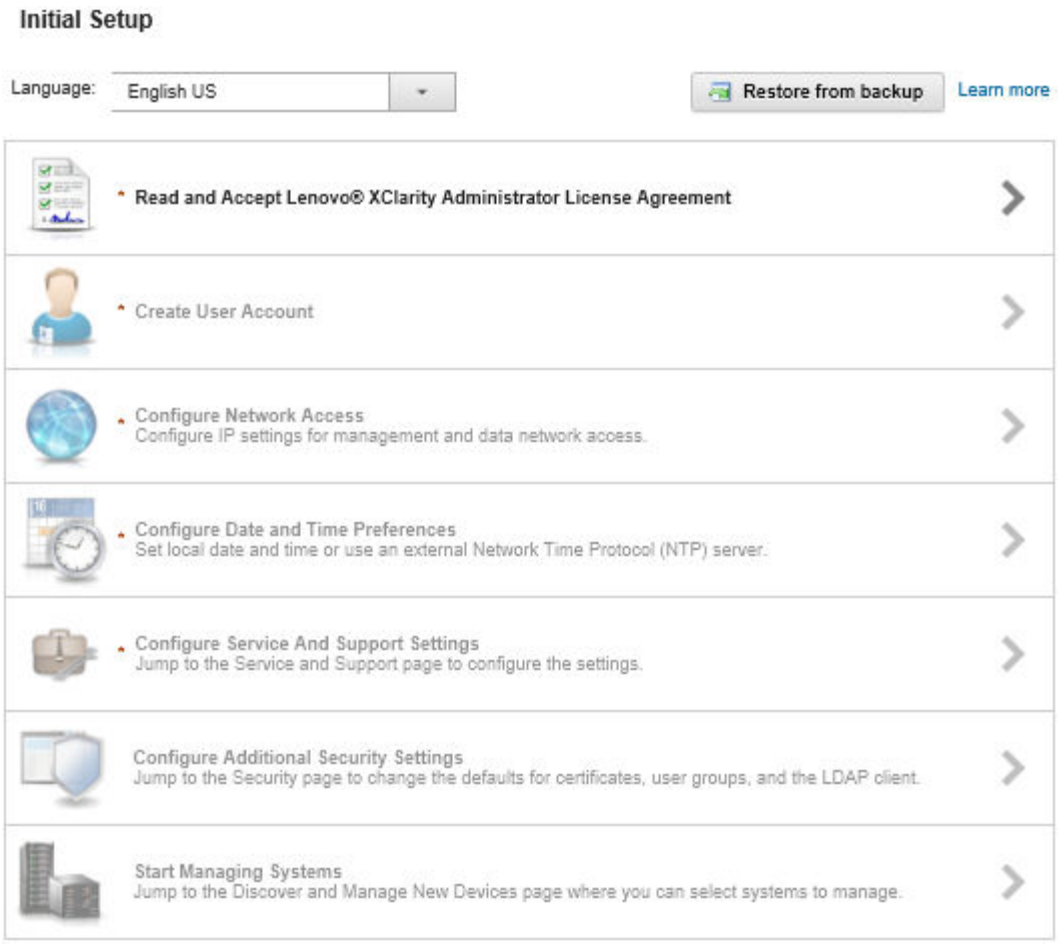
Por ejemplo, según los ejemplos mostrados para Eth0 y el índice de zona, introduzca la siguiente URL en el navegador web:

```
https://[2001:db8:56ff:fe80:bea3%2530]/ui/login.html
```

Paso 2. Es posible que reciba advertencias de seguridad o de certificado la primera vez que acceda a Lenovo XClarity Administrator. Puede hacer caso omiso de las advertencias.

Resultados

Aparece la página Configuración inicial.



Después de finalizar

Lleve a cabo los pasos de configuración iniciales para configurar XClarity Administrator (consulte Configuración de Lenovo XClarity Administrator).

Crear cuentas de usuarios

Las cuentas de usuarios se utilizan para gestionar autorización y acceso a Lenovo XClarity Administrator y a dispositivos que están sujetos a autenticación gestionada.

Acerca de esta tarea

La primera cuenta de usuario que cree debe tener el rol de Supervisor y de estar activada (habilitada).

Como medida de seguridad adicional, cree al menos dos cuentas de usuarios que tengan el rol de **Supervisor**. Asegúrese de que registra las contraseñas de estas cuentas de usuarios y las almacena en una ubicación segura por si necesita restaurar Lenovo XClarity Administrator.

Procedimiento

Para crear cuentas de usuario, lleve a cabo los pasos siguientes.

Paso 1. Rellene la siguiente información en el cuadro de diálogo Crear usuario supervisor nuevo.

- Escriba un nombre de usuario y una descripción del usuario.
- Introduzca la nueva contraseña y confírmela en los campos correspondientes. Las reglas de las contraseñas se basan en los valores de seguridad actuales de la cuenta.
- Seleccione uno o más grupos de roles para autorizar al usuario a realizar las tareas apropiadas.

  Para obtener información sobre los grupos de roles y cómo crear grupos de roles personalizados, consulte Creación de un grupo de roles en la documentación en línea de XClarity Administrator.
- Opcionalmente, establezca **Cambiar contraseña en el primer acceso** en `Yes` si desea obligar al usuario a cambiar la contraseña la primera vez que inicie sesión en XClarity Administrator.

Paso 2. Haga clic en **Crear**.

Paso 3. Haga clic en el icono **Crear** ( ) y repita los pasos anteriores para crear usuarios adicionales.

Paso 4. Haga clic en **Volver a la configuración inicial**.

Configuración del acceso de red

Para configurar el acceso de red, puede configurar hasta dos interfaces de red, el nombre de host para Lenovo XClarity Administrator y los servidores DNS que se pueden utilizar.

Acerca de esta tarea

XClarity Administrator tiene dos interfaces de red separadas que se pueden definir para su entorno, dependiendo de la topología de red que implemente. Para los dispositivos virtuales, estas redes se denominan eth0 y eth1. Para los nombres originales, puede elegir los nombres personalizados.

- Cuando solo hay una interfaz de red (eth0):
  - La interfaz debe estar configurada para admitir la detección de dispositivos y de gestión (como la configuración del servidor y las actualizaciones de firmware). Debe poder comunicarse con los CMM y los conmutadores Flex en cada chasis gestionado, el controlador de gestión de la placa base en cada servidor gestionado y cada conmutador RackSwitch.
  - Si tiene pensado adquirir actualizaciones de firmware y de controlador de dispositivo de SO usando XClarity Administrator, al menos una de las interfaces de red también debe estar conectada con Internet, preferentemente a través de un firewall. Si no es así, tiene que importar las actualizaciones al repositorio.
  - Si desea recopilar datos del servicio o bien notificación automática de problemas (incluido Llamar a casa y la herramienta de carga de Lenovo), al menos una de las interfaces de red debe estar conectada a Internet, preferentemente a través de un firewall.
  - Si desea desplegar imágenes del sistema operativo y actualizar controladores de dispositivos de SO, la interfaz debe tener conectividad de red IP a la interfaz de red del servidor que se utiliza para acceder al sistema operativo del host.

    Nota: Si implementó una red aparte para desplegar SO y actualizar controladores de dispositivos de SO, puede configurar la segunda interfaz de red para conectarse a esa red en lugar de hacerlo a la red

de datos. Sin embargo, si el sistema operativo de cada servidor no tiene acceso a la red de datos, deberá configurar una interfaz adicional en los servidores para proporcionar conectividad desde el sistema operativo host a la red de datos para el despliegue del SO y las actualizaciones de controlador de dispositivo de SO, de ser necesario.

- Cuando hay dos interfaces de red (eth0 y eth1):
  - La primera interfaz de red (normalmente, la interfaz Eth0) debe estar conectada a la red de gestión y configurada para que admita la detección de dispositivos y gestión (incluidas las actualizaciones de firmware y configuración del servidor. Debe poder comunicarse con los CMM y los conmutadores Flex en cada chasis gestionado, el controlador de gestión en cada servidor gestionado y cada conmutador RackSwitch.
  - La segunda interfaz de red (normalmente la interfaz eth1) se puede configurar para comunicarse con una red de datos interna, con una red de datos pública o ambas.
  - Si tiene pensado adquirir actualizaciones de firmware y de controlador de dispositivo de SO usando XClarity Administrator, al menos una de las interfaces de red también debe estar conectada con Internet, preferentemente a través de un firewall. Si no es así, tiene que importar las actualizaciones al repositorio.
  - Si desea recopilar datos del servicio o bien notificación automática de problemas (incluido Llamar a casa y la herramienta de carga de Lenovo), al menos una de las interfaces de red debe estar conectada a Internet, preferentemente a través de un firewall.
  - Si tiene pensado desplegar imágenes del sistema operativo y actualizar los controladores de dispositivo del SO, puede elegir utilizar la interfaz eth1 o eth0. Sin embargo, la interfaz que use debe tener la conectividad de red IP hacia la interfaz de red del servidor que se usa para acceder al sistema operativo host.

    Nota: Si implementó una red aparte para desplegar SO y actualizar controladores de dispositivos de SO, puede configurar la segunda interfaz de red para conectarse a esa red en lugar de hacerlo a la red de datos. Sin embargo, si el sistema operativo de cada servidor no tiene acceso a la red de datos, deberá configurar una interfaz adicional en los servidores para proporcionar conectividad desde el sistema operativo host a la red de datos para el despliegue del SO y las actualizaciones de controlador de dispositivo de SO, de ser necesario.

En la tabla siguiente se muestran las configuraciones que se pueden realizar para las interfaces de red de XClarity Administrator según el tipo de topología de red que se haya implementado en su entorno. Utilice esta tabla para determinar cómo definir cada interfaz de red.

Tabla 2. Rol de cada interfaz de red según la topología de red

Topología de red	Rol de la interfaz 1 (eth0)	Rol de la interfaz 2 (eth1)
Red convergente (red de gestión y datos con soporte para el despliegue del SO y actualizaciones del controlador de dispositivo del SO)	Red de gestión • Detección y gestión • Configuración del servidor • Actualizaciones de firmware • Recopilación de datos de servicio • Notificación automática de problemas (como Llamar a casa y la herramienta de actualización de Lenovo) • Recuperación de datos de garantía • Implementación de SO • Actualizaciones de controladores de dispositivos de SO	Ninguno
Red de gestión separada con soporte para el despliegue del SO y actualizaciones del controlador de dispositivo del SO y red de datos	Red de gestión • Detección y gestión • Configuración del servidor • Actualizaciones de firmware • Recopilación de datos de servicio • Notificación automática de problemas (como Llamar a casa y la herramienta de actualización de Lenovo) • Recuperación de datos de garantía • Implementación de SO • Actualizaciones de controladores de dispositivos de SO	Red de datos • Ninguno
Red de gestión separada y red de datos con soporte para el despliegue del SO y actualizaciones del controlador de dispositivo del SO	Red de gestión • Detección y gestión • Configuración del servidor • Actualizaciones de firmware • Recopilación de datos de servicio • Notificación automática de problemas (como Llamar a casa y la herramienta de actualización de Lenovo) • Recuperación de datos de garantía	Red de datos • Implementación de SO • Actualizaciones de controladores de dispositivos de SO

Tabla 2. Rol de cada interfaz de red según la topología de red (continuación)

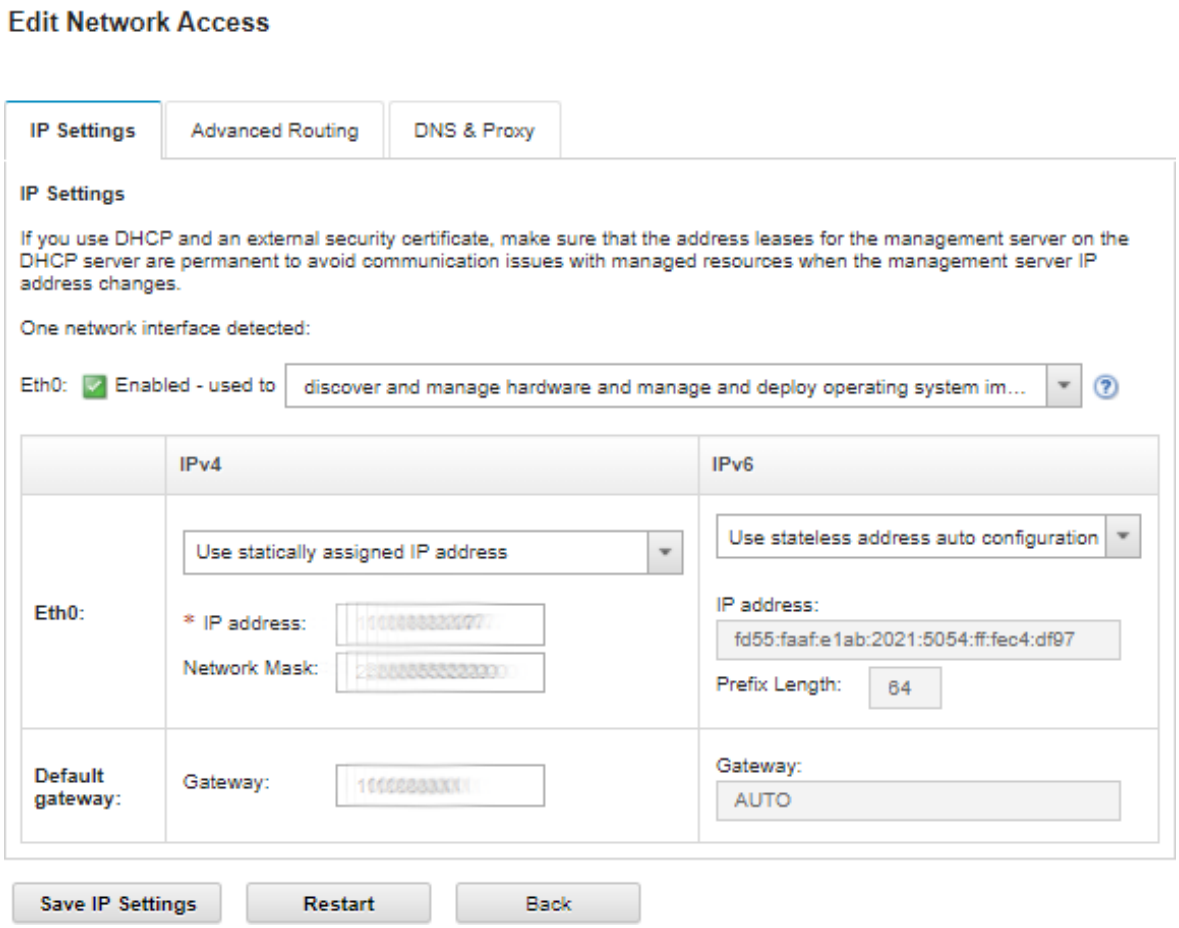
Topología de red	Rol de la interfaz 1 (eth0)	Rol de la interfaz 2 (eth1)
Red de gestión separada y red de datos sin soporte para el despliegue del SO y actualizaciones del controlador de dispositivo del SO	Red de gestión • Detección y gestión • Configuración del servidor • Actualizaciones de firmware • Recopilación de datos de servicio • Notificación automática de problemas (como Llamar a casa y la herramienta de actualización de Lenovo) • Recuperación de datos de garantía	Red de datos • Ninguno
Solo red de gestión (no se admiten el despliegue del SO y las actualizaciones de controladores de dispositivos del SO)	Red de gestión • Detección y gestión • Configuración del servidor • Actualizaciones de firmware • Recopilación de datos de servicio • Notificación automática de problemas (como Llamar a casa y la herramienta de actualización de Lenovo) • Recuperación de datos de garantía	Ninguno

Para obtener más información sobre las interfaces de red de XClarity Administrator, consulte Consideraciones de red.

Procedimiento

Para configurar el acceso de red, lleve a cabo los pasos siguientes.

