Guía del usuario de Lenovo XClarity Administrator

Versión 4.0.0

Primera edición (Febrero 2023)

Contenido

Tablas

Resumen de los cambios

Las revisiones de seguimiento del software de gestión Lenovo XClarity Administrator admiten 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.

Esta versión admite las siguientes mejoras en el software de gestión.

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

Función	Descripción
Administración	Puede enviar 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 y XCC2, de modo que los servidores gestionados puedan encontrar el servidor de gestión utilizando esta información (consulte Configuración del acceso de red).
Supervisión	Puede ver datos de inventario adicionales para los componentes de memoria persistente (PMEM) (consulte Visualización de los detalles de un servidor gestionado). Puede ver datos de inventario adicionales para los dispositivos de almacenamiento (consulte Visualización de los detalles de un servidor gestionado).
Gestión de dispositivos	Puede ver y configurar el modo de seguridad para servidores específicos por separado de XClarity Administrator (Configuración de los valores de seguridad para un servidor gestionado y Configuración de valores de criptografía en el servidor de gestión). Las direcciones IP secundarias son compatibles con el controlador de gestión de la placa base en los servidores ThinkSystem aplicables (consulte Visualización de los detalles de un servidor gestionado).
Actualizaciones de firmware	Puede actualizar el firmware de las bibliotecas de cintas IBM TS4300 (consulte Actualización de firmware en dispositivos gestionados).
Despliegue del sistema operativo	Puede desplegar los siguientes sistemas operativos para los servidores gestionados (consulte Sistemas operativos compatibles): • Cliente de Microsoft Windows 10 21H2, 10 22H2 y 11 22H2 • Red Hat Enterprise Linux 9.x • Ubuntu Server 22.04.x

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, Gestión de conmutadores.

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.

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.

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 servidores mediante el uso de patrones de configuración.

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.

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 Instalación de sistemas operativos en servidores sin sistema operativo.

Más información:

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

Gestión de usuarios

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.

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, solo 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.

Para obtener más información sobre los tipos de autenticación, consulte Gestión del servidor de autenticación.

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 personalizado.

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.

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.

- **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.

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.

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 en la documentación en línea de XClarity Administrator.

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

Documentación

La documentación de XClarity Administrator en inglés se actualiza frecuentemente. Consulte Documentación en línea de XClarity Administrator para obtener la información y los procedimientos más actualizados.

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)

Puede cambiar el idioma de la documentación en línea de las siguientes maneras:

- Cambiar la configuración de idioma en el navegador web
- Agregar `?lang=`*<language_code>* al final de la URL, por ejemplo, para mostrar la documentación en línea en chino simplificado:
  `http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/aug_product_page.html`**?lang=zh_CN**

Inicio de sesión en XClarity Administrator

Inicie sesión en la interfaz web Lenovo XClarity Administrator utilizando un navegador web compatible.

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 iniciar sesión en la interfaz web de XClarity Administrator.

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
Configuración de IP de Windows

Adaptador de Ethernet vEthernet (teamVirtualSwitch):