Paso 1. En la página Configuración inicial, haga clic en **Configurar acceso a red**. Se muestra la página Editar acceso de red.



Paso 2. Si tiene pensado desplegar sistemas operativos y actualizar los controladores de dispositivo del sistema operativo mediante XClarity Administrator, elija la interfaz de red que se utilizará para la gestión de sistemas operativos.

- Si solo se define una interfaz para XClarity Administrator, elija si dicha interfaz debe utilizarse para detectar y gestionar hardware únicamente, o si también debe utilizarse para gestionar imágenes de sistemas operativos.
- Si se definen dos interfaces para XClarity Administrator (Eth0 y Eth1), determine la interfaz que debe utilizarse para gestionar imágenes de sistemas operativos. Si elige “Ninguno”, *no* puede desplegar imágenes de sistemas operativos o actualizar los controladores de dispositivos de SO a servidores gestionados desde XClarity Administrator.

Paso 3. Especifique los valores IP.

a. Para la primera interfaz, especifique la dirección IPv4, la dirección IPv6 o ambas.

- **IPv4**. Debe asignar una dirección IPv4 a la interfaz. Puede elegir usar una dirección IP asignada de forma estática, o bien obtener una dirección IP desde un servidor DHCP.
- **IPv6**. De manera opcional, puede asignar una dirección IPv6 a la interfaz utilizando uno de los siguientes métodos de asignación:
  - Usar dirección IP asignada estáticamente
  - Usar la configuración de dirección con estado (DHCPv6)
  - Usar la configuración automática de dirección sin estado

  Nota: Para obtener información acerca de las limitaciones de la dirección IPv6, consulte Limitaciones de configuración de IP.

b. Si hay una segunda interfaz disponible, especifique la dirección IPv4, la dirección IPv6 o ambas.

Nota: Las direcciones IP que están asignadas a esta interfaz deben estar en una subred distinta de la de las direcciones IP que están asignadas a la primera interfaz. Si elige utilizar DHCP para asignar direcciones IP a ambas interfaces (Eth0 y Eth1), el servidor DHCP no debe asignar la misma subred para las direcciones IP de las dos interfaces.

- **IPv4**. Puede elegir usar una dirección IP asignada de forma estática, o bien obtener una dirección IP desde un servidor DHCP.
- **IPv6**. De manera opcional, puede asignar una dirección IPv6 a la interfaz utilizando uno de los siguientes métodos de asignación:
  - Usar dirección IP asignada estáticamente
  - Usar la configuración de dirección con estado (DHCPv6)
  - Usar la configuración automática de dirección sin estado

c. Especifique la puerta de enlace predeterminada.

Si especifica una puerta de enlace predeterminada, debe ser una dirección IP válida y debe utilizar la misma máscara de red (la misma subred) que la dirección IP de una de las interfaces de red (Eth0 o Eth1). Si utiliza una sola interfaz, puerta de enlace predeterminada esta debe estar en la misma subred que la interfaz de red.

Si cualquiera de las interfaces utiliza DHCP para obtener una dirección IP, la puerta de enlace predeterminada también utiliza DHCP. Para introducir manualmente una dirección de puerta de enlace predeterminada que invalida la que se ha recibido desde el servidor DHCP, seleccione la casilla de verificación **Puerta de enlace de sustitución**.

Sugerencias:

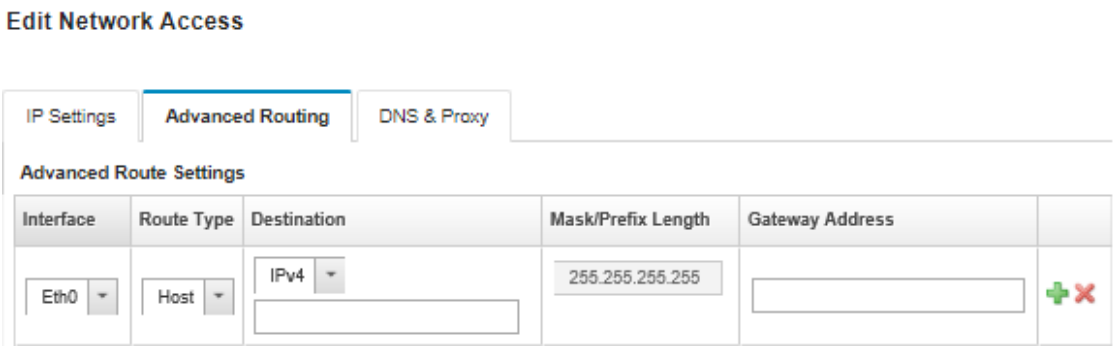
- Asegúrese de que la puerta de enlace coincida con una de las subredes de las interfaces de red. La puerta de enlace predeterminada se establece automáticamente a través de esa interfaz de red.
- Para volver a una puerta de enlace proporcionada por DHCP, borre la casilla de verificación **Puerta de enlace de sustitución**.

PRECAUCIÓN:
Si elige invalidar la puerta de enlace, tenga cuidado de introducir la dirección de la puerta de enlace correcta; de lo contrario, no se podrá acceder a este servidor de gestión y no hay ninguna forma de iniciar sesión de forma remota para corregirlo.

d. Haga clic en **Guardar la configuración de IP**.

Paso 4. **Opcional:** configure los valores avanzados.

a. Haga clic en la pestaña **Disposición avanzada**.



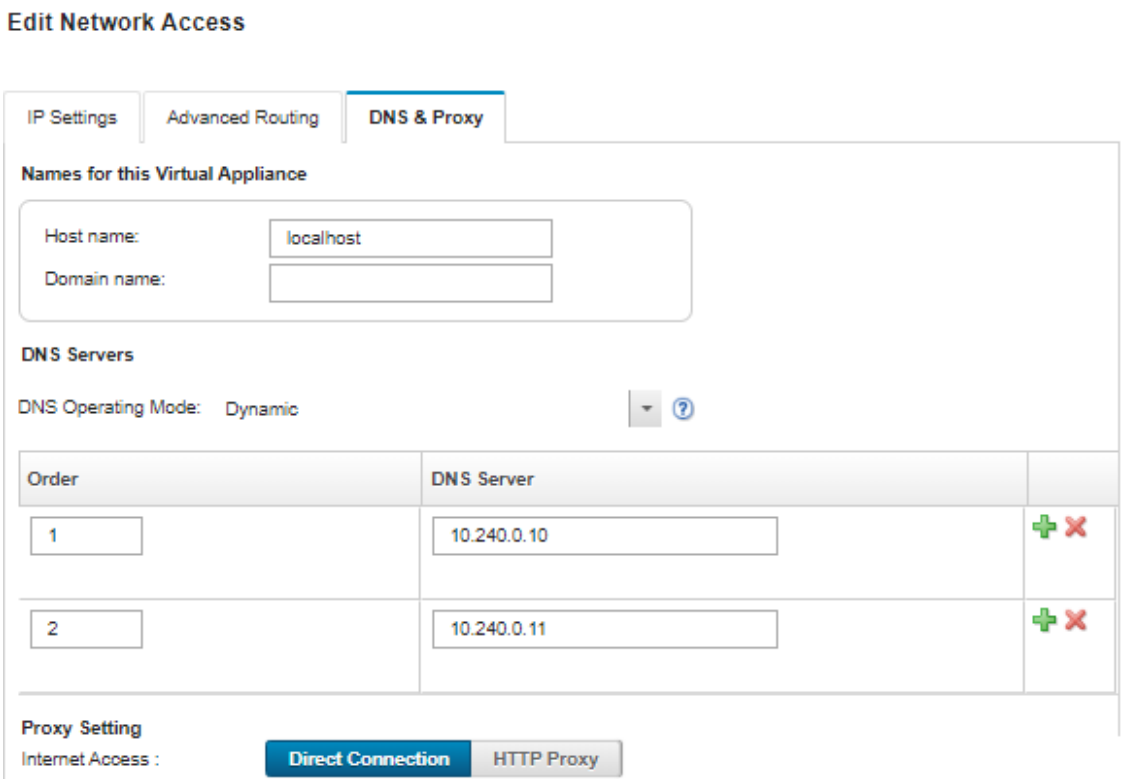
b. Especifique una o varias entradas de ruta de la tabla **Valores de ruta avanzados** para que esta interfaz las utilice.

   Para definir una o mas entradas de ruta, lleve a cabo los pasos siguientes.
   1. Elija la interfaz.
   2. Especifique el tipo de ruta, que puede ser una ruta otro host o a una red.
   3. Especifique el host de destino o la dirección de red a la que está dirigiendo la ruta.
   4. Especifique la máscara de subred de la dirección de destino.
   5. Especifique la dirección de la puerta de enlace a la que deben dirigirse los paquetes.

c. Haga clic en **Guardar disposición avanzada**.

Paso 5. También puede modificar los valores de DNS y proxy.

a. Haga clic en la pestaña **DNS y proxy**.



b. Especifique el nombre de host y el nombre de dominio que se van a utilizar para XClarity Administrator.

c. Seleccione la modalidad operativa DNS. Este puede ser **Estático** o **DHCP**.

   Atención: Debe reiniciar el servidor de gestión cuando cambie el modo de operación de DNS.

   Nota: 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 Administrator renueve la concesión de DHCP.

d. Especifique la dirección IP de uno o varios Servidores del sistema de nombres de dominio (DNS) que se van a utilizar y el orden de prioridad para cada uno.

e. Especifique si el acceso a Internet usa una conexión directa o un proxy HTTP (si XClarity Administrator tiene acceso a Internet).

   Notas: Si usa un proxy HTTP, asegúrese de que se cumplan los siguientes requisitos.

- 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.

Si elige utilizar un proxy HTTP, complete los campos obligatorios:

1. Especifique el nombre de host y el puerto del servidor proxy.
2. Elija si va a utiliza la autenticación y especifique el nombre de usuario y la contraseña si corresponde.
3. Especifique la URL de prueba de proxy.
4. Haga clic en **Proxy de texto** para verificar que los valores del proxy están configurados y que funcionan correctamente.

f. Haga clic en **Guardar DNS y proxy**.

g. Envíe el nombre de dominio completamente calificado (FQDN) y la información de DNS del servidor de gestión de XClarity Administrator a los servidores gestionados con IMM2, XCC, XCC2 y XCC3 de modo que los servidores gestionados puedan encontrar el servidor de gestión utilizando esta información.

1. Haga clic en **Insertar FQDN/DNS en BMC**.
2. Elija cómo gestionar las entradas DNS existentes en el controlador de gestión de la placa base.
   - Mantenga las entradas DNS existentes y añada las entradas DNS del servidor de gestión en la próxima ranura disponible.
   - Sustituya todas las entradas DNS existentes por las entradas DNS del servidor de gestión.
3. Escriba **SÍ** en el campo Editar.
4. Haga clic en **Aplicar**.

Se crea un trabajo para llevar a cabo esta operación. Puede supervisar el progreso del trabajo desde la tarjeta **Supervisión → Trabajos**. Si el job no se ha completado correctamente, haga clic en el enlace del trabajo para mostrar los detalles del trabajo (consulte Uso de trabajos en la documentación en línea de XClarity Administrator).

También puede quitar la información de FQDN y DNS del servidor de gestión de los servidores gestionados con IMM2, XCC y XCC2 y XCC3 si hace clic en **Quitar FQDN/DNS del BMC**. Puede elegir mantener otras entradas DNS existentes, quitar todas las entradas DNS o quitar únicamente las entradas que coincidan con la información del servidor de gestión.

Paso 6. Haga clic en **Atrás**.

Paso 7. Haga clic en **Probar conexión** para verificar los valores de red.

Configuración de fecha y hora

Aunque es posible establecer manualmente la fecha y la hora para Lenovo XClarity Administrator, un método mejor consiste en configurar un servidor de protocolo de tiempo de red (NTP) y utilizarlo para sincronizar las marcas de tiempo entre XClarity Administrator y todos los dispositivos gestionados.

Antes de empezar

Debe usar al menos uno (y hasta cuatro) servidores de protocolo de tiempo de red (NTP) para sincronizar las marcas de tiempo de todos los sucesos que se reciben desde los dispositivos gestionados con XClarity Administrator.

Consejo: debe ser posible acceder al servidor NTP mediante la red de gestión (normalmente, la interfaz Eth0). Considere la posibilidad de configurar el servidor NTP en el host en el que XClarity Administrator se encuentra en ejecución.

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

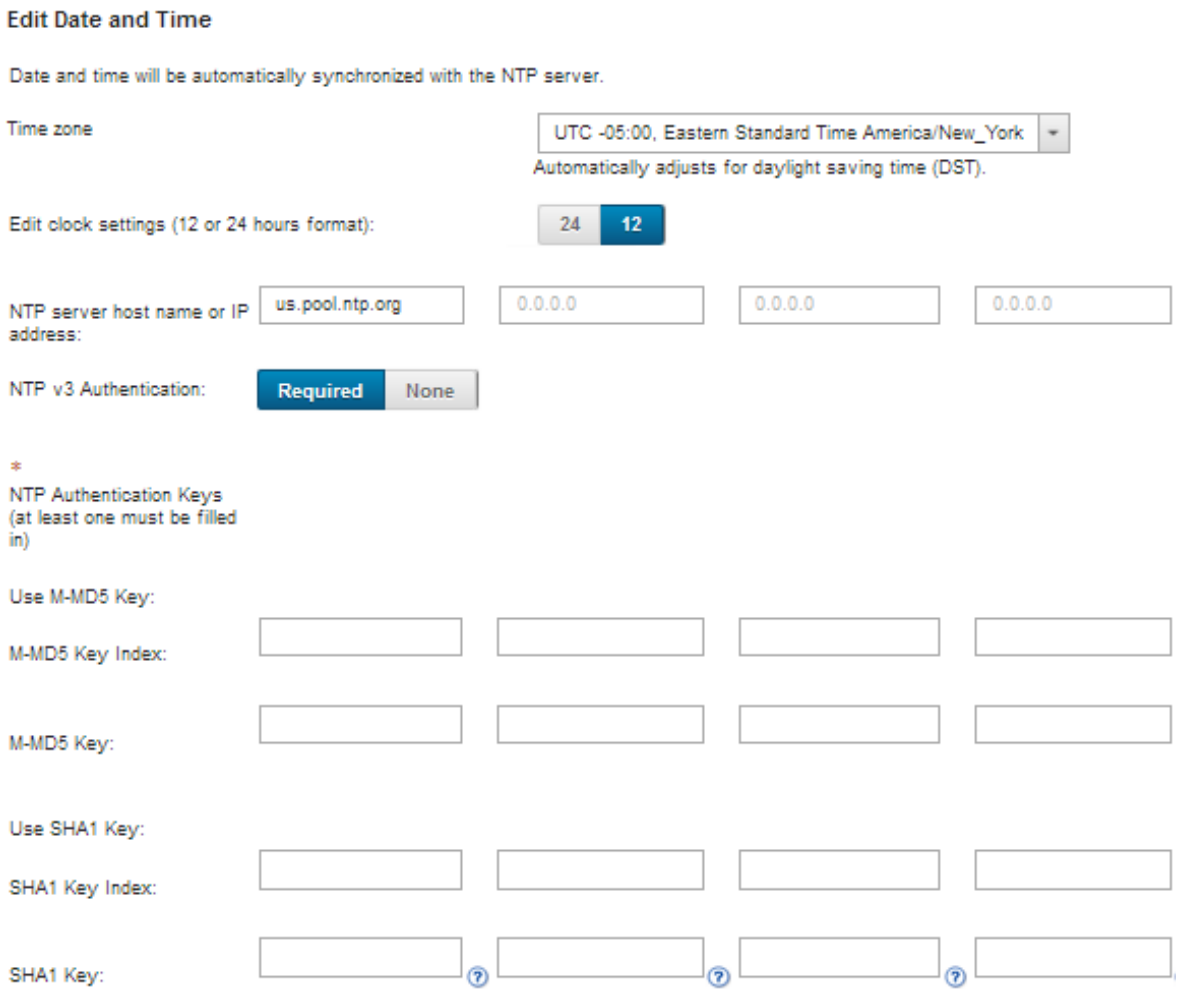
Atención: El dispositivo virtual XClarity Administrator y su host se deben configurar para sincronizarse con la misma fuente para evitar una falla de sincronización de hora inadvertida entre el XClarity Administrator y el host. Normalmente, el host está configurado para que sus dispositivos virtuales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

- Para ESXi, siga las instrucciones del VMware: página web de deshabilitar la sincronización de hora.
- Para Hyper-V, desde el Administrador de Hyper-V, haga clic con el botón derecho en XClarity Administrator máquina virtual y luego haga clic en **Configuración**. 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 configurar un servidor NTP para XClarity Administrator, lleve a cabo los pasos siguientes.

Paso 1. En la página Configuración inicial, haga clic en **Configurar preferencias de fecha y hora**. Aparece la página Editar fecha y hora.



Paso 2. Rellene el cuadro de diálogo de fecha y hora.

1. Elija la zona horaria en la que está ubicado el host de XClarity Administrator.

   Si la zona horaria seleccionada posee horario de verano (DST), la hora se ajusta automáticamente según DST.
2. Elija usar un reloj de 12 horas o 24 horas.
3. Especifique el nombre de host o la dirección IP para cada servidor NTP en su red. Puede definir hasta cuatro servidores NTP.
4. Seleccione **Requerido** para habilitar la autenticación de NTP v3, o seleccione **Ninguno** para usar la autenticación de NTP v1 entre XClarity Administrator y los servidores NTP en su red.

   Puede usar la autenticación v3 si los CMM de Flex System y los controladores de gestión de placa base tienen firmware que requiera autenticación v3 y si la autenticación NTP v3 se requiere entre XClarity Administrator y uno o más servidores NTP dentro de su red
5. Si habilitó la autenticación de NTP v3, establezca la clave de autenticación y el índice para cada servidor NTP aplicable. Puede especificar una clave M-MD5, la clave SHA1 o ambos. Si se especificaron claves M-MD5 o SHA1, XClarity Administrator envía la clave M-MD5 o SHA1 a los CMM de Flex System gestionados y los controladores de gestión que los admiten. El XClarity Administrator usa la clave para autenticar el servidor NTP.
   - Para la clave M-MD5, especifique una cadena ASCII que incluya solo letras mayúsculas y minúsculas (a z, a Z), dígitos (0-9) y los siguientes caracteres especiales @# .

- Para la clave SHA1, especifique una cadena ASCII de 40 caracteres, que incluya solo 0-9 y a-f.
- El índice de clave especificado y la clave de autenticación deben coincidir con el Id. de clave y los valores de contraseña establecidos en el servidor NTP. Por ejemplo, si el índice de clave de la clave SHA1 introducido en el servidor NTP es 5, el índice de clave especificado de la clave SHA1 de XClarity Administrator también es 5. Para obtener información acerca de cómo establecer el Id. de clave y la contraseña, consulte la documentación del servidor NTP.
- Debe especificar la clave para cada servidor NTP que usa la autenticación v3, incluso si dos o más servidores NTP utilizan la misma clave.
- Si habilita la autenticación v3, pero no proporciona una clave de autenticación y el índice para un servidor NTP, se utiliza la autenticación de v1 de forma predeterminada.
- Si especifica varios servidores NTP, los servidores NTP deben todos tener autenticación v3 o todos v1. No se admiten servidores NTP con una combinación de autenticación v3 y v1.
- Si especifica varios servidores NTP con autenticación v3, los índices clave deben ser únicos si las claves no son las mismas. Por ejemplo, el servidor NTP 1 y 2 no pueden tener el índice de clave 1 de SHA1 si las claves de SHA1 son distintas en el servidor NTP 1 y 2. Debe volver a configurar uno de los servidores NTP para aceptar la clave con un índice de clave diferente que el servidor NTP; de lo contrario, se configurará esa última clave definida que estaba asociada con un índice de clave para todos los servidores NTP con el mismo índice de clave.

Paso 3. Haga clic en **Guardar**.

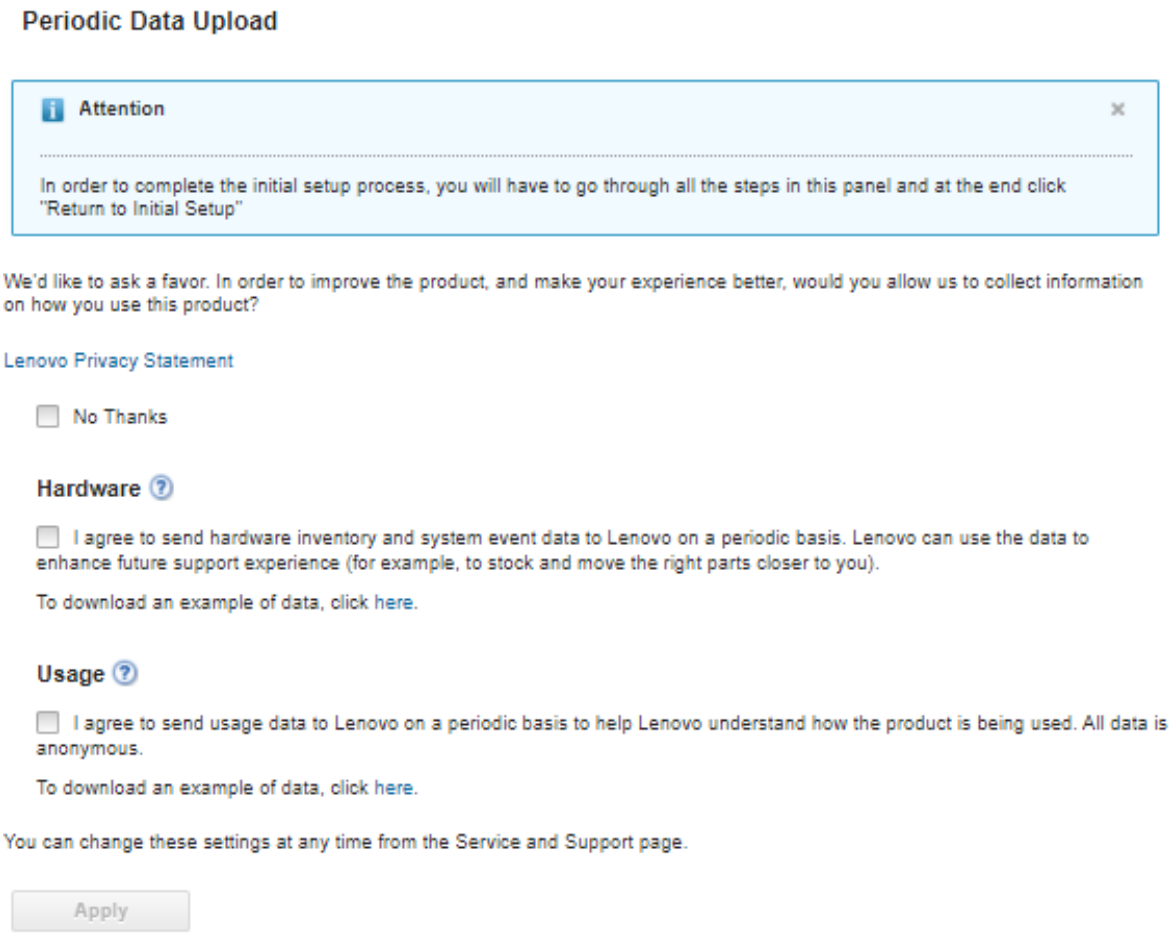
Configurar servicio y soporte

Puede configurar los valores de servicio y soporte, lo que incluye los datos de uso, soporte de Lenovo (llamar a casa), la herramienta de carga de Lenovo y la garantía de producto.

Procedimiento

Lleve a cabo los pasos siguientes para configurar la seguridad.

Paso 1. En la página Configuración inicial, haga clic en **Configurar valores de servicio y soporte**. Se abre la página Servicio y soporte.



Paso 2. Lea y acepte el Declaración de privacidad de Lenovo.

Nota: No puede recopilar ni enviar datos a Lenovo sin haber aceptado primero el Declaración de privacidad de Lenovo. Si elige rechazar la declaración de privacidad, puede revisar y aceptar la declaración de privacidad más adelante en la página de **Servicio y soporte → Configuración de Llamar a casa**.

Paso 3. Puede optar por permitir que Lenovo XClarity Administrator recopile información de uso y de hardware y hacer clic en **Aplicar**.

Puede recopilar y enviar los siguientes tipos de datos a Lenovo.

- **Datos de uso**

  Al aceptar enviar datos de uso a Lenovo se recopilan los siguientes datos y se envían cada semana. Estos datos *son anónimos*. No se recopilan datos privados (incluidos los números de serie, los UUID, los nombres de host, las direcciones IP y los nombres de usuario) ni se envían a Lenovo.
  - Registro de acciones que se han realizado
  - Lista de los sucesos que se provocaron y la marca de tiempo cuando se generaron
  - Lista de los sucesos de auditoría que se provocaron y la marca de tiempo cuando se generaron
  - Lista de trabajos que se ejecutaron e información de éxito o error para cada trabajo
  - Métricas de XClarity Administrator, incluido el uso de la memoria, el uso del procesador y el espacio del disco
  - Datos de inventario limitados sobre todos los dispositivos gestionados
- **Datos de hardware**

Al aceptar enviar datos de hardware a Lenovo, se recopilan los siguientes datos y se envían de forma periódica. Estos datos *no son anónimos*. Los datos de hardware incluyen atributos, tales como UUID y números de serie. No incluye direcciones IP ni nombres de host.

- **Datos de hardware diarios**. Se incluyen los siguientes datos para cada cambio de inventario.
  - Suceso de cambio de inventario (FQXHMDM0001I)
  - Cambios en los datos de inventario para el dispositivo asociado con ese suceso
- **Datos de hardware semanales**. Los datos de inventario se incluyen para todos los dispositivos gestionados.

Cuando se envían datos de uso y de hardware a Lenovo, se registra un suceso en el registro de auditoría.

Puede cambiar este valor en cualquier momento y descargar el último archivo que se recopiló y se envió a Lenovo utilizando los enlaces al hacer clic en **Administración → Servicio y soporte** y, a continuación, haciendo clic en la pestaña **Carga periódica de datos**.

Paso 4. Opcionalmente, haga clic en **Configuración de Llamar a casa** para configurar la notificación automática de problemas al soporte de Lenovo (llamar a casa). A continuación, haga clic en **Aplicar y habilitar** para crear el despachador de servicio de llamar a casa predeterminado, o bien haga clic en **Solo aplicar** para guardar la información de contacto.

Para obtener más información acerca de cómo configurar la notificación automática de problemas a soporte de Lenovo, consulte Configuración de la llamada a casa en la documentación en línea de XClarity Administrator.

Paso 5. Opcionalmente, haga clic en **Herramienta de carga de Lenovo** para configurar la notificación automática de problemas a la herramienta de carga de Lenovo. A continuación, haga clic en **Aplicar y habilitar** para crear el despachador de servicio predeterminado de la Herramienta de carga de Lenovo, o bien haga clic en **Solo aplicar** para guardar la información de configuración.

Para obtener más información acerca de cómo configurar la notificación automática de problemas a la herramienta de carga de Lenovo, consulte Configuración de la notificación automática de problemas para la Herramienta de carga de Lenovo en la documentación en línea de XClarity Administrator.

Paso 6. Opcionalmente, haga clic en **Garantía** para permitir que las conexiones externas que sean necesarias para recopilar información de garantía para los dispositivos gestionados.

Para obtener más información acerca de la revisión del estado de la garantía de los dispositivos gestionados (lo que incluye garantías extendidas), consulte Ver información de garantía en la documentación en línea de XClarity Administrator.

Paso 7. Opcionalmente, haga clic en **Servicio de boletín de Lenovo** permita que Lenovo envíe boletines de servicio a XClarity Administrator y haga clic en **Aplicar**

Para obtener más información sobre los tipos de boletines de servicio que envía Lenovo, consulte Obtención de boletines de Lenovo en la documentación en línea de XClarity Administrator.

Paso 8. Especifique la contraseña de recuperación de servicio que puede usar para recolectar y descargar datos de servicio y registros si XClarity Administrator deja de responder y no se puede recuperar.

Para obtener más información acerca de la contraseña de recuperación de servicio, consulte Cambio de la contraseña de recuperación de servicio en la documentación en línea de XClarity Administrator.

Paso 9. Haga clic en **Volver a la configuración inicial**.

Configurando la seguridad.

Puede configurar la seguridad, incluidos los grupos de roles, el servidor de autenticación, los valores de seguridad de la cuenta de usuario, la criptografía y los certificados.

Procedimiento

Lleve a cabo los pasos siguientes para configurar la seguridad.

Paso 1. En la página Configuración inicial, haga clic en **Configurar valores de seguridad adicionales**. Se muestra la página Seguridad.

Paso 2. Cree grupos de roles personalizados para gestionar la autorización y el acceso a los recursos (consulte Creación de un grupo de roles en la documentación en línea de XClarity Administrator).

Un *grupo de roles* es una colección de uno o varios roles que se utiliza para asignar esos roles a varios usuarios. Los roles que configure para un grupo de roles serán los que determinarán el nivel de acceso que se concede a cada usuario miembro de dicho grupo de roles. Cada usuario de XClarity Administrator debe ser miembro al menos de un grupo de roles.

Paso 3. Configure el servidor de autenticación (consulte Gestión del servidor de autenticación en la documentación en línea de XClarity Administrator).

El *servidor de autenticación* es un servidor con el Microsoft Active Directory (LDAP) que se utiliza para autenticar las credenciales de los usuarios. XClarity Administrator utiliza un solo servidor de autenticación para la gestión centralizada de usuarios en todos los dispositivos gestionados (excepto los conmutadores Flex). Cuando un dispositivos se gestiona mediante XClarity Administrator, el dispositivo gestionado y sus componentes instalados (excepto los conmutadores Flex) se configuran para utilizar el servidor de autenticación de XClarity Administrator. Las cuentas de usuarios que se definen en el servidor de autenticación se utilizan para iniciar sesión en XClarity Administrator, en los CMM y en los controladores de gestión de la placa base.

Si lo desea, puede elegir usar un servidor de autenticación externo en lugar del servidor de autenticación local en el nodo de gestión.

Paso 4. Configure los valores de seguridad de la cuenta de usuario, que controlan la complejidad de la contraseña, el bloqueo de la cuenta y el tiempo de espera por inactividad de la sesión web (consulte Cambio de los valores de seguridad de una cuenta de usuario en la documentación en línea de XClarity Administrator).

Paso 5. Configure los valores criptográficos, que definen los modos de comunicación y los protocolos que controlan la forma en la que se manejan las comunicaciones seguras entre XClarity Administrator y los dispositivos gestionados (consulte Configuración del modo criptográfico y los protocolos de comunicación en la documentación en línea de XClarity Administrator).

Paso 6. Si tiene planificado gestionar servidores de bastidor utilizando autenticación local en lugar de autenticación gestionada de XClarity Administrator, cree una o varias credenciales almacenadas que correspondan a cuentas de usuario activas en el dispositivo o en Active Directory que puedan utilizarse para iniciar sesión en los dispositivos durante el proceso de gestión. Para obtener más información sobre credenciales almacenadas, consulte Gestión de credenciales almacenadas en la documentación en línea de XClarity Administrator.

Paso 7. Si tiene pensado utilizar un certificado de servidor personalizado que incluya su propia información o utilizar un certificado firmado externamente, deberá generar y desplegar el certificado nuevo antes de empezar a gestionar los sistemas. Para obtener más información sobre cómo generar su propio certificado de seguridad, consulte Trabajo con certificados de seguridad en la documentación en línea de XClarity Administrator.