   Sufijo DNS específico de la conexión  . :
   Vínculo: dirección Link-local IPv6 Address . . . . . : 2001:db8:56ff:fe80:bea3%30
   Dirección IPv4 de configuración automática. . : 192.0.2.30
   Puerta de enlace predeterminada . . . . . :
```

  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`

Se muestra la primera página de inicio de sesión de XClarity Administrator:

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

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

Paso 3. Introduzca un Id. de usuario y una contraseña válidos y, a continuación, haga clic en **Iniciar sesión**.

La primera vez que inicie sesión con una cuenta de usuario se le pedirá que cambie la contraseña. Las contraseñas tienen que cumplir los siguientes criterios:

- (1) Debe contener al menos un carácter alfabético y no debe tener más de dos caracteres secuenciales, incluidas las secuencias de caracteres alfabéticos, dígitos y las teclas del teclado QWERTY (por ejemplo “abc”, “123” y “asd” no están permitidos).
- (2) Debe contener al menos un número (0 - 9).
- (3) Deben contener al menos *dos* de los siguientes caracteres.
  - Caracteres alfabéticos en mayúscula (A - Z)
  - Caracteres alfabéticos en minúscula (a - z)
  - Caracteres especiales ; @ _ ! ' $ & +
- (4) No se debe repetir ni invertir el nombre de usuario.
- (5) No debe contener más de dos caracteres iguales de forma consecutiva (por ejemplo, “aaa”, “111” y “...” no están permitidos).

Después de finalizar

Se muestra la página Panel de XClarity Administrator:

Nota: Si el sistema operativo del host se apaga de forma esperada, puede que reciba un error de autenticación al intentar iniciar sesión en XClarity Administrator. Para resolver este problema, restaure XClarity Administrator a partir de la última copia de seguridad realizada para acceder al servidor de gestión (consulte Copia de seguridad de Lenovo XClarity Administrator).

Puede realizar las siguientes acciones del menú de acciones del usuario (ADMIN_USER) en la barra de título de XClarity Administrator.

- Encontrará información sobre cómo usar XClarity Administrator en el sistema de ayuda integrado al hacer clic en **Ayuda**.

  La documentación de XClarity Administrator en inglés se actualiza frecuentemente. Consulte Documentación en línea de XClarity Administrator para obtener la información y los procedimientos más actualizados.
- Para ver la licencia de XClarity Administrator, haga clic en **Licencia**.
- Para ver información sobre la versión de XClarity Administrator, haga clic en **Acerca de**.
- Para cambiar el idioma de la interfaz de usuario, haga clic en **Cambiar idioma**.
- Para cerrar la sesión actual, haga clic en **Cerrar sesión**.
- Para enviar ideas y proporcionar información acerca de XClarity Administrator, puede hacer clic en **Enviar ideas** o **Enviar opinión**.
- Para hacer preguntas y recibir respuestas en el sitio web del Sitio web del foro de la comunidad de Lenovo XClarity, haga clic en **Visitar el foro**.

Consejos y técnicas de la interfaz de usuario

Considere estos consejos y técnicas al utilizar la interfaz de usuario de Lenovo XClarity Administrator

Visualización de más o menos datos por página

Puede cambiar el número de filas que se muestran por página usando los enlaces en la esquina inferior derecha de la tabla. Puede visualizar **10**, **25**, **50** o **Todas** las filas.

Búsqueda de datos en listas grandes

La mayoría de los campos pueden aceptar hasta 128 caracteres.

Existen varias formas de mostrar un subconjunto de una gran lista basada en criterios específicos.

- Puede ordenar las filas de la tabla haciendo clic en el encabezado de la columna.

  El cambio del orden de clasificación de una columna de la tabla se mantiene en todas las sesiones de usuario.
- Puede utilizar las listas desplegables **Filtrar por** y **Mostrar** que están disponibles en algunas páginas para mostrar un subconjunto de datos según los criterios seleccionados.
- Puede refinar aún más el subconjunto al ingresar texto (como el nombre o la dirección IP) en el campo **Filtros** para buscar datos que se encuentran en cualquier columna disponible.

  Puede escoger de entre las últimas 10 búsquedas seleccionando las búsquedas en el menú desplegable que se encuentra en el campo **Filtros**. La última búsqueda activa de una página se mantiene transversalmente en todas las sesiones de usuario.

Visualización de los datos de una columna

Si el tamaño de la columna impide que toda la información se visualice en la celda de la tabla (se indica con puntos suspensivos), puede ver la información completa en una ventana emergente al pasar el cursor sobre el texto en la celda.

Configure las columnas de la tabla

Puede configurar las tablas para que muestren información importante para usted.

- Puede elegir las columnas que desea mostrar u ocultar haciendo clic en **Todas las acciones → Alternar columnas**.
- Puede reorganizar las columnas arrastrando los encabezados de columna a la ubicación preferida.

Cambiar el idioma de la interfaz de usuario

Tiene una opción de configurar el idioma de la interfaz de usuario cuando inicia sesión por primera vez.

Una vez que haya iniciado sesión, puede cambiar el idioma de la interfaz de usuario haciendo clic en el menú de acciones de usuario (

), y luego en **Cambiar idioma**. Seleccione el idioma que desea mostrar.

Nota: El sistema de ayuda se muestra en el mismo idioma que se establece para la interfaz de usuario

Cómo obtener ayuda

XClarity Orchestrator ofrece varias formas de obtener ayuda con la interfaz de usuario.

- Algunas páginas proporcionan detalles adicionales sobre un campo o estado específico mediante los iconos de **Ayuda** (). Pase el cursor sobre el icono para mostrar una ventana emergente con información útil.
- Para obtener ayuda sobre cómo realizar acciones específicas desde la interfaz de usuario, haga clic en el menú de acciones de usuario (

) y luego en **Ayuda**.

Uso de la aplicación Lenovo XClarity Mobile

Lenovo XClarity Administrator ofrece una aplicación móvil para dispositivos Android e iOS. Puede utilizar la aplicación Lenovo XClarity Mobile para supervisar sistemas físicos de forma segura, obtener notificaciones y alertas de estado en tiempo real y realizar acciones en tareas de nivel de sistema. La aplicación también puede conectarse directamente a través de un puerto USB habilitado en un servidor ThinkSystem y proporcionar la capacidad virtual de LCD.

Más información:  Descripción general de la aplicación Lenovo XClarity Mobile

Si utiliza la aplicación XClarity Mobile, puede realizar las siguientes actividades:
- Configure los valores de red y las propiedades
- Ver el resumen de estado de todas las instancias de XClarity Administrator conectadas.
- Ver el resumen de estado de todos los dispositivos gestionados.
- Mostrar vistas gráficas (mapas) para chasis, servidores de bastidor y dispositivos de almacenamiento.
- Vista de grupos de recursos que se definen en el XClarity Administrator.
- Consulte la información de puerto del conmutador de bastidor y cambie el estado del puerto configurado.
- Supervise el inventario y el estado detallado de cada dispositivo gestionado.
- Supervisar los sucesos de auditoría, los sucesos de hardware y de gestión, así como las alertas y los trabajos.
- Encender y apagar el LED de ubicación en un dispositivo gestionado.
- Encender, apagar, reiniciar o restablecer un dispositivo gestionado.
- Activar la recopilación de datos de diagnóstico.
- Ver el estado y la información de garantía del dispositivo
- Configuración de notificaciones automáticas de problemas mediante Llamar a casa.
- Ver el resumen de informes de servicio abiertos y eliminar informes de servicio
- Enviar notificaciones automáticas de sucesos a su dispositivo móvil (consulte Reenviar sucesos a dispositivos móviles).
- Ver el resumen de los usuarios activos y el uso de los recursos del sistema
- Enviar comentarios acerca de esta aplicación móvil a soporte técnico de Lenovo.
- Conecte su dispositivo móvil directamente a un servidor ThinkSystem para gestionar el servidor mediante la aplicación XClarity Mobile (para dispositivos que admiten anclaje USB).
- Descargue datos del servicio de Lenovo XClarity Controller al dispositivo móvil mientras está conectado a un servidor ThinkSystem.

También puede conectar su dispositivo móvil directamente con los servidores ThinkSystem y luego iniciar la aplicación XClarity Mobile e iniciar sesión en el controlador de gestión de placa base del servidor con las mismas credenciales web y CLI. Existe un menú de información adicional y acciones disponible, el cual incluye:

- Servicio
  - Compartir información de resumen mediante correo electrónico u otros medios proporcionados por el dispositivo móvil
  - Borrar el registro de sucesos y de auditoría
  - Descargar el registro de sucesos y de auditoría al almacenamiento local del dispositivo móvil o transmitir el registro mediante otros medios proporcionados por el dispositivo móvil
  - Descargar el archivo de servicio BMC FFDC al almacenamiento local del dispositivo móvil o transmitir el archivo mediante otros medios proporcionados por el dispositivo móvil
  - Ver los datos históricos del gráfico de consumo de alimentación, térmico y del sistema
  - Habilitar el modo de servicio “Un toque”, que proporciona un resumen inmediato de las alertas activas y la información del dispositivo crítico
- Configuración inicial
  - Gestionar un nuevo dispositivo utilizando el XClarity Administrator seleccionado

  - Configurar propiedades del servidor, como la ubicación y la información de contacto para la configuración inicial
  - Ver y cambiar los valores de la interfaz de red del BMC IPv4 e IPv6
  - Especificar el orden de arranque y los valores del arranque único
  - Cambiar la asignación del puerto USB del panel frontal
  - Ver el número de rearranques del servidor y el tiempo total de alimentación
- Acciones de alimentación
  - Encender o apagar el servidor, reiniciar el servidor o activar el NMI
  - Restablezca el BMC

Consejo: una vez abierta la aplicación, debe actualizarla para ver el estado, el inventario, los sucesos y los trabajos nuevos.

Requisitos previos

- Las tabletas iOS solo son compatibles con la resolución de pantalla de iPhone. Las tabletas Android no son compatibles en la actualidad.
- Son compatibles los sistemas operativos móviles siguientes:
  - Android 7 – 11
  - iOS 10 y versiones posteriores

    Notas:

    - Android 5 solo se admite en la versión XClarity Mobile 2.3.0 y las anteriores.
    - El reconocimiento facial que se utiliza en los dispositivos iPhone X/XR/XS no es compatible.
- Asegúrese de que su dispositivo móvil dispone de una conexión de red con las instancias de XClarity Administrator. Esto puede requerir el uso de una VPN. Póngase en contacto con el administrador de la red para obtener asistencia.
- Importe el certificado de la entidad de certificación (CA) para cada una de las instancias de XClarity Administrator.

  Importante: Todas las conexiones con XClarity Administrator utilizan HTTPS. No obstante, debe haber una cadena de certificado válida antes de que la conexión se considere fiable y los datos puedan transferirse al dispositivo móvil. Para crear una cadena de certificado de confianza, debe importar el certificado autofirmado de la entidad de certificación (CA) de XClarity Administrator al dispositivo móvil.

  Para importar el certificado autofirmado de la entidad de certificación (CA) para *cada instancia de XClarity Administrator* al dispositivo móvil, lleve a cabo los pasos siguientes.

  1. Descargue el certificado de la entidad de certificación (CA) en un sistema local:
     a. Conéctese a la instancia de XClarity Administrator utilizando un navegador web en su sistema local.
     b. En la barra de menús de XClarity Administrator, haga clic en **Administración → Seguridad** para mostrar la página Seguridad.
     c. Haga clic en **Entidad de certificación** en la sección Gestión de certificados. Aparece la página Entidad de certificación.
     d. Haga clic en **Descargar certificado raíz de entidad de certificación**.

        Atención: Por lo general, no es necesario hacer clic en **Volver a generar certificado raíz de entidad de certificación** para completar este proceso. Si lo hace, puede que se produzca una interrupción en la comunicación con los dispositivos gestionados, a menos que se siga el procedimiento correcto. Para obtener más información, consulte el apartado Trabajo con certificados de seguridad.

e. Haga clic en **Guardar como DER** o **Guardar como PEM** para guardar el certificado de la entidad de certificación (CA) como un archivo DER o PEM en su sistema local. En la mayoría de los casos, el formato PEM funciona.

2. Transfiera el archivo de certificado de la entidad de certificación (CA) al dispositivo móvil, por ejemplo, usando un repositorio de almacenamiento accesible (como Dropbox™), un mensaje de correo electrónico o un sistema de transferencia de archivos a través de un cable conectado.
3. Importar el certificado de confianza de la entidad de certificación (CA):
   – (Android) Por lo general, para realizar esta operación debe seleccionar **Ajustes → Seguridad → Instalar** en el almacenamiento del teléfono y, a continuación, elegir el archivo de certificado que ha descargado.

     Importante: Si el certificado de la CA que ha instalado correctamente no ha sido firmado por un tercero, en la pantalla de los dispositivos Android aparece el mensaje `Es posible que un tercero desconocido esté vigilando la red`. Como el certificado de la CA se genera en su entorno de confianza, puede obviar este mensaje sin problemas. Asegúrese de que el mensaje se refiere realmente al certificado de la CA de XClarity Administrator antes de obviar el mensaje.
   – (iOS) Abra el mensaje de correo electrónico en su dispositivo móvil y haga clic en el vínculo de documento que se incluye en el mismo para importar el certificado de confianza de la CA.

   Atención: En iOS 10.3 y posterior, los certificados importados no son confiables de forma predeterminada. Para otorgar confianza a los certificados, seleccione **Valores → General → Acerca de → Valores de confianza de certificado** y habilite la confianza de los certificados.

Instalación y configuración

1. Descargue la aplicación XClarity Mobile desde la iTunes App Store (iOS) o desde Google Play Store (Android).
2. Para instalar la aplicación, siga las instrucciones del dispositivo móvil.

   Importante: Se requiere un código de seguridad de nivel del SO para desbloquear el acceso a la pantalla y utilizar la aplicación XClarity Mobile. Si aún no ha configurado ninguno, el sistema le indica que debe hacerlo durante la instalación.
3. Haga clic en **Valores** para añadir o editar conexiones a varias instancias de XClarity Administrator usando la detección automática o proporcionando una dirección IP y las credenciales de usuario correspondientes y, a continuación, establezca un código PIN para la aplicación, cambie el suceso y los valores del registro de auditoría y seleccione el idioma deseado.

Conectar directamente con servidores ThinkSystem

Los servidores Lenovo Think System incluyen un puerto USB en el panel frontal que puede usar para conectar su dispositivo móvil y brindar capacidades semejantes a las disponibles en el panel de visualización de información del sistema LCD en otros servidores Lenovo.

Para gestionar un servidor ThinkSystem conectándose directamente al servidor, siga estos pasos.

1. Cambie el USB del panel frontal del servidor de host a BMC al realizar uno de los siguientes pasos.
   a. En la CLI del controlador de gestión, ejecute el comando `usbfp`
   b. En la interfaz web del controlador de gestión, haga clic en **Configuración de BMC → Red → Gestión del puerto USB del panel frontal**.
   c. Mantenga presionado el LED de ubicación azul de Id. en el panel frontal por al menos 3 segundos hasta que la luz parpadee cada un par de segundos.
2. Conecte el cable USB del teléfono al puerto USB del panel frontal en el servidor ThinkSystem.
3. En su dispositivo móvil, habilite el anclaje USB.
   a. Para IOS, haga clic en **Configuración → Celular → Punto de acceso personal**.

b. Para Android, haga clic en **Configuración → Punto de acceso móvil y anclaje → Anclaje USB**.

4. En su dispositivo móvil, inicie la aplicación XClarity Mobile.
5. Si la detección automática está deshabilitada, haga clic en **Detección** en la página Detección de USB para conectar el controlador de gestión del servidor y recopilar información, incluyendo inventario, estado, firmware, configuración de red y una lista de los últimos sucesos activos.

Consejo:

- Asegúrese de utilizar un cable USB de alta calidad que admita datos y alimentación. Tenga en cuenta que algunos cables que se suministran con dispositivos móviles están diseñados únicamente para fines de carga.

  Nota: Para conectarse a ThinkSystem SD530, también debe utilizar un cable o adaptador micro USB a USB de alta calidad.
- El servidor conectado mediante USB debe estar encendido para informar el conjunto completo de estadísticas de voltaje, temperatura y uso en las tarjetas de estado.
- Si el servidor conectado mediante USB no tiene un LED/botón externo de “identificación azul” en el panel frontal, debe utilizar la interfaz web del controlador de gestión o la CLI para cambiar la selección de gestión de puerto USB del panel frontal, si es necesario.
- Los cambios realizados a la interfaz de red del controlador de gestión desde la aplicación XClarity Mobile entran en vigor inmediatamente sin que sea necesario reiniciar el controlador de gestión. Por ejemplo, si la interfaz IPv4 se cambia de dirección estática a DHCP, la interfaz obtiene inmediatamente una dirección asignada por DHCP.
- En la pestaña NewsFeed, la tarjeta “Últimos sucesos activos” inicialmente muestra hasta tres sucesos activos que se mencionan en la pestaña Sucesos activos del controlador de gestión. En la aplicación móvil, si toca ligeramente la tarjeta, se muestran todos los sucesos activos. Tenga en cuenta que esta es una lista de sucesos activos y resueltos, no una lista completa de todos los sucesos.

Uso del modo de demostración

Puede habilitar el **Modo de demostración** en la página Configuración para completar la aplicación XClarity Mobile con los datos de la demostración para dos instancias de XClarity Administrator, incluidos batidores y chasis. En este modo, puede ver el resumen del estado de las instancias de XClarity Administrator, ver el estado detallado y el inventario de dispositivos, además de poder supervisar sucesos y alertas. Sin embargo, las acciones de gestión, como encender o apagar, no están admitidas.

Notas:

- Solo puede habilitar el modo de demostración cuando no existan conexiones con instancias reales de XClarity Administrator.
- No puede añadir conexiones a instancias reales de XClarity Administrator mientras el modo de demostración esté habilitado.

Búsqueda

Puede utilizar el campo **Buscar** para mostrar los dispositivos gestionados con un nombre o estado específicos (Crítico, Advertencia o Normal). Por ejemplo, si busca “crít”, solo se muestran los dispositivos gestionados que tienen el estado crítico y que contienen la cadena de caracteres “crít” en su nombre.

Resolución de problemas

Problemas de instalación:

- La aplicación móvil Android está “firmada” con una clave segura para mejorar la seguridad. Se aumentó el tamaño de la clave segura en la nueva versión. Ya que la aplicación firmada coincide con la firma anterior de la aplicación, el proceso de seguridad de instalación de Android impide la actualización automática.

Para actualizar la aplicación móvil, desinstale la versión actual de la aplicación móvil, descargue la versión más reciente de la aplicación Android desde la tienda de aplicaciones y vuelva a instalar la aplicación. En la mayoría de los dispositivos Android, la aplicación se puede desinstalar utilizando el elemento del menú **Valores → Aplicaciones → Gestor de aplicaciones**.

Problemas relacionados con la conectividad:

- La función de fijación USB en iOS 14, 14.0.1 y 14.0.2 no funciona correctamente y, por lo tanto, la función de fijación de aplicación Lenovo XClarity Mobile no está disponible para estas versiones de iOS. Esto afecta solo a la gestión de portátiles con conexión USB en el centro de datos. La gestión remota mediante dispositivos móviles que admiten comunicaciones móviles y wifi no se ven afectados y pueden utilizarse para conectar y recopilar datos desde XClarity Administrator y para realizar acciones de gestión en dispositivos gestionados.

  Si se necesita la función de gestión de portátiles con conexión USB, no actualice a iOS 14.

  Esta notificación se actualizará cuando Apple resuelva el problema con iOS 14.
- XClarity Mobile requiere que su dispositivo móvil disponga de una conexión de red con las instancias de XClarity Administrator. Esto puede requerir el uso de una VPN. Póngase en contacto con el administrador de la red para obtener asistencia.
- Las conexiones entre su dispositivo móvil y cada una de las instancias de XClarity Administrator requieren una cadena de certificado de confianza. Consulte la documentación en línea para obtener instrucciones sobre cómo descargar e instalar los certificados de confianza de la entidad de certificación (CA) en su dispositivo móvil.

  Si el certificado de la CA que ha instalado correctamente no ha sido firmado por un tercero, en la pantalla aparece el mensaje `Es posible que un tercero desconocido esté vigilando la red`. Como el certificado de la CA se genera en su entorno de confianza, puede obviar este mensaje sin problemas. Asegúrese de que el mensaje se refiere realmente al certificado de la CA de XClarity Administrator antes de obviar el mensaje.
- Cuando cambia el dispositivo móvil de una red privada virtual (VPN) a una red local o viceversa, puede que aparezca el mensaje `La puerta de enlace segura ha rechazado el intento de conexión. Es preciso realizar un nuevo intento de conexión con la misma puerta de enlace o con otra segura, para lo cual necesitará autenticarse de nuevo`. Inicie sesión en Lenovo XClarity Mobile para seguir utilizando la aplicación.

Problemas relacionados con la seguridad:

- Si olvida el código PIN, desinstale la aplicación XClarity Mobile y vuelva a instalarla. A continuación, restablezca todas las conexiones.
- Si borra credenciales en un dispositivo Android, la clave de cifrado se eliminará y tendrá que restablecer todas las conexiones.

Problemas relacionados con los sucesos:

- De manera predeterminada, el registro de sucesos muestra los sucesos de hardware y de gestión que se han recibido en las últimas 24 horas, mientras que el registro de auditoría muestra los sucesos de auditoría que se han recibido en las últimas 2 horas. Si no se han recibido sucesos durante los períodos de tiempo seleccionados, el registro de sucesos y el registro de auditoría no aparecen en la página Supervisión de XClarity Mobile.
- Si configura el reenvío de sucesos en XClarity Administrator para que envíe los sucesos a una cuenta de correo electrónico, es posible que los vínculos incluidos en el correo electrónico no funcionen en los dispositivos Android. Asegúrese de que su versión de Android y su aplicación de correo electrónico admiten hipervínculos. Si no se admiten hipervínculos, utilice otra aplicación de correo electrónico.

Problemas relacionados con el sistema de ayuda:

- En algunos dispositivos, el sistema de ayuda no se ajusta al el tamaño de la pantalla. Utilice los controles del sistema de ayuda para maximizar y, a continuación, minimizar la página.

Capítulo 2. Administración de Lenovo XClarity Administrator

Lenovo XClarity Administrator incluye varias tareas administrativas, como agregar usuarios o ver trabajos.

Gestión de autenticación y autorización

Lenovo XClarity Administrator proporciona mecanismos de seguridad para verificar las credenciales de un usuario y controlar el acceso a recursos y tareas.

Gestión del servidor de autenticación

De forma predeterminada, Lenovo XClarity Administrator usa un servidor con Lightweight Directory Access Protocol (LDAP) para autenticar credenciales de usuario.

Acerca de esta tarea

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, solo 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, solo 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.

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:

  – 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.

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

  – 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.

  – 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).

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 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.

Para obtener información acerca de la recuperación de dispositivos gestionados, consulte “Recuperación de la gestión con un CMM tras un error de servidor de gestión” en la página 233, “Recuperación de la gestión de un servidor de bastidor o de torre tras un error de servidor de gestión” en la página 285.

Configuración de un servidor de autenticación LDAP externo

Si lo desea, puede usar un servidor de autenticación LDAP externo en lugar del servidor de autenticación de Lenovo XClarity Administrator local en el nodo de gestión.

Antes de empezar

Es preciso llevar a cabo la configuración inicial de XClarity Administrator antes de configurar el servidor de autenticación externo.

Se admiten los siguientes servidores de autenticación externos:

- OpenLDAP
- Microsoft Active Directory. Debe residir en un servidor de Microsoft Windows externo conectado a la red de gestión, red de datos o ambos.

Asegúrese de que todos los puertos requeridos para el servidor de autenticación externo estén abiertos en la red y en los firewalls. Para obtener más información acerca de los requisitos de los puertos, consulte Disponibilidad de puertos en la documentación en línea de XClarity Administrator.

Debe crear o cambiar el nombre de los grupos de roles en el servidor de autenticación local para que coincida con el de los grupos que están definidos en el servidor de autenticación externo.

Asegúrese de que haya uno o más usuarios con la autoridad **lxc-recovery** en el servidor de autenticación local. Puede utilizar esta cuenta de usuario local para autenticar directamente en XClarity Administrator cuando un error de comunicación se produce con el servidor LDAP externo.

Nota: Cuando se configura XClarity Administrator para utilizar un servidor de autenticación externo, la página Gestión de usuarios de la interfaz web de XClarity Administrator se deshabilita.

Atención: Para Active Directory, 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.

XClarity Administrator realiza un control de conectividad cada 5 minutos para mantener la conectividad en los servidores LDAP externos. Los entornos con muchos servidores LDAP podrían experimentar un alto uso de la CPU durante esta comprobación de conectividad. Para lograr el mejor rendimiento, asegúrese de que se pueda acceder a la mayor parte o a todos los servidores LDAP en el dominio, o establezca el método de selección del servidor de autenticación en **Utilizar servidores preconfigurados** y especifique solo los servidores LDAP conocidos y con acceso.

Procedimiento

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

Paso 1. Configure el método de autenticación de usuarios para Microsoft Active Directory u OpenLDAP.

Si decide usar una autenticación no segura, no se requiere ninguna configuración adicional. Los controladores de dominio de Windows Active Directory u OpenLDAP usan la autenticación LDAP no segura de forma predeterminada.

Si decide usar la autenticación LDAP segura, deberá configurar los controladores de dominio de modo que se lleve a cabo la autenticación LDAP segura. Para obtener más información sobre la configuración de la configuración de autenticación LDAP segura en Active Directory, consulte el Artículo sobre certificado de LDAP sobre SSL (LDAPS) en el sitio Web de Microsoft TechNet.

Para comprobar que los controladores de dominio de Active Directory están configurados para usar la autenticación LDAP segura:

- Busque el suceso `LDAP sobre Secure Sockets layer (SSL) ya está disponible` en la ventana Visor de sucesos de los controladores del dominio.
- Use la herramienta `ldp.exe` de Windows para comprobar que la conexión LDAP con los controladores de dominio sea segura.

Paso 2. Importe el certificado de servidor de Active Directory u OpenLDAP o el certificado raíz de la entidad de certificación que firmó el certificado de servidor.

a. En la barra de menús de XClarity Administrator, haga clic en **Administración → Seguridad**.

b. Haga clic en **Certificados de confianza** en la sección Gestión de certificados.

c. Haga clic en el icono de **Crear** ( ) para añadir un certificado.

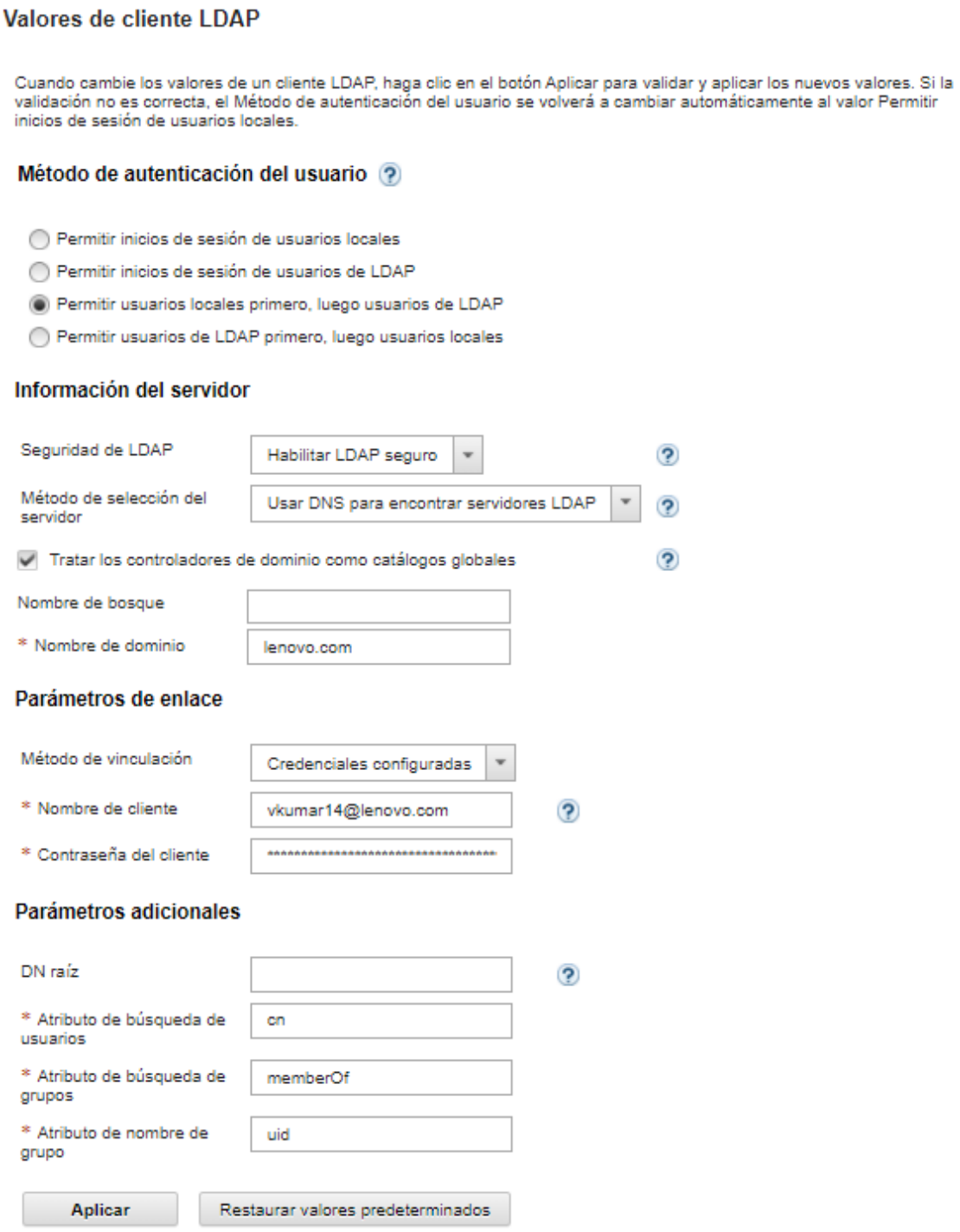
d. Examine el archivo o pegue el texto del certificado con formato PEM.

e. Haga clic en **Crear**.

Paso 3. Configure el cliente LDAP de XClarity Administrator:

a. En la barra de menús de XClarity Administrator , haga clic en **Administración → Seguridad**.

b. Haga clic en **Cliente LDAP** en la sección Usuarios y grupos para mostrar el cuadro de diálogo Valores de cliente LDAP.



c. Rellene el cuadro de diálogo de acuerdo con los criterios siguientes.

   1. Elija uno de los siguientes métodos de autenticación de usuario:

      - **Permitir inicios de sesión de usuarios locales**. La autenticación se realiza mediante la autenticación local. Cuando se selecciona esta opción, todas las cuentas de usuario se encuentran en el servidor de autenticación local del nodo de gestión.
      - **Permitir inicios de sesión de usuarios de LDAP**. Un servidor LDAP externo realiza la autenticación. Este método habilita la gestión remota de las cuentas de usuario. Cuando esta opción está seleccionada, todas las cuentas de usuarios existen remotamente en un servidor LDAP externo.

- **Permitir usuarios locales primero, luego usuarios de LDAP**. El servidor de autenticación local realiza la autenticación primero. Si esto falla, un servidor LDAP externo realiza la autenticación.
- **Permitir usuarios de LDAP primero, luego usuarios locales**. Un servidor LDAP externo realiza la autenticación primero. Si eso falla, el servidor de autenticación local realiza la autenticación.

2. Elija si desea habilitar o deshabilitar la seguridad LDAP:
   - **Habilitar LDAP seguro**. XClarity Administrator usa el protocolo LDAPS para conectarse de forma segura al servidor de autenticación externo. Cuando esta opción está seleccionada, también debe configurar certificados de confianza para habilitar el soporte LDAP seguro.
   - **Deshabilitar LDAP seguro**. XClarity Administrator usa un protocolo no seguro para conectarse al servidor de autenticación externo. Si elige esta configuración, el hardware puede quedar más vulnerable a los ataques contra la seguridad.
3. Elija uno de los siguientes métodos de selección de servidor:
   - **Usar servidores preconfigurados**. XClarity Administrator usa las direcciones IP y los puertos especificados para detectar el servidor de autenticación externo.

     Si selecciona esta opción, especifique hasta cuatro direcciones IP de servidor preconfiguradas y puertos. El cliente LDAP intenta autenticarse mediante la primera dirección de servidor. Si la autenticación produce un error, el cliente LDAP intenta autenticarse mediante la siguiente dirección IP de servidor.

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

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

     Importante: Es preciso indicar al menos un controlador de dominio, incluso si se ha especificado el catálogo global. Si solo se especifica el catálogo global, parece que la operación se ha realizado correctamente, pero no es una configuración válida.

     Cuando el modo de criptografía se establece en NIST-800-131A, es posible que XClarity Administrator no pueda conectarse a un servidor LDAP externo mediante un puerto seguro (por ejemplo, mediante LDAPS a través del puerto predeterminado 636) si el servidor LDAP no es capaz de establecer una conexión de Seguridad de capa de transporte (TLS) versión 1.2 con el cliente LDAP en XClarity Administrator.
   - **Usar DNS para encontrar servidores LDAP**. XClarity Administrator usa el nombre de dominio especificado o el nombre de bosque para detectar dinámicamente el servidor de autenticación externo. El nombre de dominio y el nombre de bosque se usan para obtener una lista de controladores de dominio y el nombre de bosque se emplea para obtener una lista de servidores de catálogo global.

     Atención: Cuando utilice DNS para buscar servidores LDAP, asegúrese de que la cuenta de usuario que vaya a utilizar para autenticarse en el servidor de autenticación externo esté alojada en los controladores de dominio especificados. Si la cuenta de usuario está alojada en un controlador de dominio secundario, incluya dicho controlador en la lista de solicitudes de servicio.
4. Elija uno de los siguientes métodos de vinculación:

- **Credenciales configuradas**. Use este método de enlace para utilizar el nombre y la contraseña de cliente que se deberán utilizar para enlazar a XClarity Administrator con el servidor de autenticación externo. Si el enlace falla, también fallará el proceso de autenticación

  El nombre de cliente puede ser cualquier nombre que el servidor LDAP admite, incluido un nombre distinguido, AMAccountName, nombre de NetBIOS o UserPrincipalName. El nombre de cliente debe ser una cuenta de usuario con el dominio que tiene al menos privilegios de solo lectura. Por ejemplo:
  ```
  cn=username,cn=users,dc=example,dc=com
  domain\username
  username@domain.com
  username
  ```

  Atención: Si cambia la contraseña del cliente en el servidor de autenticación externo, asegúrese de actualizar también la nueva contraseña en XClarity Administrator. Para obtener más información, consulte No se puede iniciar sesión en XClarity Administrator en la XClarity Administrator documentación en línea.

- **Credenciales de inicio de sesión**. Use este método de enlace para utilizar el nombre y la contraseña de usuario de Active Directory u OpenLDAP que se deberán utilizar para enlazar a XClarity Administrator con el servidor de autenticación externo.

  El Id. de usuario y la contraseña que especifica se usan solo para probar la conexión con el servidor de autenticación. Si son exitosos, se guardan los valores del cliente LDAP, pero el credencial de inicio de sesión de la prueba que especificó no se guarda. Todos los enlaces futuros utilizan el nombre de usuario y la contraseña que usó para iniciar la sesión en XClarity Administrator.

  Notas:

  – Debe haber iniciado sesión en XClarity Administrator, utilizando un Id. de usuario completamente calificado (por ejemplo, `administrator@domain.com` o `DOMAIN\admin`).