Paso 8. En el menú vertical de la página Seguridad, pulse **Volver a la configuración inicial**.

Gestión de dispositivos

Lenovo XClarity Administrator puede gestionar varios tipos de sistemas, incluido el chasis de Flex System, bastidores y servidores de torre, conmutadores RackSwitch y dispositivos de almacenamiento. Puede detectar y gestionar fácilmente una gran cantidad de dispositivos que están en su entorno importando información acerca de sus dispositivos mediante un archivo de importación masiva.

Antes de empezar

Importante:

- Puede gestionar o no gestionar un máximo de 300 dispositivos a la vez. No incluya más de 300 dispositivos en un archivo de importación masiva.
- Después de iniciar una operación de gestión o no gestión de dispositivos, espere a que se complete todo el trabajo de gestión antes de iniciar otra operación de gestión de dispositivos.

Los componentes del chasis (como CMM, nodos de cálculo, conmutadores y dispositivos de almacenamiento) se detectan y gestionan automáticamente cuando gestiona el chasis que los contiene. No puede detectar ni gestionar componentes del chasis de forma separada del chasis.

Algunos puertos deben estar disponibles para comunicarse con los CMM en el chasis y los controladores de gestión de la placa base de los servidores. Asegúrese de que estos puertos estén disponibles antes de intentar gestionar los sistemas. Para obtener más información sobre los puertos, consulte Disponibilidad de puertos.

Asegúrese de que el firmware mínimo necesario esté instalado en cada sistema que desee gestionar mediante XClarity Administrator. Encontrará los niveles de firmware mínimos requeridos del Soporte de XClarity Administrator: página web de compatibilidad haciendo clic en la pestaña **Compatibilidad** y, a continuación, pulsando el enlace de los tipos de dispositivo correspondientes.

Asegúrese de que hay al menos tres sesiones del modo de comando TCP para la comunicación fuera de banda con el CMM. Para obtener más información sobre la configuración del número de sesiones, consulte Comando tcpcmdmode en la documentación en línea de CMM.

Considere la posibilidad de implementar direcciones IPv4 *o* IPv6 para todos los CMM y conmutadores Flex que están gestionados mediante XClarity Administrator. Si implementa IPv4 para algunos CMM y conmutadores Flex e IPv6 para otros, puede que algunos sucesos no se reciban en el registro de auditoría (o como capturas de auditoría).

Asegúrese de habilitar el envío multidifusión SLP en los conmutadores de la parte superior del bastidor, así como en los direccionadores de su entorno. Consulte la documentación proporcionada con su conmutador o direccionador específicos para determinar si el envío multidifusión SLP está habilitado y para buscar los procedimientos para habilitarlo si está deshabilitado.

Importante:

- En función de la versión de firmware del conmutador RackSwitch, es posible que deba habilitar el reenvío multidifusión SLP y SSH en cada conmutador RackSwitch mediante los mandatos siguientes antes de que XClarity Administrator pueda descubrir y gestionar el conmutador. Para obtener más información, consulte el Documentación en línea de RackSwitch en System x.
- El reenvío de SLP de multidifusión debe estar habilitado en cada sistema de almacenamiento antes de que XClarity Administrator los pueda detectar.
- Si tiene pensado utilizar un certificado de servidor personalizado que incluya su propia información o utilizar un certificado firmado externamente, deberá generar y desplegar el certificado nuevo antes de

empezar a gestionar los sistemas. Para obtener más información sobre cómo generar su propio certificado de seguridad, consulte Trabajo con certificados de seguridad en la documentación en línea de XClarity Administrator.

- Si tiene pensado utilizar otro software de gestión además de Lenovo XClarity Administrator para supervisar sus chasis y ese software de gestión utiliza la comunicación SNMPv3, primero debe crear un Id. de usuario del CMM local que esté configurado con la información adecuada de SNMPv3 y, a continuación, iniciar sesión en el CMM utilizando ese Id. de usuario y cambiar la contraseña. Para obtener más información, consulte Consideraciones de gestión en la documentación en línea de XClarity Administrator.
- Los protocolos de detección del servicio, como SLP y SSDP, permiten que XClarity Administrator detecte automáticamente el tipo de dispositivo que se gestionará y que luego se utilice el mecanismo adecuado para gestionar el dispositivo. Algunos tipos de dispositivo no admiten los protocolos de detección del servicio y, en algunos entornos, los protocolos de detección del servicio están desactivados de manera intencional. En cualquier caso, debe elegir el tipo de dispositivo adecuado para completar el proceso de gestión. Los siguientes tipos de dispositivos deben identificarse de manera explícita.
  - Conmutador Lenovo ThinkSystem DB Series
  - Conmutador NVIDIA Mellanox

Acerca de esta tarea

XClarity Administrator puede descubrir sistemas en su entorno investigando si hay dispositivos gestionables que están en la misma subred IP que XClarity Administrator, utilizando una dirección IP especificada o un rango de direcciones IP o importando información desde una hoja de cálculo.

De forma predeterminada, los dispositivos se gestionan utilizando autenticación gestionada de XClarity Administrator para iniciar sesión en los dispositivos. Cuando se gestionan servidores de bastidor y chasis de Lenovo, puede optar por utilizar autenticación local o gestionada para iniciar sesión en los dispositivos.

- Cuando se utiliza la *autenticación local* para los servidores de bastidor, chasis de Lenovo y conmutadores de bastidor de Lenovo, XClarity Administrator usa una credencial almacenada para autenticar el dispositivo. La *credencial almacenada* puede corresponder con una cuenta de usuario activa en el dispositivo o con una cuenta de usuario en un servidor de Active Directory.

  Debe crear una credencial almacenada en XClarity Administrator que coincida con una cuenta de usuario activa en el dispositivo o una cuenta de usuario en un servidor de Active Directory antes de gestionar el dispositivo utilizando la autenticación local (consulte Gestión de credenciales almacenadas en la documentación en línea de XClarity Administrator).

  Notas:

  - Cuando se habilita la autenticación local para un dispositivo, no puede editar las credenciales almacenadas para dicho dispositivo utilizando XClarity Administrator.
  - Los dispositivos RackSwitch solo admiten credenciales almacenadas para la autenticación. Las credenciales de usuario de XClarity Administrator no se admiten.
- Usar la *autenticación gestionada* le permite gestionar y supervisar varios dispositivos utilizando las credenciales en el servidor de autenticación de XClarity Administrator en lugar las credenciales locales. Cuando un dispositivo se gestiona mediante autenticación gestionada (fuera de los servidores ThinkServer, System x M4 y conmutadores), XClarity Administrator configura el dispositivo gestionado y sus componentes instalados para utilizar el servidor autenticación de XClarity Administrator para la gestión centralizada de usuarios de todos los dispositivos.
  - Cuando se habilita la autenticación gestionada, puede gestionar dispositivos utilizando las credenciales ingresadas manualmente o almacenadas (consulte Gestión de cuentas de usuario y en la documentación en línea de XClarity Administrator).La credencial almacenada solo se utilizará hasta que

XClarity Administrator configure los valores de LDAP en el dispositivo. Después de eso, cualquier cambio de la credencial almacenada no tiene efecto la gestión o la supervisión de dicho dispositivo.

- Si se utiliza un servidor LDAP local o externo como el servidor de autenticación de XClarity Administrator, las cuentas de usuario que están definidas en el servidor de autenticación se utilizan para iniciar sesión en XClarity Administrator, en los CMM y en los controladores de gestión de la placa base del dominio de XClarity Administrator. Las cuentas de usuario del CMM local y del controlador de gestión están deshabilitadas.

  Nota: Para los servidores Think Edge SE450, SE350 V2 y SE360 V2, la cuenta de usuario local predeterminada permanece habilitada y el resto de las cuentas locales están deshabilitadas.

- Si se utiliza un proveedor de identidad SAML 2.0 como el servidor de autenticación de XClarity Administrator, los dispositivos gestionados no pueden acceder a las cuentas SAML. No obstante, cuando se utiliza un proveedor de identidad SAML y un servidor LDAP juntos, si el proveedor de identidad utiliza cuentas que existen en el servidor LDAP, las cuentas de usuario LDAP pueden utilizarse para iniciar sesión en los dispositivos gestionados, mientras que los métodos de autenticación más avanzados proporcionados por SAML 2.0 (como la autenticación de varios factores y el inicio de sesión único) pueden utilizarse para iniciar sesión en XClarity Administrator.
- El inicio de sesión único permite a un usuario que ya inició sesión en XClarity Administrator iniciar sesión automáticamente en el control de gestión de la placa base. El inicio de sesión único está habilitado de forma predeterminada cuando un servidor ThinkSystem o ThinkAgile se incluye en la gestión por XClarity Administrator (a menos que el servidor se esté gestionando con contraseñas de CyberArk). Puede configurar el valor global para habilitar o deshabilitar el inicio de sesión único en todos los servidores ThinkSystem y ThinkAgile gestionados. Habilitar el inicio de sesión único para un servidor ThinkSystem y ThinkAgile específico sustituye el valor global de todos los servidores ThinkSystem y ThinkAgile (consulte Gestión de servidores en la documentación en línea de XClarity Administrator).

  Nota: El inicio de sesión único se deshabilita automáticamente cuando se utiliza el sistema de gestión de identidades CyberArk para la autenticación.

- Cuando se habilita la autenticación gestionada para los servidores ThinkSystem SR635 y SR655:
  - El firmware del controlador de gestión de la placa base admite hasta cinco roles de usuario LDAP. XClarity Administrator añade estos roles de usuario LDAP a los servidores durante la gestión: **lxc-supervisor**, **lxc-sysmgr**, **lxc-admin**, **lxc-fw-admin** y **lxc-os-admin**.Los usuarios deben tener asignado al menos uno de los roles de usuario LDAP especificados para comunicarse con servidores ThinkSystem SR635 y SR655.
  - El firmware del controlador de gestión no admite usuarios LDAP que tengan el mismo nombre de usuario que el usuario local del servidor.
- Para servidores ThinkServer y System x M4, no se usa el servidor de autenticación de XClarity Administrator. Por el contrario, se crea una cuenta IPMI en el dispositivo con el prefijo “LXCA_” seguido de una cadena aleatoria. (Las cuentas de usuario de IPM local no se deshabilitan). Cuando anula la gestión de un servidor ThinkServer, se deshabilita la cuenta de usuario “LXCA_” y se sustituye el prefijo “LXCA_” con el prefijo “DISABLED_”. Para determinar si un servidor ThinkServer está gestionado por otra instancia, XClarity Administrator comprueba la existencia de cuentas IPMI con el prefijo “LXCA_”. Si elige forzar la gestión de un servidor ThinkServer gestionado, se deshabilitan todas las cuentas IPMI en el dispositivo con el prefijo “LXCA_” y cambian de nombre. Considere la posibilidad de borrar manualmente las cuentas IPMI que ya no se utilizan.

  Si usa credenciales ingresadas manualmente, XClarity Administrator crea automáticamente una credencial almacenada y usa esa credencial almacenada para gestionar el dispositivo.

  Notas: Cuando se habilita la autenticación gestionada para un dispositivo, no puede editar las credenciales almacenadas para dicho dispositivo utilizando XClarity Administrator.

- Cada vez que gestiona un dispositivo mediante las credenciales ingresadas manualmente, se crea una nueva credencial almacenad para ese dispositivo, incluso si se han creado otras credenciales almacenadas para ese dispositivo durante un proceso de gestión anterior.
- Cuando se anula la gestión de un dispositivo, XClarity Administrator no elimina las credenciales almacenadas que se crearon automáticamente para ese dispositivo durante el proceso de gestión.

Una vez que XClarity Administrator gestiona los sistemas, XClarity Administrator sondea periódicamente todos los sistemas gestionados para recopilar información, como el inventario, los datos de producto fundamentales y el estado. Puede consultar y supervisar cada sistema gestionado y realizar acciones de gestión (como configurar los valores del sistema, desplegar imágenes del sistema operativo y encenderlo y apagarlo).

Un sistema solo puede estar gestionado al mismo tiempo por un XClarity Administrator. La gestión por parte de varios gestores no es compatible. Si un sistema está gestionado por un XClarity Administrator y desea gestionarlo con otro XClarity Administrator, primero debe dejar de gestionar el sistema en el XClarity Administrator actual. A continuación, puede gestionar el sistema con otro XClarity Administrator. Para obtener información acerca de cómo anular la gestión de un sistema, consulte Anulación de la gestión de chasis, Anular la gestión de servidores y Dejar de gestionar un conmutador RackSwitch, Anular la gestión de un sistema de almacenamiento de Lenovo Storage en la documentación en línea de XClarity Administrator.

Nota: XClarity Administrator no modifica los valores de seguridad ni criptográficos (el modo criptográfico y el modo utilizado para comunicaciones seguras) durante el proceso de gestión. Puede modificar los valores criptográficos una vez gestionado el sistema (consulte Configuración del modo criptográfico y los protocolos de comunicación en la documentación en línea de XClarity Administrator).

Nota: XClarity Administrator se puede rellenar previamente con el inventario de hardware para un chasis de demostración (incluido CMM, nodos de cálculo y conmutadores) y un servidor de bastidores o de torre de demostración que simula el hardware real. Los dispositivos de demostración estén rellenados en las páginas de interfaz web y pueden utilizarse para mostrar las operaciones de gestión. Sin embargo, las operaciones de gestión producirán un error. Por ejemplo, puede crear un patrón de configuración y desplegar el patrón en un servidor de demostración, pero el despliegue producirá un error. Puede quitar los dispositivos de demostración al anular su gestión (consulte Anulación de la gestión de chasis y Anular la gestión de servidores en la documentación en línea de XClarity Administrator). Una vez eliminados los dispositivos de demostración, no se pueden volver a gestionar.

Procedimiento

Para detectar y gestionar sistemas en XClarity Administrator utilizando un archivo de importación masiva, lleve a cabo los siguientes pasos.

Nota: Cuando gestiona los conmutadores mediante una importación masiva, HTTPS está habilitado en el conmutador y los clientes NTP en el conmutador se configuran para utilizar la configuración de NTP desde el servidor de gestión. Para cambiar estos valores, debe gestionar manualmente los conmutadores.

1. En la barra de menús de XClarity Administrator, haga clic en **Hardware → Detectar y gestionar dispositivos nuevos**. Se muestra la página Detectar y gestionar.
2. Haga clic en la casilla de verificación **Habilitar encapsulación en todos los dispositivos gestionados futuros** para cambiar las reglas de firewall en todos los dispositivos durante el proceso de gestión para que solo se acepten las solicitudes entrantes de XClarity Administrator.

   Notas:

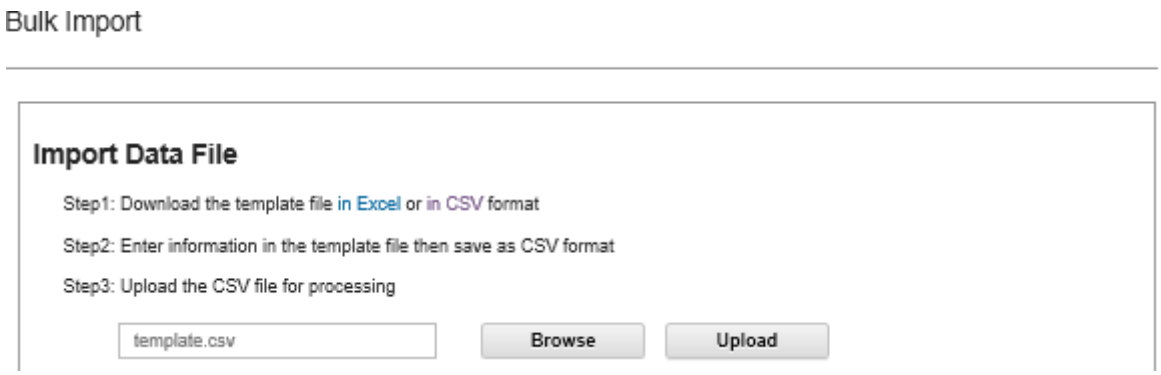
   - La encapsulación no es compatible en conmutadores, dispositivos de almacenamiento y chasis y servidores que no son de Lenovo.