  – Debe utilizar un nombre de cliente de prueba completamente calificado para el método de vinculación.

  Atención: Para configurar el método de vinculación para utilizar las credenciales de inicio de sesión, el controlador de gestión para cada servidor gestionado debe estar ejecutando firmware a partir de septiembre de 2016 o con posterioridad.

5. En el campo **DN raíz**, se recomienda que no especifique un nombre distinguido raíz, sobre todo para entornos con varios dominios. Cuando este campo está vacío, XClarity Administrator consulta al servidor de autenticación externo para conocer los contextos de asignación de nombres. Si utiliza DNS para detectar el servidor de autenticación externo, o si especifica varios servidores (por ejemplo, `dc=example,dc=com`), opcionalmente, puede especificar la entrada de nivel superior en el árbol del directorio LDAP. En este caso, las búsquedas se inician utilizando el nombre distinguido raíz especificado como la base de búsqueda.
6. Especifique el atributo a utilizar para buscar el nombre de usuario.

   Cuando el método de vinculación está configurado como **Credenciales configuradas**, una solicitud de búsqueda sigue el enlace inicial al servidor LDAP al recuperar la información específica acerca del usuario, incluyendo el DN de usuario, permisos de inicio y membresía de grupo. Esta solicitud de búsqueda debe especificar el nombre del atributo que representa los Id. de usuario en ese servidor. Este nombre del atributo se configura en este campo. Si este campo se deja en blanco, el valor predeterminado es **cn**.

7. Especifique el nombre del atributo que se utiliza para identificar los grupos a los que un usuario pertenece. Si este campo se deja en blanco, el nombre del atributo en el filtro se coloca **memberOf**.
8. Especifique el nombre del atributo que se utiliza para identificar el nombre de grupo que está configurado de por el servidor LDAP. Si este campo se deja en blanco, el valor predeterminado es **uid**.

d. Haga clic en **Aplicar**.

XClarity Administrator intenta probar la configuración para detectar errores comunes. Si la prueba falla, se muestran mensajes de error que indican el origen de los errores. Si la prueba tiene éxito y las conexiones a los servidores especificados se realizan correctamente, la autenticación del usuario puede seguir fallando si:

- No existe un usuario local con la autoridad de **lxc-recovery**.
- El nombre distinguido raíz no es correcto.
- Si el usuario no es miembro de al menos un grupo en el servidor de autenticación externo que coincida con el nombre de un grupo de roles en el servidor de autenticación de XClarity Administrator. XClarity Administrator no puede detectar si el nombre distinguido raíz es correcto; no obstante, sí que puede detectar si un usuario es miembro de al menos un grupo. Si el usuario no es miembro de al menos un grupo, cuando el usuario intenta iniciar sesión en XClarity Administrator aparece un mensaje de error. Para obtener más información acerca de la resolución de problemas relacionados con los servidores de autenticación externos, consulte Problemas relacionados con la conectividad en la documentación en línea de XClarity Administrator.

Paso 4. Cree una cuenta de usuario externa que pueda tener acceso a XClarity Administrator:

a. Desde el servidor de autenticación externo, cree una cuenta de usuario. Para obtener instrucciones, consulte la documentación de Active Directory u OpenLDAP.

b. Cree un grupo global de Active Directory u OpenLDAP con el nombre de un grupo predefinido y autorizado. El grupo debe existir en el contexto del nombre distinguido raíz definido en el cliente LDAP.

c. Añada al usuario de Active Directory u OpenLDAP como miembro del grupo de seguridad creado anteriormente.

d. Inicie sesión en XClarity Administrator mediante el nombre de usuario de Active Directory u OpenLDAP.

e. **Opcional:** defina y cree grupos adicionales. Puede autorizar estos grupos y asignarles roles desde la página Usuarios y grupos.

f. Si el LDAP seguro está habilitado, importe los certificados de confianza al servidor LDAP externo (consulte Instalación de un certificado de servidor firmado externamente y personalizado).

Resultados

XClarity Administrator valida la conexión al servidor LDAP. Si la validación se realiza correctamente, la autenticación del usuario en el servidor de autenticación externo se lleva a cabo al iniciar sesión en XClarity Administrator, el CMM y el controlador de gestión.

Si no se consigue realizar la validación, el modo de autenticación se revierte automáticamente a la opción **Permitir inicios de sesión de usuarios locales** y se muestra un mensaje en el que se explica la causa del error.

Nota: Es preciso que se hayan configurado los grupos de roles correctos en XClarity Administrator y que las cuentas de usuarios estén definidas como miembros de uno de estos grupos de roles en el servidor de Active Directory. De lo contrario, la autenticación de usuario no se realizará.

Configurar un proveedor de identidad SAML externo

Puede elegir usar un Security Assertion Markup Language (SAML) 2.0 proveedor de identidad para realizar la autenticación y autorización de Lenovo XClarity Administrator.

Antes de empezar

Es preciso llevar a cabo la configuración inicial de XClarity Administrator antes de configurar el proveedor de identidad.

El proveedor de identidad debe ser Microsoft Active Directory Federated Service (AD FS) y se puede conectar a la red de gestión, la red de datos o a ambas. Ya que la autenticación se realiza a través de su navegador web, el navegador web debe tener acceso a XClarity Administrator y al servidor SAML.

Puede descargar los metadatos de IDP utilizando la siguiente URL: `https://<ADFS_IP_Address>/federationmetadata/2007-06/federationmetadata.xml`, donde *<ADFS_IP_Address>* es la dirección IP de AD FS (por ejemplo, https://10.192.0.0/federationmetadata/2007-06/federationmetadata.xml).

Debe crear o cambiar el nombre de los grupos de roles en el servidor de autenticación de ubicaciones para que coincida con el de los grupos que están definidos en el servidor de autenticación externo.

Para configurar un proveedor de identidad SAML, debe iniciar sesión como usuario miembro del grupo **lxc_admin** o **lxc_supervisor**.

Acerca de esta tarea

XClarity Administrator es compatible con el uso de un proveedor de identidad Security Assertion Markup Language 2.0 para autenticar y autorizar usuarios. Además de introducir un nombre de usuario y una contraseña, el proveedor de identidad puede configurarse para que requiera criterios adicionales para validar la identidad del usuario, como la introducción de un código PIN, la lectura de una tarjeta inteligente y la autenticación mediante un certificado de cliente.

Cuando se configura XClarity Administrator para que use proveedor de identidad, las solicitudes de inicio de sesión interactivas de la interfaz web de XClarity Administrator se redirigen al proveedor de identidad para la autenticación. Después de autenticar un usuario, el navegador web se redirige de regreso a XClarity Administrator.

Nota: Si el proveedor de identidad está habilitado, puede omitir el proveedor de identidad e iniciar sesión en XClarity Administrator mediante el servidor de autenticación LDAP local o externo abriendo el navegador web en la página de inicio de sesión de XClarity Administrator (por ejemplo, `https://<ip_address>/ui/login.htm`).

Cuando se configura XClarity Administrator para utilizar un perfil de proveedor de identidad, la página Gestión de usuarios de la interfaz web de XClarity Administrator no se deshabilita. Se requieren cuentas de usuario locales para iniciar sesión directamente en un chasis o servidor gestionados (excepto cuando la Encapsulación está habilitada en ese dispositivo) y para la autenticación de PowerShell y de las API REST.

Procedimiento

Lleve a cabo los pasos siguientes para configurar un proveedor de identidad SAML externo (AD FS).

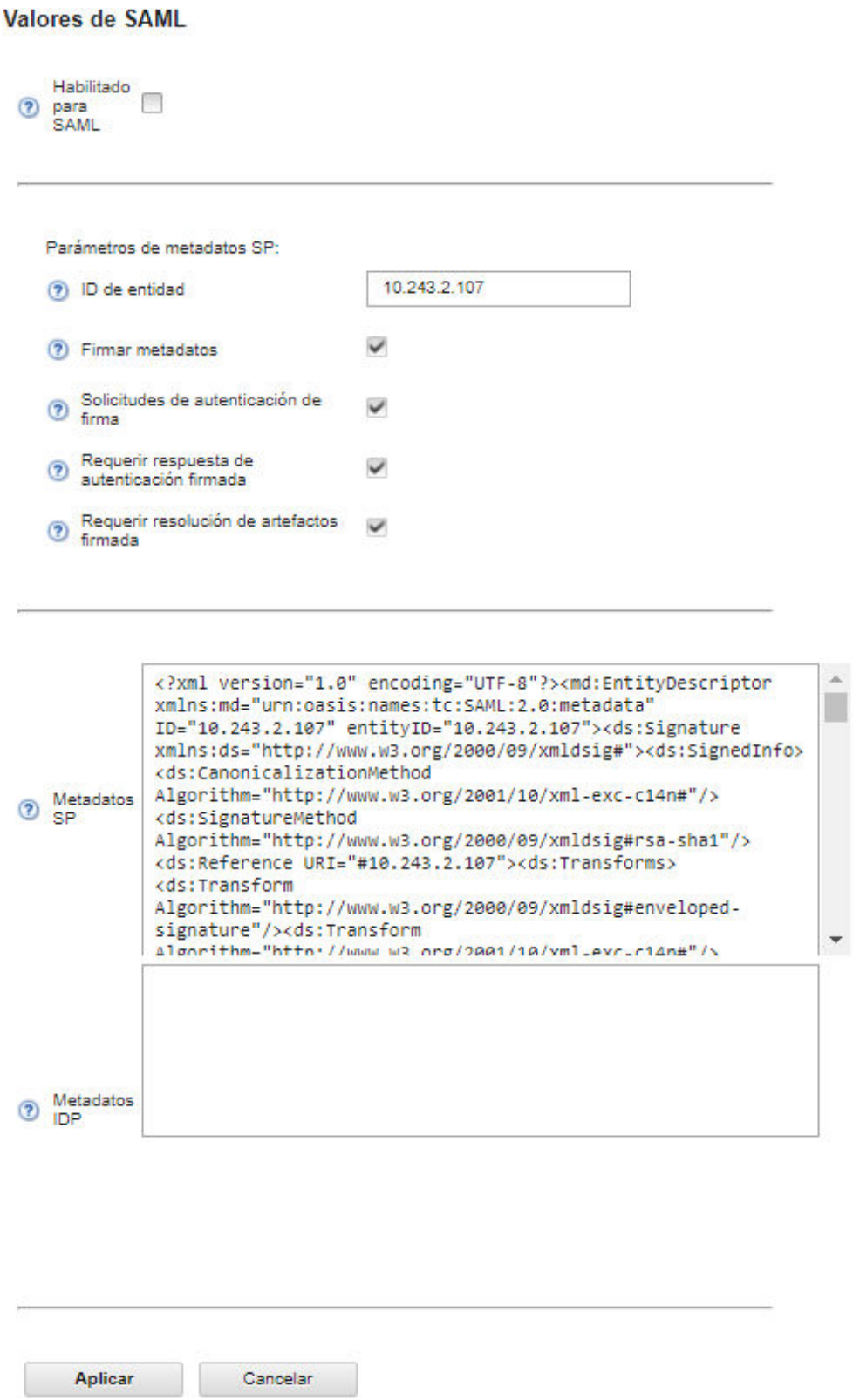
Paso 1. Cree una cuenta de usuario de recuperación que se pueda usar para iniciar sesión en XClarity Administrator si el proveedor de identidad llega a estar no disponible (consulte Gestión de cuentas de usuario).

Paso 2. Recupere los metadatos del proveedor de identidad (IDP) desde el proveedor de identidad y, a continuación, guarde el archivo en el host de XClarity Administrator.

Paso 3. Configure el cliente SAML de XClarity Administrator.

a. En la barra de menús de XClarity Administrator , haga clic en **Administración → Seguridad**.

b. Haga clic en **Configuración de SAML** en la sección Usuarios y grupos para mostrar el cuadro de diálogo Configuración de SAML.



c. Rellene los campos en la página Configuración de SAML:
   1. Compruebe que el Id. de entidad coincide con la dirección IP del servidor de gestión XClarity Administrator.
   2. Elija si desea que los metadatos generados se firmen digitalmente.

3. Elija si desea que las solicitudes de autenticación se firmen.
4. Elija si desea que las respuestas de autenticación se firmen.
5. Elija si desea que las solicitudes de resolución de artefactos que se envían al proveedor de identidad remoto se firmen.
6. Pegue los metadatos del proveedor de identidad (IDP) SAML generados por el proveedor de identidad y recuperados en el Paso 2 3 en la página 27 en el campo **Metadatos de IDP**.

d. Haga clic en **Aplicar** para aplicar los cambios y actualizar el campo Metadatos SP.

Atención: *No* seleccione **SAML habilitado** en este momento. Habilitará SAML en un paso posterior para reiniciar XClarity Administrator.

e. Copie y pegue los datos en el campo **Metadatos de SP** en un archivo y guárdelo con la extensión .XML (por ejemplo, sp_metadata.xml). Copie el archivo al host AD FS.

Paso 4. Configure AD FS.

a. Abra la herramienta de gestión AD FS.
b. Haga clic en **ADFS → Confianzas en terceros confiables**.
c. Haga clic en con el botón derecho en **Confianzas en terceros confiables** y luego haga clic en **Agregar confianza en tercero confiable** para mostrar el asistente
d. Haga clic en **Inicio**
e. En la página Seleccionar el origen de los datos, seleccione **Importar datos sobre el tercero confiable desde un archivo** y, a continuación, elija el archivo de metadatos de SP que guardó en el paso 3e.
f. Introduzca un nombre de visualización.
g. Haga clic en **Siguiente** en todas las páginas para elegir los valores predeterminados.
h. Haga clic en **Finalizar** para mostrar la página Reglas de reclamación
i. Deje la opción predeterminada de **Enviar atributos de LDAP como reclamaciones** y haga clic en **Siguiente**.
j. Introduzca un nombre de regla de reclamación.
k. Seleccione **Active Directory** para el almacenamiento de atributos.
l. Agregue una asignación. En el lado izquierdo seleccione **SAM-Account-Name** y en el lado derecho seleccione **Id. de nombre** para el tipo de reclamación saliente.
m. Agregue otra asignación. En el lado izquierdo seleccione **Token-Groups-Unqualified Names** y en el lado derecho seleccione **Grupo** para el tipo de reclamación saliente
n. Haga clic en **Aceptar**.
o. Busque la confianza que acaba de crear en la lista **Confianzas en terceros confiables**.
p. Haga clic con el botón derecho del ratón en la confianza y, a continuación, haga clic en **Seleccionar propiedades**. Aparece el cuadro de diálogo Propiedades de la confianza.
q. Haga clic en la pestaña **Avanzado** y, a continuación, seleccione `SHA-1` como el algoritmo hash seguro.

Paso 5. Guarde el certificado de servidor de AD FS.

a. Haga clic en **Consola AD FS → Servicios → Certificados**.
b. Seleccione **Certificado** en Token-signing.
c. Haga clic en con el botón derecho el certificado y haga clic en **Ver certificado**.
d. Haga clic en la pestaña **Detalles**.

e. Haga clic en **Copiar en el archivo** y guarde el certificado como un archivo binario con cifrado DER de X.509 (.CER).

f. Copie el archivo .CER del certificado de servidor en el host XClarity Administrator.

Paso 6. Importe el certificado de confianza de AD FS en la interfaz web de XClarity Administrator.

a. En la barra de menús de XClarity Administrator, haga clic en **Administración → Seguridad**.

b. Haga clic en **Certificados de confianza** en la sección Gestión de certificados.

c. Haga clic en el icono de **Crear** ( ) para añadir un certificado.

d. Seleccione el archivo .CER del certificado de servidor que guardó en el paso anterior.

e. Haga clic en **Crear**.

Paso 7. Haga clic en **Configuración de SAML**, en la sección Usuarios y grupos para mostrar el cuadro de diálogo Configuración de SAML.

Paso 8. Seleccione **SAML habilitado** para habilitar la gestión de cuentas de usuarios con el uso de un proveedor de identidad externo. Cuando esta opción está seleccionada, todas las cuentas de usuarios existen remotamente en un proveedor de identidad.

Paso 9. Haga clic en **Aplicar** para aplicar los cambios y reiniciar el servidor de gestión.

Paso 10. Espere unos minutos para que XClarity Administrator se reinicie.

Atención: No reinicie el dispositivo virtual manualmente durante este proceso.

Paso 11. Cierre el navegador web y vuelva a abrirlo.

Paso 12. Inicie sesión en la interfaz web de XClarity Administrator desde el proveedor de identidad.

Resultados

XClarity Administrator intenta probar la configuración para detectar errores comunes. Si la prueba falla, se muestran mensajes de error que indican el origen de los errores.

XClarity Administrator valida la conexión de proveedor de identidad. Si la validación se realiza correctamente, la autenticación del usuario en el proveedor de identidad se lleva a cabo al iniciar sesión en XClarity Administrator.

Configuración de un sistema de gestión de identidades externo

Un *sistema de gestión de identidades* es un almacén de contraseñas externo que se puede utilizar opcionalmente con Lenovo XClarity Administrator para almacenar XClarity Administrator y credenciales de XClarity Controller. Cuando se agrega un sistema de gestión de identidades a XClarity Administrator, XClarity Administrator recupera las contraseñas del sistema de gestión de identidades, en lugar de hacerlo de los servidores de autenticación.

Acerca de esta tarea

XClarity Administrator es compatible con el siguiente sistema de gestión de identidades.

- CyberArk

Configuración de un sistema de gestión de identidades CyberArk

CyberArk es un almacén de contraseñas externo que se puede utilizar opcionalmente con Lenovo XClarity Administrator para almacenar credenciales de XClarity Administrator y Lenovo XClarity Controller. Después de almacenar una contraseña de cuenta en CyberArk, CyberArk gestiona la contraseña

Acerca de esta tarea

XClarity Administrator le permite almacenar sus contraseñas XCC en sistemas de gestión de identidades proporcionados por CyberArk, un servicio de terceros. Lenovo no es responsable del servicio CyberArk, usted es responsable de su relación directa con 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.

Procedimiento

Para configurar XClarity Administrator para utilizar CyberArk, lleve a cabo los pasos siguientes.

Paso 1. Configure CyberArk.

1. En la barra de menús de XClarity Administrator, haga clic en **Administración → Seguridad**.
2. Haga clic en **CyberArk** en la sección Identity Management (Gestión de identidades).
3. Haga clic en **Editar los detalles del servidor CyberArk** en la barra de herramientas.
4. Especifique el nombre de host o la dirección IP de CyberArk y el número de puerto.
5. Haga clic en **Aplicar**.

Paso 2. Importe el certificado de autenticación mutua XClarity Administrator a CyberArk.

1. En la barra de menús de XClarity Administrator, haga clic en **Administración → Seguridad**.
2. Haga clic en **Certificado de servidor** en la sección Certificate Management (Gestión de certificados).
3. Haga clic en la pestaña **Certificado de cliente**.
4. Seleccione **CyberArk** como el tipo de servidor.
5. Haga clic en **Volver a generar certificado** para generar un nuevo certificado de autenticación mutua TLS para CyberArk.

   Atención: Si vuelve a generar el certificado de autenticación mutua TLS para CyberArk después de establecer una conexión entre XClarity Administrator y CyberArk, la conexión se perderá hasta que importe el certificado nuevo en CyberArk.
6. Haga clic en **Descargar certificado** y luego haga clic en **Guardar como der** o **Guardar como pem** para guardar el certificado de servidor como archivo en su sistema local.
7. Importe el certificado descargado en CyberArk.

Paso 3. Importe el certificado de CA raíz de CyberArk en XClarity Administrator.

1. Descargue el certificado de CA raíz de CyberArk.
2. En la barra de menús de XClarity Administrator, haga clic en **Administración → Seguridad**.
3. Haga clic en **Certificados de confianza** en la sección Gestión de certificados.
4. Haga clic en el icono de **Crear** ( ) para añadir un certificado.
5. Examine el archivo o pegue el texto del certificado con formato PEM.
6. Haga clic en **Crear**.

Paso 4. Agregue rutas de acceso que identifiquen la ubicación de las cuentas de usuario integradas en CyberArk.

1. En la barra de menús de XClarity Administrator, haga clic en **Administración → Seguridad**.
2. Haga clic en **CyberArk** en la sección Identity Management (Gestión de identidades).

3. Haga clic en la pestaña **Rutas**.
4. Haga clic en el icono **Crear** ( ) para mostrar el cuadro de diálogo Crear ruta de CyberArk.

5. Opcionalmente, especifique el ID de la aplicación, el seguro y la carpeta donde se almacenan las cuentas de usuario en CyberArk.

   Si especifica el ID de la aplicación y el seguro y, opcionalmente, la carpeta, XClarity Administrator intente encontrar la cuenta de usuario en la ubicación especificada.

   Si especifica una combinación de campos distintos del ID de la aplicación y el seguro (por ejemplo, si especifica solo el ID de la aplicación, solo el seguro y la carpeta o solo el ID de la aplicación y la carpeta), XClarity Administrator filtra la ruta utilizando los valores especificados.
6. Haga clic en **Aplicar**.

Después de finalizar

- Modifique una ruta de CyberArk seleccionada haciendo clic en el icono **Editar** ( ).
- Elimine una ruta de CyberArk seleccionada haciendo clic en el icono **Eliminar** ( ).

Determinar el tipo de método de autenticación que usa Lenovo XClarity Administrator

Puede determinar el tipo de método de autenticación que se usan actualmente a partir de las pestañas **Cliente LDAP** y **Configuración de SAML** en la página Seguridad.

Acerca de esta tarea

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, solo 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, solo 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.

Procedimiento

Para determinar el tipo de servidor de autenticación que usa el software de gestión, lleve a cabo los pasos siguientes.

Paso 1. En la barra de menús de XClarity Administrator , haga clic en **Administración → Seguridad**.

Paso 2. Haga clic en **Cliente LDAP** en la sección Usuarios y grupos para mostrar el cuadro de diálogo Valores de cliente LDAP.

Compruebe qué método de autenticación del usuario está seleccionado:

- **Permitir inicios de sesión de usuarios locales**. La autenticación se realiza mediante la autenticación local. Cuando se selecciona esta opción, todas las cuentas de usuario se encuentran en el servidor de autenticación local del nodo de gestión.
- **Permitir inicios de sesión de usuarios de LDAP**. Un servidor LDAP externo realiza la autenticación. Este método habilita la gestión remota de las cuentas de usuario. Cuando esta opción está seleccionada, todas las cuentas de usuarios existen remotamente en un servidor LDAP externo.
- **Permitir usuarios locales primero, luego usuarios de LDAP**. El servidor de autenticación local realiza la autenticación primero. Si esto falla, un servidor LDAP externo realiza la autenticación.
- **Permitir usuarios de LDAP primero, luego usuarios locales**. Un servidor LDAP externo realiza la autenticación primero. Si eso falla, el servidor de autenticación local realiza la autenticación.

Paso 3. Haga clic en **Configuración de SAML** en la sección Usuarios y grupos para mostrar la página Configuración de SAML.

Si se selecciona **SAML habilitado**, entonces se usa proveedor de identidad.

Acceso a Lenovo XClarity Administrator después de un error en el servidor LDAP externo

Si usa un servidor de autenticación LDAP externo y se produce un error en él o este no está disponible, use el procedimiento siguiente para recuperar el acceso a la interfaz web de Lenovo XClarity Administrator mediante el servidor de autenticación local del nodo de gestión.

Procedimiento

Para cambiar los valores del cliente LDAP, lleve a cabo los pasos siguientes.

Paso 1. Inicie sesión en la interfaz web del XClarity Administrator, utilizando una cuenta de usuario con autoridad de recuperación **lxc-recovery**. Para obtener más información sobre el nombre del dominio de cliente, consulte Configuración de un servidor de autenticación LDAP externo.

Paso 2. En la barra de menús de XClarity Administrator , haga clic en **Administración → Seguridad**.

Paso 3. Haga clic en **Cliente LDAP** en la sección Usuarios y grupos para mostrar el cuadro de diálogo Cliente LDAP.

Paso 4. Seleccione **Permitir inicios de sesión de usuarios locales** como método de autenticación de usuarios a fin de habilitar la gestión local de las cuentas de usuarios. Cuando esta opción está seleccionada, todas las cuentas de usuarios están presentes localmente en el servidor de gestión.

Paso 5. Haga clic en **Aplicar**.

Resultados

Ahora, puede usar las cuentas de usuarios del servidor de autenticación local para tener acceso al servidor de gestión de XClarity Administrator. Una vez que se restaure el servidor de autenticación externo y esté disponible para el servidor de gestión, puede cambiar el valor del cliente LDAP de modo que se vuelva a usar el servidor de autenticación externo.

Acceso a Lenovo XClarity Administrator después de un error de proveedor de identidad de SAML externo

Si usa un proveedor de identidad de SAML externo y se produce un error en él o este no está disponible, use el procedimiento siguiente para recuperar el acceso a la interfaz web de Lenovo XClarity Administrator mediante el servidor de autenticación local de XClarity Administrator.

Procedimiento

Lleve a cabo los pasos siguientes para cambiar los valores del cliente SAML.

Paso 1. Abra el navegador web en la página de inicio de sesión de XClarity Administrator (por ejemplo, `https://<ip_address>/ui/login.html`).

Paso 2. Inicie sesión en la interfaz web de XClarity Administrator mediante una cuenta de usuario de recuperación local que creó durante la configuración de proveedor de identidad.

Paso 3. En la barra de menús de XClarity Administrator , haga clic en **Administración → Seguridad**.

Paso 4. Haga clic en **Configuración de SAML** en la sección Usuarios y grupos para mostrar el cuadro de diálogo Configuración de SAML.

Paso 5. Borrar **Habilitar SAML** para deshabilitar proveedor de identidad SAML. Cuando se borra esta opción, se usa el servidor de autenticación local o el servidor LDAP externo (si está configurado) para la autenticación.

Paso 6. Haga clic en **Aplicar**.

Resultados