- La gestión de un servidor de bastidor puede tardar bastante tiempo cuando la interfaz de red de gestión está configurada para utilizar el protocolo de configuración dinámica de host (DHCP) y cuando la encapsulación está habilitada.

La encapsulación se puede habilitar o deshabilitar en dispositivos específicos después de que se hayan gestionado.

Atención: Si se habilita la encapsulación y XClarity Administrator no está disponible antes de que se elimine la gestión de un dispositivo, se deben realizar algunos pasos para deshabilitar la encapsulación y establecer comunicación con el dispositivo. Para los procedimientos de recuperación, consulte el Recuperación de la gestión de chasis con un CMM después de un error en el servidor de gestión y Recuperación de la gestión de un servidor de bastidor o de torre después de un error de servidor de gestión en la documentación en línea de XClarity Administrator.

3. Haga clic en **Importación masiva**. Se muestra el cuadro de asistente de Importación masiva.



4. Haga clic en el enlace **en Excel** o **en CSV** en la página Importar archivo de datos para descargar el archivo de importación masiva de plantillas en el formato Excel o CSV.

Importante: El archivo de plantilla puede cambiar de una versión a la siguiente. Asegúrese de utilizar siempre la última plantilla.

5. Complete la hoja de cálculo de datos en el archivo de plantilla y guarde el archivo en formato CSV *delimitado por comas*.

Consejo: El archivo de plantilla de Excel incluye una hoja de cálculo **Datos** y una hoja de cálculo **Léame**. Utilice la hoja de cálculo **Datos** para rellenar los datos de dispositivo. La hoja de cálculo **Léame** proporciona información sobre cómo completar cada campo de la hoja de cálculo **Datos** (incluidos qué campos se requieren) y datos de muestra.

Importante:

- Los dispositivos se gestionan en el orden que se indica en el archivo de importación masiva.
- XClarity Administrator utiliza la información de asignación de bastidor que se define en la configuración del dispositivo cuando el dispositivo es gestionado. Si cambia la asignación del bastidor en XClarity Administrator, XClarity Administrator actualiza la configuración del dispositivo. Si actualiza la configuración del dispositivo después de gestionar el dispositivo, los cambios se reflejarán en XClarity Administrator.
- Aunque no se requiere, se recomienda crear explícitamente un bastidor en la hoja de cálculo antes de asignar el bastidor a un dispositivo. Si un bastidor no está definido explícitamente y el bastidor aún no existe en XClarity Administrator, la información designación de bastidor que se especifica para un dispositivo se uso para crear el bastidor con una altura predeterminada de 52U.

  Si desea utilizar otra altura para el bastidor, debe definir explícitamente el bastidor en la hoja de cálculo antes de asignarlo a un dispositivo.

Para definir sus dispositivos en el archivo de importación masiva, complete las siguientes columnas.

- (Columnas A a C) Para la detección básica, debe especificar el tipo de dispositivo y la dirección IP o el número de serie actuales para el dispositivo. Se admiten los tipos siguientes:
  - **filler**. Espacios reservados para un dispositivo no gestionado. En la vista de bastidores, este dispositivo se muestra como gráfico de relleno genérico. Consulte la hoja de cálculo **Readme** (Léame) en la plantilla de Excel para conocer los tipos de relleno adicionales.
  - **flexchassis**. 10U Flex System Chassis
  - **server**. Servidores de bastidor y de torre compatibles con XClarity Administrator
  - **rack**. Bastidores de 6U, 12U, 18U, 25U, 37U, 42U, 45U, 46U, 48U, 50U y 52U. No se admiten otras alturas de bastidor. El valor predeterminado utilizado es 52U.
  - **storage**. Dispositivos de almacenamiento
  - **switch**. Conmutadores RackSwitch

  Nota: Los nodos de cálculo, conmutadores y dispositivos de almacenamiento de Flex System se consideran como parte del proceso de detección y gestión del chasis.
- (Columnas D a H) Si elige utilizar credenciales introducidas manualmente en lugar de credenciales almacenadas (columnas Z) o identidad (Columnas AF a AJ), especifique el nombre de usuario y la contraseña actuales. Las credenciales ingresadas manualmente son útiles si las credenciales son distintas para algunos dispositivos. Si no especifica credenciales para uno o varios dispositivos en el archivo de importación masiva, se utilizan en su lugar las credenciales globales que especifique en el cuadro de diálogo Importación masiva. Para obtener más información sobre los usuarios ingresados y la autenticación gestionada, consulte Gestión de cuentas de usuario en la documentación en línea de XClarity Administrator.

  Notas:
  - Para utilizar las credenciales introducidas manualmente, debe seleccionar la autenticación gestionada de XClarity Administrator.
  - Algunos campos no corresponden a algunos dispositivos.
  - (Para chasis) Si seleccionó autenticación gestionada (en la columna AA o en el cuadro de diálogo Importación masiva), debe especificar una contraseña de `RECOVERY_ID` en la columna G del archivo de importación masiva o en el cuadro de diálogo Importación masiva. Si seleccionó autenticación local, no se permiten contraseñas de recuperación. No especifique una contraseña de recuperación en la columna G del archivo de importación masiva ni en el cuadro de diálogo Importación masiva.
  - (Para servidores de bastidor) Si seleccionó autenticación gestionada (en la columna AA o en el cuadro de diálogo Importación masiva), tiene la opción de especificar una contraseña de recuperación en la columna G del archivo de importación masiva o en el cuadro de diálogo Importación masiva. Si seleccionó autenticación local, no se permiten contraseñas de recuperación. No especifique una contraseña de recuperación en la columna G del archivo de importación masiva ni en el cuadro de diálogo Importación masiva.
  - (Para los conmutadores de bastidor) Los dispositivos RackSwitch solo admiten credenciales almacenadas (en la columna Z) para autenticar a los conmutadores. No se admiten las credenciales de usuario manuales.
- (Columnas I a U) Opcionalmente, puede proporcionar información adicional si desea aplicar cambios al dispositivo después de una gestión correcta.

  Nota: Algunos campos no corresponden a algunos dispositivos. Estos campos no se aplican a los conmutadores RackSwitch.

- (Columnas V a Z) Opcionalmente, puede proporcionar información para la creación de bastidores y asignación, incluido el nombre de bastidor, la ubicación, la habitación, la unidad de bastidor más baja y la altura.

  Notas:

  – Cuando se crea un bastidor, debe especificar el nombre y la altura del bastidor. Se admiten las siguientes alturas de bastidor: Bastidores de 6U, 12U, 18U, 25U, 37U, 42U, 45U, 46U, 48U, 50U y 52U. No se admiten otras alturas de bastidor.

  – Cuando se crea un rellena genérico, debe especificar el nombre y la altura del relleno. Se admiten las siguientes alturas de rellenos: 1U, 2U y 4U.

  – Al crear un relleno específico, se omite la altura de relleno. XClarity Administrator conoce la altura de cada relleno específico. Consulte la hoja de cálculo de la plantilla para los tipos de relleno y su altura.

  – Cuando se asigna un dispositivo al bastidor, se omite la altura del dispositivo. La altura del dispositivo se recupera desde el inventario de dispositivos.

- (Columna AA) Si no se realizó correctamente la gestión debido a una de las siguientes condiciones de error, repita este proceso mediante la opción de forzar gestión.

  – Si la gestión de XClarity Administrator produjo un error y no se puede recuperar.

    Nota: Si la instancia de sustitución de XClarity Administrator utiliza la misma dirección IP que la instancia de XClarity Administrator que ha producido el error, puede volver a gestionar el dispositivo utilizando la cuenta y la contraseña del RECOVERY_ID (si corresponde) y la opción Forzar gestión.

  – Si la gestión de XClarity Administrator se desactivó antes de que se anulara la gestión de los dispositivos.

  – Si no se anuló correctamente la gestión de los dispositivos.

  Los dispositivos solo pueden estar gestionados al mismo tiempo por una instancia de XClarity Administrator. La gestión por parte de varias instancias de XClarity Administrator no es compatible. Si un dispositivo está gestionado por un XClarity Administrator y desea gestionarlo con otro XClarity Administrator, primero debe dejar de gestionar el dispositivo de almacenamiento en el XClarity Administrator inicial y luego gestionarlo con el nuevo XClarity Administrator.

  Importante: Si cambia la dirección IP de un servidor después de que el servidor está gestionado por XClarity Administrator, XClarity Administrator reconoce la nueva dirección IP y continúa gestionando el servidor. Sin embargo, XClarity Administrator no reconoce el cambio de dirección IP para algunos servidores. Si XClarity Administrator muestra que el servidor está fuera de línea después de que se modificara la dirección IP, gestione el servidor nuevamente mediante la opción Forzar gestión.

- (Columnas AB) Si elige utilizar las credenciales almacenadas en lugar de las credenciales ingresadas manualmente (columnas D a H) o identidad (Columnas AF a AJ), especifique el ID de la credencial almacenada. Puede encontrar el Id. de credencial almacenado en la página Credenciales almacenadas al hacer clic en **Administración → Seguridad** desde el menú XClarity Administrator y, a continuación, al hacer clic en **Credenciales almacenadas** en la barra de navegación izquierda. Para obtener más información sobre credenciales almacenadas y la autenticación local, consulte Gestión de credenciales almacenadas en la documentación en línea de XClarity Administrator.

  Notas:

  – Los dispositivos RackSwtich solo admiten credenciales almacenadas para la autenticación. No se admiten credenciales de usuario manuales (en la columna D).

  – Si gestiona un dispositivo utilizando las credenciales almacenadas y habilita la autenticación gestionada, no puede editar las credenciales almacenadas.

- (Columna AC) Para chasis y servidores de bastidor, si elige usar la autenticación gestionada (en la columna AA o en el cuadro de diálogo Importación masiva), debe especificar una contraseña de RECOVERY_ID en la columna G del archivo de importación masiva o en el cuadro de diálogo Importación masiva. Si seleccionó autenticación local, no se permiten contraseñas de recuperación. No especifique una contraseña de recuperación en la columna G del archivo de importación masiva ni en el cuadro de diálogo Importación masiva.
- (Columna AD) Para los servidores de bastidor, puede optar por utilizar la autenticación local en lugar de la autenticación gestionada de XClarity Administrator al especificar FALSE en esta columna. Para obtener más información acerca de autenticación gestionada y local, consulte Gestión del servidor de autenticación en la documentación en línea de XClarity Administrator.
- (Columna AE) Opcionalmente, puede especificar una lista de grupos de roles que pueden ver y gestionar el dispositivo. Solo puede especificar grupos de roles a los que pertenece el usuario actual.

  Nota: Si agrega dispositivos en un chasis gestionado, los nuevos dispositivos pertenecen a los mismos grupos de roles que el chasis.
- (Columnas AF a AJ) Si elige utilizar un sistema de gestión de identidad en lugar de credenciales introducidas manualmente (columnas D a H) o credenciales almacenadas (columnas AB), especifique la dirección IP o el nombre de host del servidor gestionado, el nombre de usuario y, opcionalmente, el ID de la aplicación, la seguridad y la carpeta.

  Si especifica el ID de aplicación, también debe especificar el seguro y la carpeta, si corresponde.

  Si no especifica el ID de la aplicación, XClarity Administrator utiliza las rutas que se definieron al configurar CyberArk para identificar las cuentas incorporadas en CyberArk (consulte Configuración de un sistema de gestión de identidades CyberArk en la documentación en línea de XClarity Administrator).

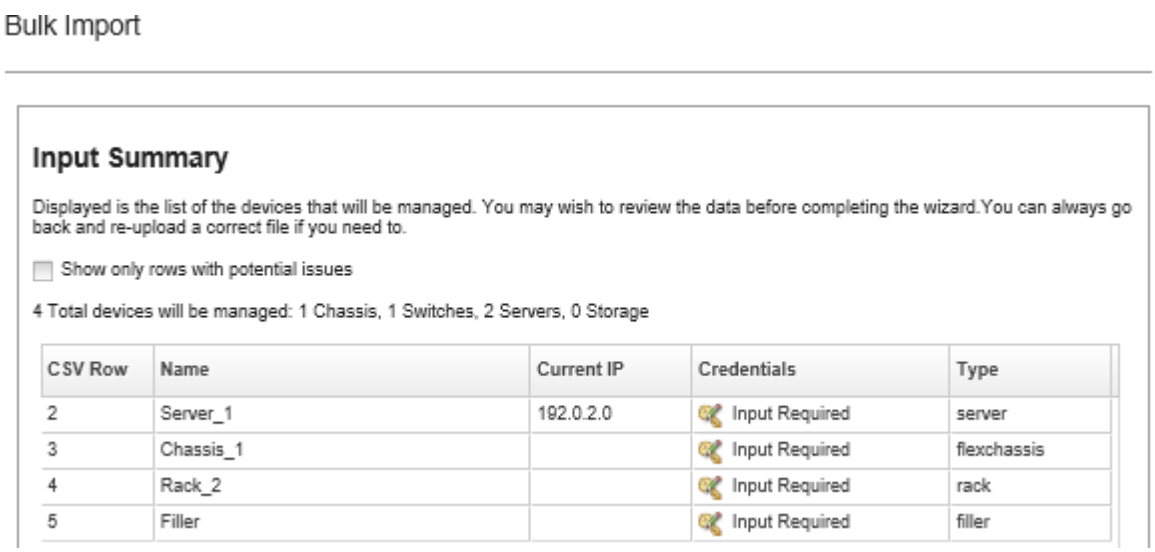
  Nota: Solo se admiten los servidores ThinkSystem o ThinkAgile. El sistema de gestión de identidades se debe configurar en XClarity Administrator y Lenovo XClarity Controller para los servidores gestionados ThinkSystem o ThinkAgile se debe integrar con CyberArk (consulte Configuración de un sistema de gestión de identidades CyberArk en la documentación en línea de XClarity Administrator).

En la figura siguiente se muestra un ejemplo del archivo de importación masiva:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
Required fields (Type + SN or IP)								Optional fields										
Type	Serial Number	Current IP	Current username	Current password	New password	Recovery password	Switch enable password	New IPv4	IPv4 subnet mask	IPv4 default gateway	IPv4 DNS1	IPv4 DNS2	New IPv6	IPv6 prefix	IPv6 gateway	IPv6 DNS1	IPv6 DNS2	Domain
server		10.1.0.198																
server	P67X30EL																	
flexchassis		10.1.0.213	USERID	passw0rdx	Pa55word@	abcd1234												
flexchassis	Z3499DD				Pa55word@	abcd1234		9.27.20.51	255.255.255.0	9.27.20.1	9.0.148.50	9.0.146.50						ebg.lenovo.com
server	35T88XP												2002:939	2002:9:	2002:939:	2002:9:	2002:9	ebg.lenovo.com
server		10.1.0.214						10.1.2.213	255.255.255.0	10.1.2.1	9.0.148.50	9.0.146.50						ebg.lenovo.com
rack																		
rack																		
filler																		
filler																		
filler																		

R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG	AH	AI	AJ
IPv6 DNS2	Domain	Host name	User-defined name	Rack name	Location	Room	Lowest rack unit	Height	Force	Stored credentials ID	Stored credentials ID for RECOVERY_ID	Managed authentication	Role Groups	IdentityManagementSystemEnabled	IMS type	IMS AppID	Folder	Safe
														TRUE	CyberArk	LXCA		Test
			chassis03	SH3G05A34			25		TRUE									
	ebg.lenovo.com	chassis01	chassis01	SH3G05A34			5											
2002:9	ebg.lenovo.com	host4	c02node01	SH3G05B12			38			2	3	FALSE						
	ebg.lenovo.com	host5	web02	SH3G05B12			10											
			SG2R01A01					37										
			SH3G05A34					46										
			APC UPS	SH3G05A34			1	4										
			FC switch	SH3G05A34			40	2										
			KVM switch	SH3G05B12			22	1										

6. Desde el asistente de Bulk Import (Importación masiva), introduzca el nombre del archivo CSV para cargar el archivo de procesamiento. Puede hacer clic en **Examinar** para buscar el archivo.
7. Haga clic en **Cargar** para cargar y validar el archivo.
8. Haga clic en **Siguiente** para mostrar la página de resumen de entrada con una lista de dispositivos a gestionar.