Ahora, puede usar las cuentas de usuarios del servidor de autenticación local para tener acceso al servidor de gestión de XClarity Administrator. Una vez que se restaure el proveedor de identidad externo y esté disponible para el servidor de gestión, puede cambiar el modo de autenticación a proveedor de identidad.

Gestión de cuentas de usuario

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

Acerca de esta tarea

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.

Nota: Las cuentas de usuario de SYSMGR_* y SYSRDR_* (donde * es un “” que se ha elegido aleatoriamente a partir de los caracteres A – Z y 0 – 9) son generadas y utilizadas por XClarity Administrator como cuentas de usuario de servicio y se utilizan en funciones como la autenticación gestionada, el despliegue del SO y las actualizaciones de firmware. Las contraseñas SYSMGR_* y SYSRDR_* se giran cada vez que se arranca XClarity Administrator y poco antes de que expire el periodo de caducidad de la contraseña.

Creación de un usuario

Las cuentas de usuarios se utilizan para gestionar la autorización y el acceso a los recursos.

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 agregar un usuario a XClarity Administrator, lleve a cabo los pasos siguientes.

Paso 1. En la barra de menús de XClarity Administrator , haga clic en **Administración → Seguridad**.

Paso 2. Haga clic en **Usuarios locales** en la sección Usuarios y grupos para mostrar el cuadro de diálogo Gestión de usuarios.

Paso 3. Haga clic en el icono **Crear** ( ) para crear un usuario. Se muestra el cuadro de diálogo Crear nuevo usuario.

Paso 4. Rellene la siguiente información en el cuadro de diálogo.

- 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 personalizado.
- 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 5. Haga clic en **Crear**.

Después de finalizar

La cuenta de usuario se muestra en la tabla Gestión de usuarios. La tabla muestra los grupos de roles asociados y el estado de cuenta de cada cuenta de usuario.

Una vez que haya creado una cuenta de usuario, puede realizar las siguientes acciones en una cuenta de usuario seleccionada:

- Modificar el nombre de usuario, la descripción y el rol de la cuenta de usuario pulsando el icono **Editar** ( ).
- Eliminar la cuenta de usuario pulsando el icono **Eliminar** ( ).
- Restablecer la contraseña de la cuenta de usuario (consulte Restablecimiento de la contraseña de un usuario).
- Desbloquear la cuenta (consulte Desbloqueo de un usuario).
- Habilitar o deshabilitar una cuenta de usuario (consulte Habilitación o deshabilitación de un usuario).

Habilitación o deshabilitación de un usuario

Puede habilitar o deshabilitar una cuenta de usuario local en el servidor de autenticación.

Procedimiento

Para habilitar o deshabilitar una cuenta de usuario, lleve a cabo los pasos siguientes.

- Si se utiliza el servidor de autenticación local:
  1. En la barra de título de Lenovo XClarity Administrator, haga clic en **Administración → Seguridad**.
  2. Haga clic en **Usuarios locales** en la sección Usuarios y grupos para mostrar el cuadro de diálogo Gestión de usuarios.

3. Seleccione una cuenta de usuario.
4. Si la cuenta de usuario está habilitada, haga clic en **Todas las acciones → Deshabilitar cuenta seleccionada** para deshabilitar el usuario. El estado de cuenta de la tabla cambia a `Disabled`.
5. Si la cuenta de usuario está deshabilitada, haga clic en **Todas las acciones → Habilitar cuenta seleccionada** para habilitar el usuario. El estado de cuenta de la tabla cambia a `Enabled`.

- Si se utiliza un servidor LDAP externo, habilite o deshabilite la cuenta de usuario en Microsoft Active Directory.
- Si se utiliza un proveedor de identidad SAML externo, habilite o deshabilite una cuenta de usuario en el proveedor de identidad.

Cerrar la sesión de un usuario activo

Puede cerrar la sesión (finalizar) a un usuario activo de Lenovo XClarity Administrator.

Debe tener iniciada la sesión en XClarity Administrator utilizando una cuenta de usuario con autoridad de **lxc-supervisor** o **lxc-security-admin**.

Procedimiento

Para cerrar la sesión de un usuario activo, lleve a cabo estos pasos.

Paso 1. En la barra de título de XClarity Administrator, haga clic en **Administración → Seguridad**.

Paso 2. Pulse **Sesiones activas** en la sección Usuarios y grupos para mostrar el cuadro de diálogo Gestión de sesiones activas.

Paso 3. Seleccione una o varias cuentas de usuarios.

Paso 4. Haga clic en **Cerrar sesión del usuario**.

Cambio de contraseña de una cuenta de usuario

Puede cambiar la contraseña de su cuenta de usuario.

Procedimiento

Lleve a cabo los pasos siguientes para cambiar la contraseña.

- Si se utiliza el servidor de autenticación local:
  1. Desde la barra de título de Lenovo XClarity Administrator, haga clic en el menú de acción de usuario (

) y haga clic en **Cambiar contraseña**. Se muestra el cuadro de diálogo Cambiar contraseña.

2. Especifique la contraseña actual.
3. 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.
4. Haga clic en **Cambiar**.

- Si se utiliza un servidor de autenticación externo, cambie la contraseña en Microsoft Active Directory.

  Atención: Si actualiza Microsoft Active Directory con una nueva contraseña de la cuenta de cliente usada para enlazar XClarity Administrator con el servidor de autenticación externo, asegúrese de actualizar también la nueva contraseña en la interfaz web de XClarity Administrator (consulte Configuración de un servidor de autenticación LDAP externo).
- Si usa un proveedor de identidad SAML externo, cambie su contraseña en el proveedor de identidad.

Restablecimiento de la contraseña de un usuario

Puede restablecer la contraseña de cualquier cuenta de usuario.

Procedimiento

Para restablecer una contraseña, lleve a cabo los pasos siguientes.

- Si se utiliza el servidor de autenticación local, restablezca la contraseña desde la interfaz web de Lenovo XClarity Administrator:
  1. En la barra de menús de XClarity Administrator , haga clic en **Administración → Seguridad**.
  2. Haga clic en **Usuarios locales** en la sección Usuarios y grupos para mostrar el cuadro de diálogo Gestión de usuarios.
  3. Seleccione una cuenta de usuario de la tabla.
  4. Si la cuenta de usuario está habilitada, haga clic en **Todas las acciones → Restablecer contraseña del usuario seleccionado**. Se muestra el cuadro de diálogo Restablecer contraseña.
     a. 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.

b. Opcionalmente, establezca **Cambiar al acceder por primera vez** en `Yes` si desea obligar al usuario a cambiar la contraseña la primera vez que inicie sesión en XClarity Administrator.
c. Haga clic en **Restablecer**.

- Si se utiliza un servidor LDAP externo, restablezca la contraseña en Microsoft Active Directory.
- Si se usa un proveedor de identidad SAML externo, restablezca la contraseña en el proveedor de identidad.
- Si no puede iniciar sesión en XClarity Administrator utilizando otra cuenta de supervisor o si no existe otra cuenta del supervisor, puede restablecer la contraseña de un usuario local con autoridad de recuperación o de supervisor montando una imagen ISO que contiene un archivo de configuración con la nueva contraseña. Para obtener más información, consulte Se olvidó la contraseña de recuperación local o de usuario supervisor en la documentación en línea de XClarity Administrator.

Desbloqueo de un usuario

Puede desbloquear una cuenta de usuario que se haya bloqueado en Lenovo XClarity Administrator. Una cuenta de usuario puede bloquearse temporalmente si el usuario realiza demasiados intentos de inicio de sesión no válidos.

Acerca de esta tarea

Los valores de seguridad de la cuenta de usuario controlan la cantidad de tiempo que debe transcurrir antes de que un usuario que ha sido bloqueado pueda intentar iniciar sesión de nuevo. Si el valor de **Periodo de bloqueo por número máximo de errores de inicio de sesión** está establecido en `0`, la cuenta de usuario permanecerá bloqueada hasta que el administrador la desbloquee expresamente. Para obtener más información sobre el periodo de bloqueo por número máximo de errores de inicio de sesión, consulte Cambio de los valores de seguridad de una cuenta de usuario.

También puede habilitar o deshabilitar permanentemente una cuenta de usuario. Para obtener más información, consulte el apartado Habilitación o deshabilitación de un usuario.

Nota: Para desbloquear una cuenta de usuario debe tener autoridad de Supervisor.

Consejo: puede utilizar XClarity Administrator para desbloquear las cuentas de usuario que se gestionan utilizando el servidor de autenticación local. No puede desbloquear las cuentas de usuario de un servidor de autenticación externo mediante XClarity Administrator.

Procedimiento

Para desbloquear una cuenta de usuario, lleve a cabo los pasos siguientes.

- Si se utiliza el servidor de autenticación local:
  1. En la barra de menús de XClarity Administrator , haga clic en **Administración → Seguridad**.
  2. Haga clic en **Usuarios locales** en la sección Usuarios y grupos para mostrar el cuadro de diálogo Gestión de usuarios.
  3. Seleccione la cuenta de usuario en la tabla.
  4. Haga clic en **Todas las acciones → Desbloquear cuenta para el usuario seleccionado**.
- Si se utiliza un servidor LDAP externo, desbloquee la cuenta de usuario en Microsoft Active Directory.
- Si se usa un proveedor de identidad SAML externo, desbloquee la cuenta de usuario en el proveedor de identidad.

Supervisión de usuarios activos

Desde la página Panel puede determinar los usuarios que han iniciado una sesión en la interfaz web de Lenovo XClarity Administrator.

Procedimiento

- Puede obtener una lista de usuarios activos y sus direcciones IP haciendo clic en **Panel** en la barra de menú de XClarity Administrator.

  Las sesiones de usuario activas se enumeran en la sección Actividad.

- Puede obtener una lista de todos los usuarios activos (fuera del usuario actual) y sus direcciones IP haciendo clic en **Administración → Seguridad** en la barra de menú de XClarity Administrator y luego haga clic en **Sesiones activas**.

  Nota: Las sesiones de usuario que están inactivas por más tiempo que el período de tiempo determinado se desconectan automáticamente. Puede establecer el periodo de inactividad haciendo clic en **Administración → Seguridad** desde la barra de menú de XClarity Administrator, haga clic en Valores de seguridad de la cuenta y luego ajuste el valor **Tiempo de espera por inactividad de sesión web**. Tenga en cuenta que el cambio no afecta a las sesiones activas del usuario. Solo afecta a las sesiones de usuario que se inician después de cambiar el valor.

Gestión de credenciales almacenadas

Se usan *credenciales almacenadas* para gestionar la autorización y acceso a los chasis y servidores gestionados por Lenovo XClarity Administrator mediante la autenticación local.

Antes de empezar

Debe tener autoridad de **lxc-supervisor** o **lxc-security-admin** para crear, modificar o eliminar credenciales almacenadas.

Acerca de esta tarea

Una credencial almacenada debe corresponder con una cuenta de usuario local en un dispositivo o con una cuenta de usuario en un servidor de Active Directory.

Si elige gestionar dispositivos mediante autenticación local en lugar de autenticación gestionada de XClarity Administrator, debe seleccionar una cuenta de credenciales almacenadas durante el proceso de gestión.

Importante: XClarity Administrator no valida el nombre de usuario y la contraseña que se especificó para la credencial almacenada. Es responsabilidad del usuario asegurarse de que la información especificada corresponda con una cuenta de usuario activa en el dispositivo local o en Active Directory (si el dispositivo gestionado está configurado para utilizar Active Directory para la autenticación).