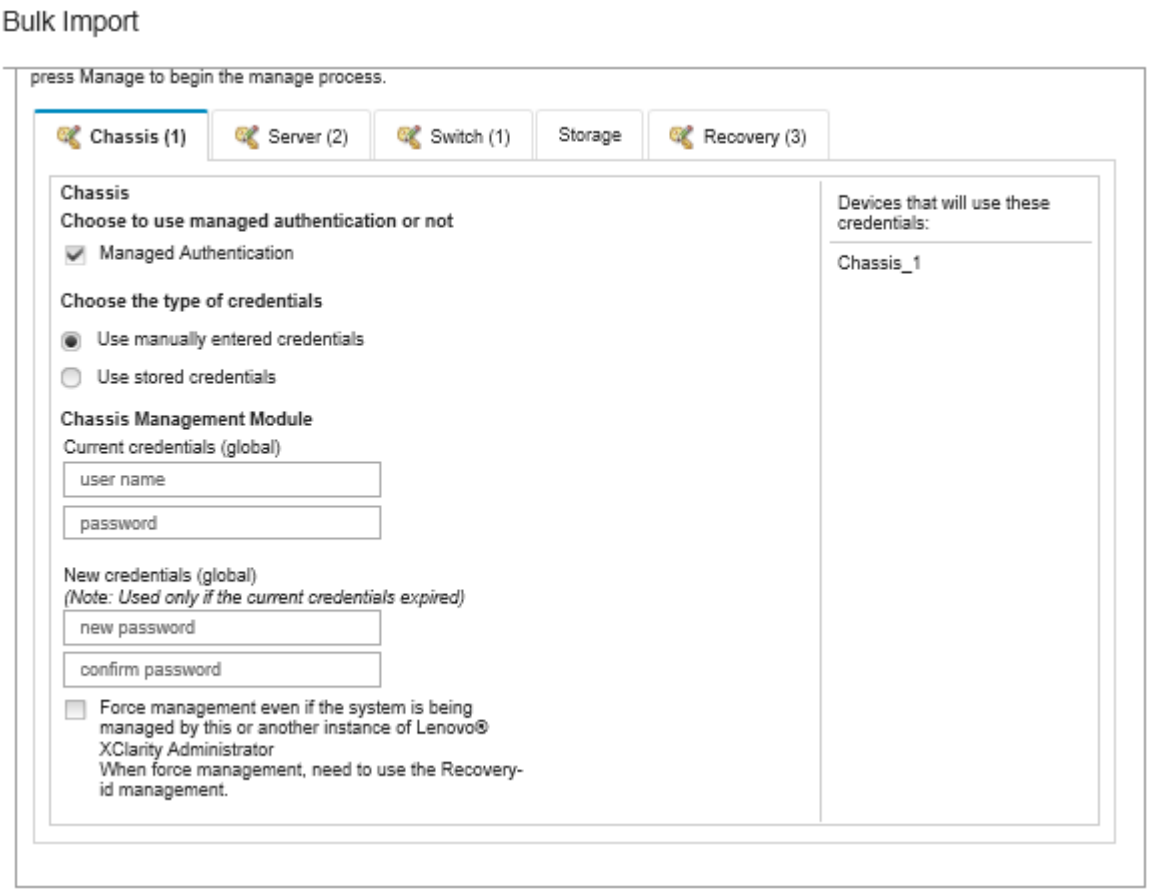


9. Revise el resumen de los dispositivos que desea gestionar.

   Seleccione **Mostrar solo filas con posibles problemas** para listar las filas con datos incompletos. Corrija los problemas en el archivo de importación masiva y haga clic en **Atrás** para cargar un archivo CSV corregido.

   Notas:

   - Si los datos necesarios no se incluyen en el archivo de importación masiva, los dispositivos asociados no se gestionan.
   - La página Resumen de entrada marca las filas que no tienen información de credenciales. Si no especifica credenciales en el archivo de importación masiva, se utilizan en su lugar las credenciales globales que especifique en el asistente de Importación masiva.
10. Haga clic en **Siguiente** para mostrar la página de Credenciales del dispositivo.



11. **Opcional:** haga clic en cada pestaña y, opcionalmente, especifique los valores globales y las credenciales que se utilizarán para todos los dispositivos de un tipo específico. Se muestran los dispositivos que utilizarán los valores globales y las credenciales en el lado derecho de cada pestaña.

    Si elige utilizar las credenciales globales, las credenciales para un tipo de dispositivo específico deben ser las mismas para todos los dispositivos del mismo tipo que no tienen credenciales especificadas en el archivo de importación masiva. Por ejemplo, las credenciales del CMM deben ser iguales para todos los chasis iguales y las credenciales de gestión de almacenamiento deben ser iguales para todos los dispositivos de almacenamiento. Si las credenciales no son las mismas, debe especificar las credenciales en el archivo de importación masiva.

    - **Chasis**. Especifique el tipo de modo y las credenciales de autenticación. Especifique las credenciales actuales para iniciar sesión en todos los chasis que se enumeran en el archivo de importación masiva. Especifique la contraseña nueva por utilizar si caducaron las credenciales actuales de CMM.

      Si gestiona un chasis a la fuerza, especifique la cuenta y la contraseña de RECOVERY_ID para las credenciales del dispositivo.
    - **Servidores**. Especifique el tipo de modo y las credenciales de autenticación. Especifique las credenciales actuales para iniciar sesión en todos los servidores de bastidor y de torre que se enumeran en el archivo de importación masiva. Especifique la contraseña nueva por utilizar si caducaron las credenciales actuales del controlador de gestión de placa base.

      Si gestiona un servidor a la fuerza, especifique la cuenta y la contraseña de RECOVERY_ID para las credenciales del dispositivo.
    - **Conmutadores**. Especifique las credenciales almacenadas para iniciar sesión en todos los conmutadores RackSwitch que se enumeran en el archivo de importación masiva. Si está habilitado, también especifique la contraseña para “habilitar” que se usa para ingresar a Privileged Exec Mode en el conmutador.

- **Storage**. Especifique las credenciales actuales para iniciar sesión en todos los dispositivos de almacenamiento que se enumeran en el archivo de importación masiva.
- **Recuperación**. Especifique la contraseña de recuperación para iniciar sesión en todos los servidores chasis que se enumeran en el archivo de importación masiva.

  Puede elegir utilizar una cuenta de usuario local o una credencial de recuperación almacenada. En cualquier caso, el nombre de usuario siempre es `RECOVERY_ID`.

  Al especificar una contraseña, se crea la cuenta `RECOVERY_ID` en el dispositivo y se deshabilita todas las cuentas de usuario locales.

  – Para los chasis, se requiere la contraseña de recuperación.
  – Para los servidores, está disponible la opción de contraseña de recuperación si seleccionó autenticación gestionada. Esta opción no está permitida si seleccionó autenticación local.
  – Asegúrese de crear una contraseña que siga las políticas de seguridad y de contraseña del dispositivo. Las políticas de seguridad y de contraseña pueden variar.
  – Asegúrese de guardar la contraseña de recuperación para utilizarla en el futuro.
  – Los servidores ThinkServer y System x M4 no admiten cuentas de recuperación.

La información que especifica en el archivo de importación masiva sobrescribe la información similar que especifique en la página de Credenciales de dispositivo.

Opcionalmente, puede elegir forzar la gestión de cada tipo de dispositivo si:

- Actualmente, otro sistema de gestión gestiona los dispositivos, como otra instancia de XClarity Administrator o IBM Flex System Manager
- Se desactivó XClarity Administrator, pero no se anuló la gestión de los dispositivos antes de desactivarlo
- No se anuló correctamente la gestión de los dispositivos y no se borró la suscripción de CIM

Nota: Si la gestión del dispositivo la realiza otra instancia de XClarity Administrator, parece que el dispositivo lo gestiona la instancia original por un período de tiempo después de que se produzca la gestión forzada. Puede anular la gestión del dispositivo para quitarlo de la instancia original de XClarity Administrator.

12. Haga clic en **Gestionar**. Se muestra la página de Resultados de supervisión con información sobre el estado de la gestión de cada dispositivo en el archivo de importación masiva.

    Se crea un trabajo para el proceso de gestión. Si cierra al asistente de Importación masiva, el proceso de gestión continúa ejecutándose en segundo plano. Puede supervisar el estado del proceso de gestión desde el registro de trabajos. Para obtener más información acerca del registro de trabajos, consulte Supervisión de trabajos en la documentación en línea de XClarity Administrator.

    Si XClarity Administrator no puede iniciar sesión en un dispositivo utilizando las credenciales especificadas en el archivo de importación masiva o las credenciales globales especificadas en el cuadro de diálogo, la gestión de dicho dispositivo produce un error y XClarity Administrator se desplaza al siguiente dispositivo del archivo de importación masiva.

    Notas: Si no se realizó correctamente la gestión debido a una de las siguientes condiciones de error, repita este proceso mediante la opción **Forzar gestión**.

    - Si la gestión de XClarity Administrator produjo un error y no se puede recuperar.

      Nota: Si la instancia de sustitución de XClarity Administrator utiliza la misma dirección IP que la instancia de XClarity Administrator que ha producido el error, puede volver a gestionar el dispositivo utilizando la cuenta y la contraseña del RECOVERY_ID (si corresponde) y la opción **Forzar gestión**.

- Si la gestión de XClarity Administrator se desactivó antes de que se anulara la gestión de los dispositivos.
- Si no se anuló correctamente la gestión de los dispositivos.

Atención: Los dispositivos solo pueden estar gestionados al mismo tiempo por una instancia de XClarity Administrator. La gestión por parte de varias instancias de XClarity Administrator no es compatible. Si un dispositivo está gestionado por un XClarity Administrator y desea gestionarlo con otro XClarity Administrator, primero debe dejar de gestionar el dispositivo de almacenamiento en el XClarity Administrator inicial y luego gestionarlo con el nuevo XClarity Administrator.

13. Si el archivo de importación masiva incluye un chasis nuevo, valide y cambie los valores de la red de gestión de todo el chasis (incluidos los nodos de cálculo y los conmutadores Flex) y configure la información del nodo de cálculo, el almacenamiento local, los adaptadores de E/S, los destinos de arranque y los valores de firmware creando y desplegando patrones de servidor. Para obtener más información, consulte Modificación de los valores IP de gestión de un chasis y Configuración de servicios usando XClarity Administrator en la XClarity Administrator documentación en línea.

Después de finalizar

Después de gestionar sus sistemas, puede realizar las acciones siguientes:

- Detecte y gestione sistemas adicionales (consulte Gestión del chasis, Gestión de bastidores, Gestión de servidores, Gestión de los dispositivos de almacenamiento y Gestión de conmutadores en la documentación en línea de Lenovo XClarity Administrator).
- Configure la información del sistema, así como el almacenamiento local, los adaptadores de E/S, los valores de arranque y los valores de firmware, creando y desplegando patrones del servidor (consulte Configuración de servicios usando XClarity Administrator en la documentación en línea de Lenovo XClarity Administrator).
- Despliegue imágenes del sistema operativo en los servidores que todavía no tienen un sistema operativo instalado (consulte Despliegue de la imagen de un sistema operativo en la documentación en línea de XClarity Administrator).
- Actualice el firmware de los dispositivos que no cumplen las políticas actuales (consulte Actualización de firmware en dispositivos gestionados en la documentación en línea de XClarity Administrator).
- Añada los sistemas recién gestionados al bastidor adecuado para reflejar el entorno físico (consulte Gestión de bastidores en la documentación en línea de XClarity Administrator).
- Supervise el estado y los detalles de hardware (consulte Visualización del estado de un servidor gestionado en la documentación en línea de XClarity Administrator).
- Supervise los sucesos y las alertas (consulte Trabajo con sucesos y Trabajo con alertas en la documentación en línea de XClarity Administrator).
- Deshabilitar o habilitar el inicio de sesión único para los servidores gestionados ThinkSystem y ThinkAgile.
  - Para todos los servidores ThinkSystem y ThinkAgile gestionados (globalmente), haga clic en **Gestión → Seguridad** desde la barra de menú de XClarity Administrator, haga clic en **Sesiones activas** y habilite o deshabilite el **inicio de sesión único**.
  - Para un servidor ThinkSystem y ThinkAgile específico, haga clic en **Hardware → Servidor** desde la barra de menú de XClarity Administrator y, a continuación, haga clic en **Todas las acciones → Seguridad → Habilitar inicio de sesión único** o **Todas las acciones → Seguridad → Deshabilitar inicio de sesión único**.

Nota: El inicio de sesión único permite a un usuario que ya inició sesión en XClarity Administrator iniciar sesión automáticamente en el control de gestión de la placa base. El inicio de sesión único está habilitado de forma predeterminada cuando un servidor ThinkSystem o ThinkAgile se incluye en la gestión por XClarity Administrator (a menos que el servidor se esté gestionando con contraseñas de CyberArk). Puede configurar el valor global para habilitar o deshabilitar el inicio de sesión único en todos los

servidores ThinkSystem y ThinkAgile gestionados. Habilitar el inicio de sesión único para un servidor ThinkSystem y ThinkAgile específico sustituye el valor global de todos los servidores ThinkSystem y ThinkAgile.

Capítulo 5. Registro de XClarity Administrator

Al registrar la instancia de Lenovo XClarity Administrator, puede utilizar las funciones básicas sin recibir advertencias recurrentes sobre la caducidad de la versión de prueba y las licencias no compatibles. Después del registro, deja de aparecer la advertencia de licencia no compatible. Sin embargo, todas las funciones que requieren de una licencia se mantienen deshabilitadas hasta que adquiere e instala licencias en función de la cantidad de dispositivos gestionados.

Acerca de esta tarea

El registro de la instancia de XClarity Administrator no requiere que comparta su información de contacto. Lenovo no comparte la información proporcionada con otras entidades externas.

Si ha instalado licencias para funciones avanzadas, no es necesario que registre su instancia de XClarity Administrator. Para obtener más información acerca de las licencias y las funciones avanzadas, consulte Instalación de licencia de habilitación de funciones completas.

Procedimiento

Lleve a cabo los pasos siguientes para registrar XClarity Administrator.

- Si XClarity Administrator está conectado a Internet
  1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Administración → Registro** para mostrar la página Registro.
  2. Haga clic en **Registrar** para registrar una nueva instancia de XClarity Administrator.
  3. Llene el nombre de la empresa, la cantidad de dispositivos que gestionará XClarity Administrator y el país en el que se encuentra XClarity Administrator.
  4. Haga clic en **Enviar**.
- Si XClarity Administrator no está conectado a Internet
  1. Registre XClarity Administrator.
     a. En un navegador web, abra Portal web de registro de Lenovo XClarity.
     b. Llene el nombre de la empresa, la cantidad de dispositivos que gestionará XClarity Administrator y el país en el que se encuentra XClarity Administrator.
     c. Haga clic en **Enviar** para recibir un token de registro.
  2. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Administración → Registro** para mostrar la página Registro.
  3. Haga clic en el icono **Importar** para importar el token de registro.
  4. Llene el token de registro que recibió en el paso 1.
  5. Haga clic en **Enviar**.

Capítulo 6. Instalación de licencia de habilitación de funciones completas

Después de que caduque la versión de prueba gratuita de 90 días, debe adquirir e instalar las licencias de Lenovo XClarity Pro para todos los dispositivos administrados que admiten funciones avanzadas para seguir utilizando las características de implementación de sistema operativo y configuración de dispositivos en Lenovo XClarity Administrator. Debe disponer de Lenovo XClarity Pro licencias para *todos* los dispositivos gestionados con el fin de obtener el servicio y soporte de XClarity Administrator.

Antes de empezar

Más información: XClarity Administrator: Instalación de la licencia

Revise las consideraciones de licencia siguientes.

- Una licencia *no está* vinculada a un dispositivo específico.
- 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 Administrator.
  - Servidores ThinkServer
  - Servidores System x M4
  - Servidores System x X5
  - Servidores System x3850 X6 y x3950 X6 (3837)
  - Dispositivos de almacenamiento
  - Conmutadores

Debe tener privilegios de **lxc-supervisor** o **lxc-security-admin** para instalar licencias.

Acerca de esta tarea

XClarity Administrator es compatible con la siguiente licencia.

- **Lenovo XClarity Pro**. Cada licencia proporciona los siguientes derechos para un único dispositivo.
  - Servicio técnico y soporte para Lenovo XClarity Integrator
  - Servicio técnico y soporte para XClarity Administrator
  - Funciones avanzadas dentro de XClarity Administrator:
    - Configuración de servidores mediante el uso de patrones de configuración
    - Despliegue de sistemas operativos
    - Informar a los problemas de XClarity Administrator mediante la función Llamar a casa (Llamar a casa para las alertas de hardware no se ve afectada).

El período de activación de la licencia se inicia cuando se adquiere la licencia y se crea el código de autorización.

El cumplimiento de la licencia se determina en función del número de dispositivos administrados que admiten las funciones avanzadas. El número de dispositivos administrados no debe superar el número de licencias en todas las claves de licencia activas. Si XClarity Administrator no cumple con las licencias instaladas (por ejemplo, si las licencias caducan o si la administración de dispositivos adicionales supera el número total de licencias activas), tiene un período de gracia de 90 días para instalar las licencias adecuadas. Cada vez que XClarity Administrator pasa a no estar en cumplimiento, el periodo de gracia se restablece a 90 días. Si el periodo de gracia (incluida la prueba gratuita) finaliza antes de que se cumplan las licencias, las funciones avanzadas están deshabilitadas para todos los dispositivos.

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

Si está utilizando una licencia de evaluación gratuita o tiene un periodo de gracia para cumplir con la norma y actualiza a una versión posterior de XClarity Administrator, la licencia de evaluación o el periodo de gracia se restablecen a 90 días.

Notas:

- Las características de configuración del servidor y de despliegue del sistema operativo se deshabilitan cuando finaliza el periodo de gracia.
- La función Llamar a casa para los problemas de XClarity Administrator (la característica Llamar a casa de software) está deshabilitada cuando las licencias están fuera de conformidad. No hay un periodo de gracia para esta función. Sin embargo, la función Llamar a casa para las alertas de hardware no se ve afectada.

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

Puede determinar el estado de la licencia, incluido el número de días quedan de la licencia de prueba, al hacer clic en el menú de acciones del usuario (

) en la barra de título de XClarity Administrator y, después, al hacer clic en **Acerca de**.

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 (países de Norteamérica)
  - ESDAP@lenovo.com (países de Asia-Pacífico)
  - ESDEMEA@lenovo.com (países de Europa, Medio Oriente y Asia)
  - ESDLA@lenovo.com (países de Latinoamérica)
  - ESDChina@Lenovo.com (China)
- Si la información acerca de la autorización no es correcta, póngase en contacto con el Soporte de Lenovo a 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.

Instalación de licencias de habilitación de funciones completas mediante la interfaz de web de XClarity Administrator

Si XClarity Administrator tiene acceso a Internet, puede usar la interfaz de web de XClarity Administrator para obtener y recuperar licencias para la autorización existente y, a continuación, importar e instalar las licencias canjeadas.

Antes de empezar

Póngase en contacto con su representante de Lenovo o socio comercial autorizado para comprar licencias de Lenovo XClarity Pro en función de las funciones que desea habilitar y el número de dispositivos que desea administrar. Después de comprar licencias, se le envía un código de autorización en un *correo electrónico de prueba de derecho*. El código de autorización es una cadena alfanumérica de 22 caracteres, que debe tener en cuenta e instalar las licencias. Si no recibe el correo electrónico y compró licencias mediante un Business Partner, póngase en contacto con su Business Partner para solicitar el código de autorización.

También puede recuperar sus códigos de autorización de Características del portal web on Demand, haciendo clic en **Recuperar el código de autorización**.

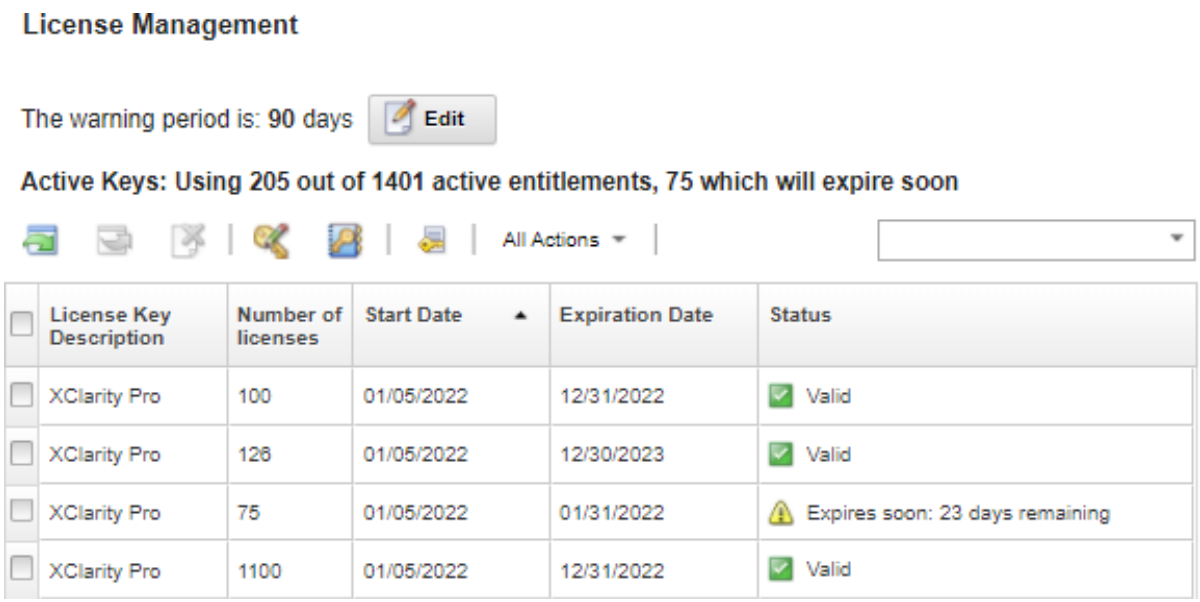
Procedimiento

Para instalar licencias de Lenovo XClarity Pro en el servidor de gestión, realice uno de los procedimientos siguientes.

- **Canjee e instale todas las licencias restantes o un subconjunto de ellas desde un solo código de autorización**

  Puede crear todas o un subconjunto de licencias disponibles para un solo código de autorización con el fin de crear una clave de activación de licencia, que es un archivo que contiene cada información acerca de la licenciada. A continuación, puede instalar las licencias canjeadas utilizando ese archivo de clave de activación de licencia.

  1. En la barra de menús de XClarity Administrator, haga clic en **Administración → Licencias** para mostrar la página Administración de licencias.



2. Haga clic en el icono **Solicitar clave de activación** ( ) para mostrar el cuadro de diálogo Solicitar clave de activación.
3. Haga clic en **Código de autorización único**.
4. Introduzca el código de autorización de 22 caracteres y haga clic en **Buscar** para obtener información sobre las licencias compradas para el código de autorización especificado desde el sitio web de Features on Demand.

   Si no se acepta el código de autorización que recibió, póngase en contacto del soporte con Lenovo.
5. Introduzca el número de cliente de 10 dígitos 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 este código de autorización, haga coincidir el número en el campo **Licencias disponibles**.

   Si canjea un subconjunto de licencias disponibles, puede canjear el resto de las licencias más tarde utilizando el mismo código de autorización.

   Consejo: cada XClarity Administrator admite hasta 1.000 dispositivos administrados. Por lo tanto, una clave de activación de licencia única puede instalar en una instancia de XClarity Administrator no puede tener más de 1.000 licencias.
7. Revise la información de contacto para ver la exactitud y realice modificaciones si es necesario.
8. Haga clic en **Enviar solicitud** para crear las licencias y crear la clave de activación de la licencia.
9. Seleccione la clave de activación de la licencia que contiene las licencias para instalar.
10. Haga clic en **Instalar** para instalar las licencias en el servidor de gestión.
11. Haga clic en **Cerrar**.

- **Canjee e instale todas las licencias restantes de varios códigos de autorización**

  Puede canjear todas las licencias restantes de varios códigos de autorización. Se crea una clave de activación de licencia para cada código de autorización. A continuación, puede instalar las licencias canjeadas utilizando las claves de activación de licencia. Los códigos de autorización deben proporcionarse en un archivo con formato CSV, utilizando la plantilla proporcionada.

  1. En la barra de menús de XClarity Administrator, haga clic en **Administración → Licencias** para mostrar la página Administración de licencias.

2. Haga clic en el icono **Solicitar clave de activación** () para mostrar el cuadro de diálogo Solicitar clave de activación.
3. Haga clic en **Varios códigos de autorización**.
4. Haga clic en el enlace **Descargar plantilla** para abrir un archivo de Excel. Añada cada código de autorización al archivo y guarde el archivo en formato CSV en su sistema local.
5. Haga clic en **Examinar** para buscar y seleccionar el archivo CSV del código de autorización y, a continuación, haga clic en **Buscar** para obtener información sobre el código de autorización del sitio web del soporte de Lenovo.
6. Revise la información acerca de la licencia adquirida y las claves de activación de licencia disponibles que están asociadas con cada código de autorización.
7. Introduzca el número de cliente de 10 dígitos de Lenovo en el campo **Número de cliente de Lenovo**.
8. Revise la información de contacto para ver la exactitud y realice modificaciones si es necesario. A continuación, haga clic en **Continuar**.
9. Seleccione **Sí, quiero canjear los códigos de autorización válidos** y, a continuación, haga clic en **Enviar solicitud** para generar las claves de activación de licencia.
10. Seleccione las claves de activación de licencia que desea instalar.
11. Haga clic en **Instalar** para instalar las claves de activación de licencia en el servidor de gestión.
12. Haga clic en **Cerrar**.

- **Recuperación e instalación de licencias licenciadas canjeadas**

  Puede descargar las claves de activación de licencia en el sistema local desde una instancia de XClarity Administrator que tenga acceso a la instancia de Características del portal web on Demand y, a continuación, importar e instalar dichas claves de activación de licencia en otra instancia de XClarity Administrator. Esto resulta útil cuando desea instalar licencias en una instancia de XClarity Administrator que no tiene acceso a Internet o cuando se vuelve a instalar XClarity Administrator y tiene que restaurar las licencias instaladas.

  1. En la barra de menús de XClarity Administrator, haga clic en **Administración → Licencias** para mostrar la página Administración de licencias.
  2. Haga clic en el icono **Recuperar historial** () para mostrar el cuadro de diálogo Recuperar historial.
  3. Introduzca el número de cliente de Lenovo o el código de autorización de 22 caracteres.
  4. Haga clic en **Buscar** para recuperar información acerca de las licencias disponibles y canjeadas.

     Si no se acepta el código de autorización que recibió, póngase en contacto del soporte con Lenovo.
  5. Seleccione los archivos de clave de licencia que desea instalar.
  6. Haga clic en **Instalar** para instalar las claves de activación de licencia en XClarity Administrator.
  7. Haga clic en **Cerrar**.

- **Importar e instalar licencias canjeadas en otra instancia de XClarity Administrator**

  Si tiene licencias licencia licenciadas por medio de una instancia de XClarity Administrator y desea instalar estas en otra instancias de XClarity Administrator o si se produce una condición de error que requiere que restaure las licencias instaladas, puede importar el archivo de clave de licencia desde el sistema local a la otra instancia de XClarity Administrator.

  1. Desde una instancia de XClarity Administrator que tiene acceso a Características del portal web on Demand, recupere las claves de activación de licencia de Características del portal web on Demand y, a continuación, guarde las claves de activación de licencia como un archivo en el sistema local.
     a. En la barra de menús de XClarity Administrator, haga clic en **Administración → Licencias** para mostrar la página Administración de licencias.

b. Haga clic en el icono **Recuperar historial** () para mostrar el cuadro de diálogo Recuperar historial.

c. Introduzca el código de autorización de 22 caracteres.

d. Haga clic en **Buscar** para recuperar información acerca de las licencias disponibles y licenciadas para ese código de autorización.

   Si no se acepta el código de autorización que recibió, póngase en contacto del soporte con Lenovo.

e. Seleccione los archivos de claves de activación de licencia que desea instalar.

f. Haga clic en **Descargar** para guardar los archivos de la clave de licencia en el sistema local.

2. Desde la instancia de XClarity Administrator en la que desea instalar las claves de activación de licencia:

   a. En la barra de menús de XClarity Administrator, haga clic en **Administración → Licencias** para mostrar la página Administración de licencias.

   b. Haga clic en el icono **Importar y aplicar** () para importar e instalar las licencias.

   c. Haga clic en **Examinar** para seleccionar las claves de activación de las licencias que desea instalar.

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

   d. Haga clic en **Aceptar licencia** para importar y aplicar las licencias.

      Una vez completada la instalación, las claves de activación de licencia se muestran en la tabla con el número de licencias instaladas y el periodo de activación (fechas de inicio y caducidad).

Después de finalizar

Puede llevar a cabo las siguientes acciones desde la página Licencias.

- Descargue una o más claves de activación de licencia específicas en el sistema local haciendo clic en el icono **Exportar** ().

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

- Elimine claves de activación de licencia específicas haciendo clic en el icono de **Eliminar** ().
- Configure el periodo de advertencia de licencia haciendo clic en el botón **Editar** que se encuentra en la parte superior de la página. El periodo de advertencia de licencia es el número de días antes de que caduque la licencia cuando XClarity Administrator activa una advertencia.

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 (países de Norteamérica)
  - ESDAP@lenovo.com (países de Asia-Pacífico)
  - ESDEMEA@lenovo.com (países de Europa, Medio Oriente y Asia)
  - ESDLA@lenovo.com (países de Latinoamérica)
  - ESDChina@Lenovo.com (China)

- Si la información acerca de la autorización no es correcta, póngase en contacto con el Soporte de Lenovo a 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.

Instalación de licencias de habilitación de funciones completas mediante el portal web Features on Demand

Si XClarity Administrator *no* tiene acceso a Internet, puede licenciar y recuperar los códigos de autorización existentes utilizando los Características del portal web on Demand de otro sistema que tenga acceso de red al XClarity Administrator. A continuación, puede utilizar la interfaz web de XClarity Administrator para importar e instalar las licencias licenciadas.

Procedimiento

Para instalar licencias de Lenovo XClarity Pro en el servidor de gestión, realice los siguientes pasos.

Paso 1. Adquiera una licencia de Lenovo XClarity Pro para cada dispositivo gestionado.

Póngase en contacto con su representante de Lenovo o socio comercial autorizado para comprar licencias de Lenovo XClarity Pro en función de las funciones que desea habilitar y el número de dispositivos que desea administrar. Después de comprar licencias, se le envía un código de autorización en un *correo electrónico de prueba de derecho*. El código de autorización es una cadena alfanumérica de 22 caracteres, que debe tener en cuenta e instalar las licencias. Si no recibe el correo electrónico y compró licencias mediante un Business Partner, póngase en contacto con su Business Partner para solicitar el código de autorización.

También puede recuperar sus códigos de autorización de Características del portal web on Demand, haciendo clic en **Recuperar el código de autorización**.

Paso 2. Canjee todas las licencias o un subconjunto utilizando el código de autorización. Cuando se generan licencias, se genera un archivo de clave de activación de licencia.

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 este código de autorización, haga coincidir 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 de licencia utilizando el mismo código de autorización.

   Consejo: cada XClarity Administrator admite hasta 1.000 dispositivos administrados. Por lo tanto, una clave de activación de licencia única que instala en una instancia de XClarity Administrator no debe tener más de 1.000 licencias.

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 de licencia.
8. Opcionalmente, especifique destinatarios adicionales para recibir las claves de activación de licencia.
9. Haga clic en **Enviar** para enviar las claves de activación de licencia.

   La persona asignada al pedido de compra y los destinatarios adicionales recibirán un correo electrónico con la clave de activación de licencia. La clave es un archivo en formato .KEY.

   Nota: También puede descargar las claves de activación de licencia (individualmente o por lotes) desde el Características del portal web on Demand haciendo clic en **Recuperar historial** y utilizando el número de cliente de Lenovo para buscar las claves de activación de licencia y, a continuación, descargar todas las claves o un subconjunto de ellas. Luego, 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. Importe e instale las licencias en XClarity Administrator.

1. En la barra de menús de XClarity Administrator, haga clic en **Administración → Licencias** para mostrar la página Administración de licencias.
2. Haga clic en el icono **Importar y aplicar** () para instalar las licencias.
3. Haga clic en **Examinar** para seleccionar el archivo de clave de activación de licencia de las licencias que desea instalar.

   Consejo: para importar varias claves de activación de licencias, comprima el archivo .KEY en un archivo ZIP y seleccione el archivo ZIP para importarlo.
4. Haga clic en **Aceptar licencia** para importar y aplicar las licencias.

   Una vez completada la instalación, la clave de activación de licencia se muestra en la tabla con el número de licencias instaladas y el periodo de activación (fechas de inicio y caducidad).

Después de finalizar

Puede llevar a cabo las siguientes acciones desde la página Licencias.

- Descargue una o más claves de activación de licencia específicas en el sistema local haciendo clic en el icono **Exportar** ().

  Nota: Al exportar varias claves de activación de licencia, los archivos se descargan como un único archivo ZIP.
- Elimine claves de activación de licencia específicas haciendo clic en el icono de **Eliminar** ().
- Configure el periodo de advertencia de licencia haciendo clic en el botón **Editar** que se encuentra en la parte superior de la página. El periodo de advertencia de licencia es el número de días antes de que caduque la licencia cuando XClarity Administrator activa una advertencia.

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 (países de Norteamérica)
  - ESDAP@lenovo.com (países de Asia-Pacífico)
  - ESDEMEA@lenovo.com (países de Europa, Medio Oriente y Asia)

  - ESDLA@lenovo.com (países de Latinoamérica)
  - ESDChina@Lenovo.com (China)
- Si la información acerca de la autorización no es correcta, póngase en contacto con el Soporte de Lenovo a 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.

Capítulo 7. Actualización de XClarity Administrator como un contenedor

Cuando se ejecuta como un contenedor de Lenovo XClarity Administrator, utilice este procedimiento de actualización para instalar el software más reciente como un nuevo contenedor y enlazar los volúmenes del contenedor original con el nuevo contenedor.

Antes de empezar

Para actualizar XClarity Administrator como un contenedor de acoplamiento desde **v4.0** a **v4.1**, consulte Actualización de XClarity Administrator v4.0 a v4.1 como contenedor.

No se puede actualizar desde una versión anterior de XClarity Administrator como un contenedor de acoplamiento a XClarity Administrator **v4.0**. En su lugar, debe instalar la *imagen completa* de XClarity Administrator **v4.0** (consulte Instalación de Lenovo XClarity Administrator).

Para gestionar instancias de XClarity Administrator versión **4.0** o posterior con Lenovo XClarity Orchestrator, se requiere XClarity Orchestrator versión **2.0** o posterior. Si desea actualizar XClarity Administrator a la versión 4.0 o posterior, asegúrese de que XClarity Orchestrator ya tenga la versión 2.0 o posterior.

Acerca de esta tarea

El archivo `docker-compose.yml` usa las variables de entorno siguientes, las cuales ha configurado durante la instalación del contenedor *original*. El nuevo contenedor también usa estas variables de entorno.

- **CONTAINER_NAME**. Nombre de contenedor único, que se utiliza para crear volúmenes de docker para cada instancia de XClarity Administrator (por ejemplo, `CONTAINER_NAME=LXCA-203`)

  XClarity Administrator utiliza el nombre del contenedor para crear los volúmenes para el contenedor. Si utiliza el mismo nombre de contenedor para el nuevo contenedor, la nueva instancia de XClarity Administrator se utilizará en los mismos volúmenes y, por lo tanto, tendrá acceso a los mismos datos y valores del sistema que la instancia original de XClarity Administrator (contenedor).

  Si cambia el mismo nombre de contenedor, se crean nuevos volúmenes para el contenedor y la nueva instancia de XClarity Administrator no se tendrá acceso a los mismos datos y valores del sistema que la instancia original de XClarity Administrator (contenedor). Si necesita cambiar el nombre del contenedor o la dirección IP, cree una copia de seguridad de los datos y los valores del sistema para la instancia original de XClarity Administrator antes de instalar el nuevo contenedor y, a continuación, utilice dicha copia de seguridad para restaurar los datos del sistema y los valores en el nuevo contenedor.
- **ADDRESS**. Dirección IPv4 o IPv6 estática para el contenedor (por ejemplo, `ADDRESS=192.0.2.0`)

  Si cambia la dirección IP de XClarity Administrator después de gestionar dispositivos, es posible que los dispositivos queden en estado fuera de línea en XClarity Administrator. Asegúrese de anular la gestión de todos los dispositivos antes de cambiar la dirección IP.
- **BACKUP_MOUNT** y **FIRMWARE_MOUNT**. (Opcional) Rutas para los usos compartidos remotos que se pueden utilizar para almacenar copias de seguridad de XClarity Administrator o usar como repositorio remoto para las actualizaciones de firmware. Las rutas deben ser `/mnt/backup_share` y `/mnt/fw_share`, respectivamente.

Nota: XClarity Administrator *no* se ejecuta como un contenedor con privilegios.

Procedimiento

Para importar un contenedor de XClarity Administrator, lleve a cabo los pasos siguientes.

Paso 1. Descargue la imagen del contenedor de XClarity Administrator desde el Página web de descarga de XClarity Administrator a una estación de trabajo cliente. Inicie sesión en el sitio web y utilice la clave de acceso que se le facilitó para descargar la imagen.

Paso 2. Importe la imagen del contenedor de XClarity Administrator a su host y ejecute el siguiente comando.

```
docker load -i lnvgy_sw_lxca_110-3.5.0_anyos_noarch
```

Paso 3. Edite el mismo `docker-compose.yml` que se utilizó para el contenedor original. Actualice la propiedad de la imagen en la parte superior del archivo para que apunte a la nueva imagen de docker desde el paso 2. Puede cambiar la etiqueta de imagen utilizando el comando `docker tag`.

A continuación se muestra un archivo yml de muestra.

```
version: '3.8'

services:

  lxca:
    image: lenovo/lxca:lnvgy_sw_lxca_container_111-4.0.0_anyos_noarch
    container_name: ${CONTAINER_NAME}
    tty: true
    stop_grace_period: 60s
    volumes:
      # Bind mount remote shares to the container
      - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
      - /home/<<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
      # Docker volume mount
      - data:/opt/lenovo/lxca/data
      - postgresql:/var/lib/postgresql/data
      - log:/var/log
      - confluent-etc:/etc/confluent
      - confluent-log:/var/log/confluent
      - confluent:/var/lib/confluent
      - propconf:/opt/lenovo/lxca/bin/conf
    networks:
      lan:
        ipv4_address: ${ADDRESS}

volumes:
  data:
    name: ${CONTAINER_NAME}-data
  postgresql:
    name: ${CONTAINER_NAME}-postgresql
  log:
    name: ${CONTAINER_NAME}-log
  confluent-etc:
    name: ${CONTAINER_NAME}-confluent-etc
  confluent-log:
    name: ${CONTAINER_NAME}-confluent-log
  confluent:
    name: ${CONTAINER_NAME}-confluent
  propconf:
    name: ${CONTAINER_NAME}-propconf

networks:
  lan:
    name: lan
    driver: macvlan
    driver_opts:
```

```
    parent: eth0
  ipam:
    config:
      - subnet: 192.0.0.0/19
        gateway: 192.0.30.1
```

Paso 4. Apague el contenedor *original* al ejecutar el siguiente comando.
```
docker-compose -p ${CONTAINER_NAME} down
```

Paso 5. Despliegue la *nueva* imagen en docker al ejecutar el siguiente comando, donde <*ENV_FILENAME*> es el nombre del archivo de variables ambientales.
```
COMPOSE_HTTP_TIMEOUT=300 docker-compose -p ${CONTAINER_NAME} --env-file <ENV_FILENAME> up -d
```

Actualización de XClarity Administrator v4.0 a v4.1 como contenedor

Cuando se ejecuta Lenovo XClarity Administrator como un contenedor de acoplamiento, utilice este procedimiento de actualización para instalar el software más reciente como un nuevo contenedor y enlazar los volúmenes del contenedor original con el nuevo contenedor.

Antes de empezar

Actualizar XClarity Administrator de v4.0 a v4.1 como contenedor requiere un script de actualización especial para que determinado archivo no persistente sea persistente.

El nivel de registro se restablece al valor predeterminado una vez que se completa la actualización.

Asegúrese de que exista un usuario no root de Linux en el sistema host y de que el usuario no root pueda ejecutar comandos de Docker. Si no es así, ejecute los siguientes comandos para agregar el usuario al grupo de Docker.
```
bash
sudo groupadd docker
sudo gpasswd -a $USER docker
newgrp docker
docker ps
```

Acerca de esta tarea

Nota: XClarity Administrator *no* se ejecuta como un contenedor con privilegios.

Procedimiento

Para importar un contenedor de XClarity Administrator, lleve a cabo los pasos siguientes.

Paso 1. Cambie al usuario no root en el grupo de Docker.

Paso 2. Descargue el archivo de imagen de contenedor de XClarity Administrator (`do-container-update.sh`, `docker-compose.env`, `docker-compose.yml`, `lnvgy_sw_lxca_*.tar.gz`) desde la Página web de descarga de XClarity Administrator a su sistema local en un directorio nuevo. Inicie sesión en el sitio web y utilice la clave de acceso que se le facilitó para descargar la imagen.

Paso 3. Importe la imagen del contenedor de XClarity Administrator a su host y ejecute el siguiente comando.
```
docker load -i <CONTAINER-IMAGE-FILENAME>
```

Por ejemplo:
```
docker load -i lnvgy_sw_lxca_110-4.1.0_anyos_noarch
```

Paso 4. Edite el *nuevo* archivo `docker-compose.env` y actualice las variables de entorno siguientes para que coincidan con los valores del archivo `docker-compose.env` *original*.

A continuación hay un archivo de entorno de muestra.

```
CONTAINER_NAME="LXCA-400"
ADDRESS="192.0.2.0"
BACKUP_MOUNT="/mnt/backup_share"
FIRMWARE_MOUNT="/mnt/fw_share"
```

Paso 5. Edite el *nuevo* archivo `docker-compose.yml`. Actualice la propiedad de la **imagen** en la parte superior del archivo con el nombre de archivo de la nueva imagen de acoplamiento y, a continuación, actualice los valores de las configuraciones de red (subred, puerta de enlace y DNS) para que coincidan con los valores del archivo *original* `docker-compose.yml`.

A continuación se muestra un archivo yml de muestra.

```
version: '3.8'

services:

  lxca:
    image: lenovo/lxca:4.1.0-124
    container_name: ${CONTAINER_NAME}
    tty: true
    stop_grace_period: 60s
    volumes:
      #bind mount example
      - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
      - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
      #docker volume mount
      - data:/opt/lenovo/lxca/data
      - postgresql:/var/lib/postgresql
      - log:/var/log
      - confluent-etc:/etc/confluent
      - confluent-log:/var/log/confluent
      - confluent:/var/lib/confluent
      - propconf:/opt/lenovo/lxca/bin/conf
      - ssh:/etc/ssh
      - xcat:/etc/xcat
    networks:
      lan:
        ipv4_address: ${ADDRESS}
    dns: 192.0.30.10
         192.0.30.11
    deploy:
      resources:
        limits:
          cpus: "2.0"
          memory: "8g"

volumes:
  data:
    name: ${CONTAINER_NAME}-data
  postgresql:
    name: ${CONTAINER_NAME}-postgresql
  log:
    name: ${CONTAINER_NAME}-log
  confluent-etc:
    name: ${CONTAINER_NAME}-confluent-etc
  confluent-log:
    name: ${CONTAINER_NAME}-confluent-log
  confluent:
    name: ${CONTAINER_NAME}-confluent
```

```
  propconf:
    name: ${CONTAINER_NAME}-propconf
  ssh:
    name: ${CONTAINER_NAME}-ssh
  xcat:
    name: ${CONTAINER_NAME}-xcat
networks:
  lan:
    name: lan
    driver: macvlan
    driver_opts:
      parent: eth0
    ipam:
      config:
        - subnet: 192.0.0.0/19
          gateway: 192.0.30.1
```

Paso 6. Actualice la imagen del contenedor en el repositorio ejecutando el siguiente comando, donde <*ORIGINAL-CONTAINER-IMAGE-PATH*> la ubicación de los archivos de contenedor originales y <*NEW-CONTAINER-IMAGE-PATH*> es la ubicación donde descargó los nuevos archivos de imágenes del contenedor en el paso 2.

```
bash do-container-update.sh <ORIGINAL-CONTAINER-IMAGE-PATH> <NEW-CONTAINER-IMAGE-PATH>
```

Por ejemplo:

```
bash do-container-update.sh /home/$USER/lxca-400 /home/$USER/lxca-410
```

Nota: Durante el proceso de actualización, se le solicitará que ingrese la contraseña para el mandato `sudo`. Debe introducir la contraseña para continuar.

Capítulo 8. Desinstalación de XClarity Administrator

Siga estos pasos para desinstalar un dispositivo virtual Lenovo XClarity Administrator o un contenedor.

Procedimiento

Para desinstalar el dispositivo virtual de XClarity Administrator, siga los pasos que se describen a continuación.

Paso 1. Anule la gestión de todos los dispositivos gestionados actualmente mediante XClarity Administrator (consulte Gestión del chasis, Gestión de servidores y Gestión de conmutadores en la documentación en línea de XClarity Administrator).

Paso 2. Dependiendo del sistema operativo, desinstale XClarity Administrator:

- **Docker-compose**Ejecute el siguiente comando para detener el contenedor y quitar las redes y los volúmenes.
  ```
  docker-compose down -v
  ```
- **CentOS, Red Hat, Rocky y Ubuntu**
  1. Conéctese al host que utiliza el gestor de máquina virtual.
  2. Haga clic con el botón derecho en la máquina virtual y, a continuación, haga clic en **Apagar → Forzar el apagado**.
  3. Haga clic con el botón derecho otra vez en la máquina virtual y, a continuación, haga clic en **Eliminar**. Aparece el cuadro de diálogo Confirmación de eliminación.
  4. Seleccione todas las casillas de verificación y haga clic en **Eliminar**.
- **ESXi**
  1. Conéctese al host a través de VMware vSphere Client.
  2. Haga clic en con el botón derecho en la máquina virtual y, a continuación, haga clic en **Alimentación → Apagar**.
  3. Haga clic en con el botón derecho otra vez en la máquina virtual y, a continuación, haga clic en **Eliminar del disco**.
- **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. Haga clic con el botón derecho en la 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**.