Atención: Las credenciales almacenadas deben tener acceso de supervisor o la autoridad suficiente para realizar cambios de configuración en el dispositivo. Si intenta gestionar un servidor con credenciales almacenadas que no tienen la autoridad suficiente en el dispositivo, el proceso de gestión puede realizarse correctamente, pero se pueden producir errores en acciones de inventario administrativas adicionales en el dispositivo, debido a errores de acceso denegado, lo que puede conducir a problemas de conectividad percibidos con el dispositivo.

Procedimiento

Para agregar una credencial almacenada a XClarity Administrator, lleve a cabo los pasos siguientes.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Administración → Seguridad**. Se muestra la página Seguridad.

Paso 2. Haga clic en **Credenciales almacenadas** en la sección Autenticación gestionada para mostrar la página Credencial almacenada.

Paso 3. Haga clic en el icono **Crear** ( ) para crear una credencial almacenada. Se muestra el cuadro de diálogo Create New Stored Credentials (Crear nuevas credenciales almacenadas)

Paso 4. Rellene la siguiente información en el cuadro de diálogo.
- Escriba un nombre de usuario y una descripción opcional de la credencial almacenada.
- Introduzca y confirme la contraseña de la credencial almacenada.
- De manera opcional, introduzca y, a continuación, confirme las credenciales de recuperación almacenadas RECOVERY_ID.

Paso 5. Haga clic en **Crear una credencial almacenada**.

Después de finalizar

Se muestra la cuenta de credencial almacenada en la tabla Credencial almacenada. La tabla muestra el Id. y la descripción asociada a cada cuenta de credencial almacenada.

Desde la página Credenciales almacenadas, también puede realizar las acciones siguientes en una cuenta de credencial almacenada:

- Modificar el nombre de usuario, contraseña y descripción de una cuenta de credencial almacenada al hacer clic en el icono **Editar** ( ).

  Nota: Si gestiona un dispositivo utilizando una credencial almacenada y habilita la autenticación gestionada, no puede editar la credencial.

- Eliminar la cuenta de credencial almacenada al hacer clic en el icono **Eliminar** ( ).

Para resolver credenciales almacenadas caducadas o no válidas, consulte Resolución de credenciales almacenadas caducadas o no válidas para un servidor.

Funciones de gestión y grupos de roles

Un *rol* se utiliza para controlar el acceso de usuario a los recursos y para limitar las acciones que pueden realizar con ellos. 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 Lenovo XClarity Administrator debe ser miembro al menos de un grupo de roles.

Creación de un rol personalizado

Un *rol* es un conjunto de *privilegios*, o permisos para realizar una acción específica. Lenovo XClarity Administrator incluye varios roles predefinidos (predeterminados). También puede crear roles personalizados que hacen cumplir un único conjunto de privilegios de que los usuarios pueden realizar.

Antes de empezar

Debe tener autoridad de **lxc-supervisor** o **lxc-security-admin** para realizar esta tarea.

Acerca de esta tarea

Para crear un rol personalizado, seleccione uno o varios roles predefinidos que tengan el alcance más cercano al rol que desee crear y luego borre los privilegios individuales que desee restringir. De este modo se garantiza que se obtengan todos los privilegios que se van a realizar y que el rol se construye correctamente con privilegios dependientes.

Algunos privilegios XClarity Administrator dependen de los privilegios del módulo de gestión correspondientes para realizar acciones en los dispositivos gestionados (consulte Privilegios de módulo de gestión v1 y Privilegios de módulo de gestión v2). Un privilegio XClarity Administrator puede permitirle solicitar una acción en un dispositivo gestionado, pero el dispositivo rechazará la solicitud si no dispone de

los privilegios correspondientes para el CMM, el IMM o XCC. Por ejemplo, si crea un rol personalizado para realizar acciones de alimentación en dispositivos gestionados, debe añadir el privilegio **lxc-inventory-modify-device-power-state** y:

- Para un servidor ThinkSystem en un bastidor, añada el privilegio **mm-power-and-restart-access-v1**.
- Para un chasis de Flex System completo (incluidos los dispositivos del chasis), añada el privilegio **mm-power-and-restart-access-v1**.
- Para un servidor ThinkSystem en un chasis, añada **mm-power-and-restart-access-v1**, **mm-blade-operator-v2** y el privilegio **mm-blade-#-scope-v2** que coincide con el servidor de destino.

Todos los roles contienen privilegios de solo lectura. Ningún rol personalizado puede ser más restrictivo que el rol de **lxc-operator**.

Si un usuario no tiene privilegios para realizar acciones específicas, los elementos del menú, los iconos de la barra de herramientas y los botones que ejecutan esas acciones están deshabilitados (atenuados).

XClarity Administrator proporciona un grupo de roles para cada rol predefinido, utilizando el mismo nombre que el rol. Considere la posibilidad de crear un grupo de roles para los nuevos roles que cree. Para obtener más información acerca de los grupos de roles, consulte Creación de un grupo de roles personalizado.

- **lxc-supervisor**. Los usuarios que tienen asignado este rol pueden acceder, configurar y realizar todas las operaciones disponibles en el servidor de gestión y en todos los dispositivos gestionados.Los usuarios que tienen asignado este rol siempre tienen acceso a todos los dispositivos gestionados. No se puede restringir el acceso a los dispositivos para este rol.
- **lxc-admin**. Los usuarios que tienen asignado este rol pueden modificar los valores no relacionados con la seguridad y realizar todas las operaciones no relacionadas con la seguridad en el servidor de gestión, incluida la capacidad para actualizar y reiniciar el servidor de gestión. Este rol también proporciona la capacidad para ver toda la información de estado y configuración en el servidor de gestión y en los dispositivos gestionados.
- **lxc-security-admin**. Los usuarios que tienen asignado este rol pueden modificar los valores de seguridad y realizar las operaciones relacionadas con la seguridad en el servidor de gestión y en todos los dispositivos gestionados. Este rol también proporciona la capacidad para ver toda la información de estado y configuración en el servidor de gestión y en los dispositivos gestionados.

  Los usuarios que tienen asignado este rol siempre tienen acceso a todos los dispositivos gestionados. No se puede restringir el acceso a los dispositivos para este rol.
- **lxc-hw-admin**. Los usuarios que tienen asignado este rol pueden modificar los valores no relacionados con la seguridad y realizar las operaciones no relacionadas con la seguridad en los dispositivos gestionados, incluida la capacidad para actualizar y reiniciar los dispositivos gestionados. Este rol también proporciona la capacidad para ver toda la información de estado y configuración en el servidor de gestión y en todos los dispositivos gestionados.
- **lxc-fw-admin**. Los usuarios a quienes se les asigna este rol pueden crear políticas de firmware y desplegarlas en los dispositivos gestionados. Los usuarios que no están asignados a este rol solo pueden ver información de la política.
- **lxc-os-admin**. Los usuarios a quienes se les asigna este rol pueden descargar y desplegar sistemas operativos y actualizaciones de controladores de dispositivos en los servidores gestionados. Los usuarios que no están asignados a este rol solo pueden ver información del sistema operativo y el controlador de dispositivo.
- **lxc-service-admin**. Los usuarios que se asignaron este rol pueden recopilar y descargar archivos de servicio para XClarity Administrator y los dispositivos gestionados. Los usuarios que no están asignados a este rol pueden recopilar, pero no descargar datos de servicio.
- **lxc-hw-manager**. Los usuarios que tienen asignado este rol pueden detectar nuevos dispositivos y dejarlos bajo el control de gestión de XClarity Administrator. Este rol prohíbe a los usuarios realizar operaciones o modificar los valores de las configuraciones en el servidor de gestión y los dispositivos gestionados, más allá de dichas operaciones necesarias para detectar y gestionar dispositivos nuevos.

- **lxc-operator**. Los usuarios que tienen asignado este rol pueden ver toda la información de estado y configuración del servidor de gestión y en los dispositivos gestionados. Este rol prohíbe a los usuarios realizar cualquier operación o modificar los valores de configuración en el servidor de gestión y en dispositivos gestionados.
- **lxc-recovery**. Los usuarios que tienen asignado este rol pueden modificar los valores de seguridad y realizar las operaciones relacionadas con la seguridad en el servidor de gestión. Estos usuarios también se pueden autenticar directamente en XClarity Administrator incluso si el método de autenticación se configura en un servidor LDAP externo. Este rol proporciona un mecanismo de recuperación en caso de que ocurra un error de comunicación con el servidor LDAP externo que utiliza la configuración de "Credenciales de inicio de sesión".

  Los usuarios que tienen asignado este rol siempre tienen acceso a todos los dispositivos gestionados. No se puede restringir el acceso a los dispositivos para este rol.

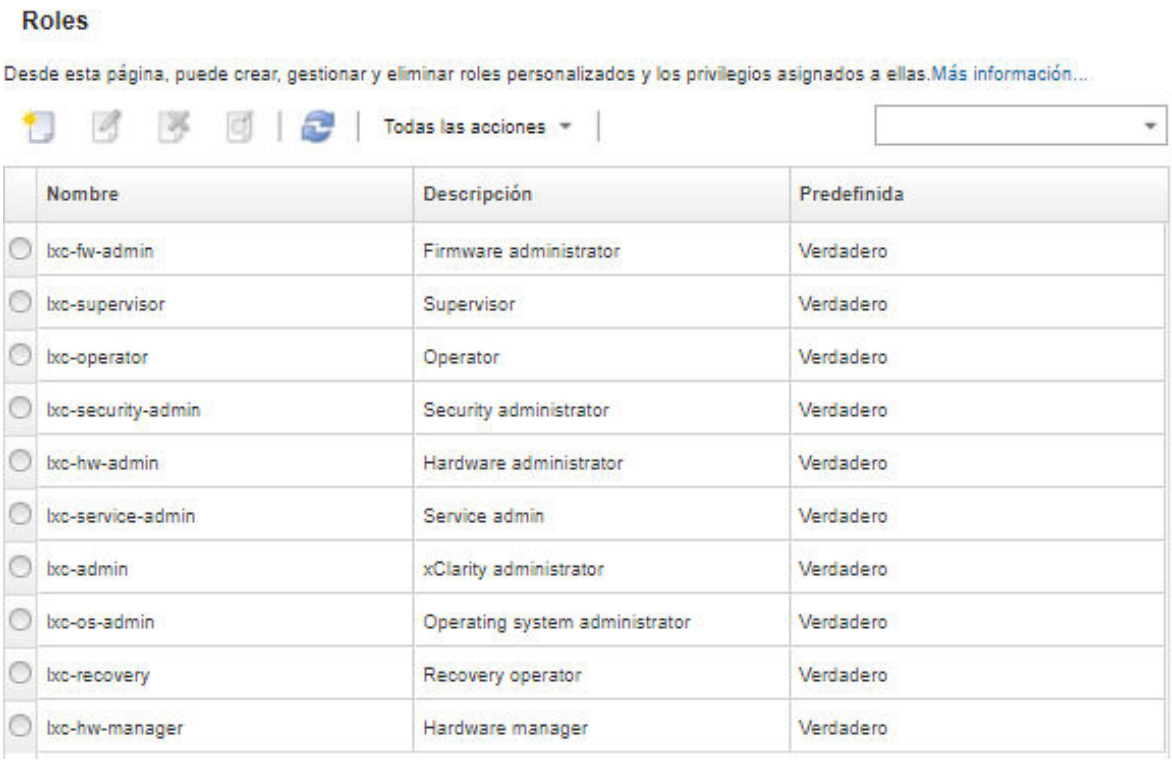
Los siguientes roles predefinidos están *reservados* y no se pueden usar para crear nuevos grupos de roles o asignarse a nuevos usuarios.
- **lxc-sysrdr**
- **lxc-sysmgr**

Procedimiento

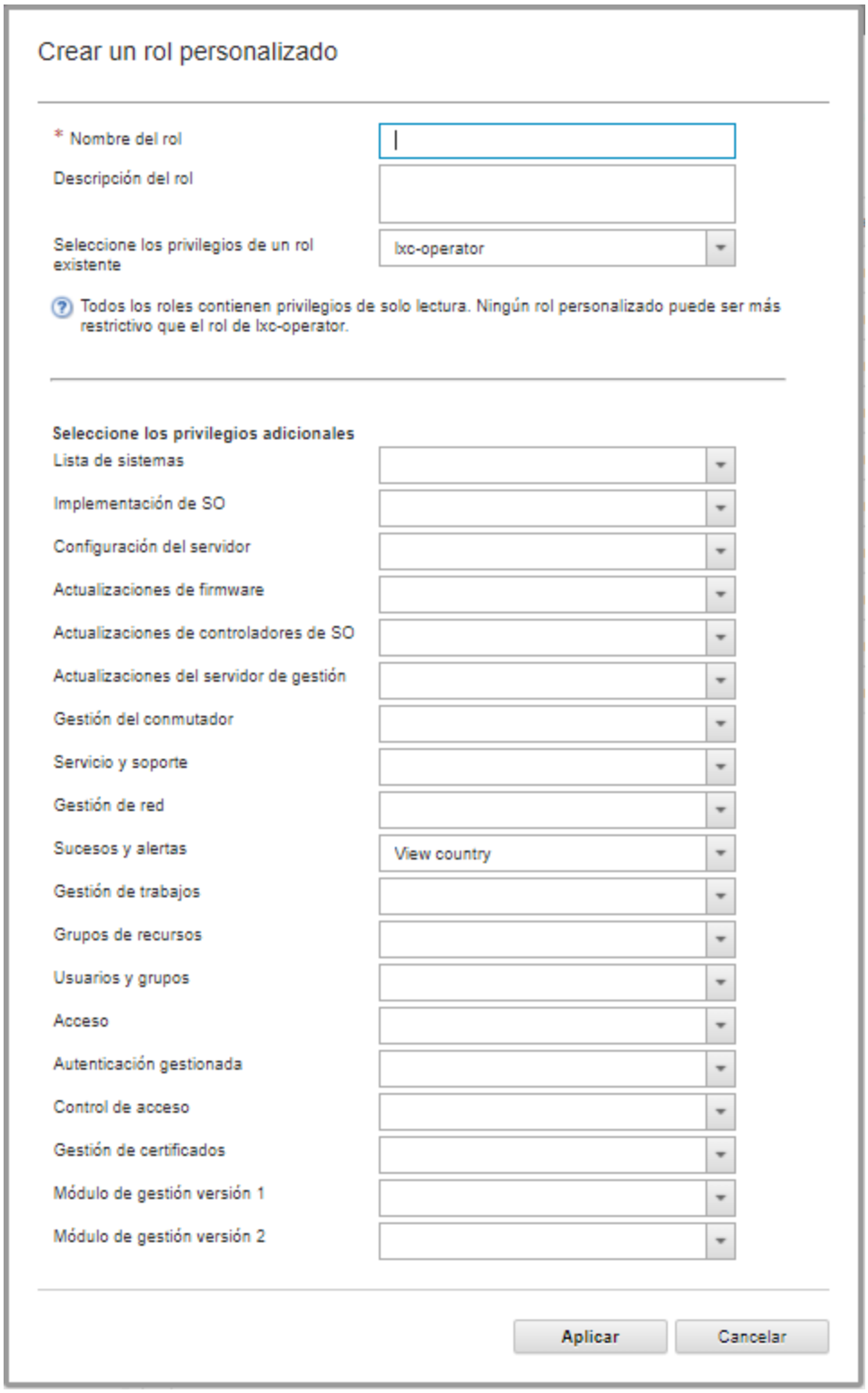
Para crear un rol personalizado, complete los pasos siguientes.

Paso 1. En la barra de menús de XClarity Administrator , haga clic en **Administración → Seguridad**.

Paso 2. Haga clic en **Roles** en la sección Usuarios y grupos para mostrar el cuadro de diálogo Gestión de roles.



Paso 3. Haga clic en el icono **Crear** ( ) para crear un rol. Se muestra el cuadro de diálogo Create Custom Role Crear rol predeterminado.



Paso 4. Escriba un nombre de rol y una descripción.

Paso 5. Seleccione un rol predefinido que se usará como punto de partida para este rol personalizado.

Si selecciona un rol existente, los privilegios que están asociados con esa función se seleccionan en el cuadro de diálogo.

Paso 6. Modificar los privilegios para el nuevo rol activando o desactivando privilegios del menú desplegable **Seleccionar privilegios adicionales**.

Nota: Si selecciona todos los privilegios de categoría específica y se agregan privilegios se añaden la categoría al actualizar o mejorar XClarity Administrator, los nuevos privilegios se agregan automáticamente al rol personalizado

Paso 7. Haga clic en **Crear**. El rol nuevo se añade a la tabla de la página Gestión de roles.

Resultados

También puede llevar a cabo las siguientes acciones.

- Ver los privilegios asociados con un rol específico seleccionando el rol y pulsando el ícono **Ver** ( ).
- Cambiar el nombre del rol personalizado o editarlo haciendo clic en el icono **Editar** ( ). Cuando se modifica un rol personalizado, puede cambiar los privilegios seleccionados, la descripción y la lista de usuarios que están asociados con el rol.

  Nota: No puede modificar un rol predefinido
- Eliminar el grupo de roles predefinido o personalizado haciendo clic en el icono **Eliminar** ( ).
- Agregar o eliminar las funciones de un grupo de roles (consulte Agregar y quitar varios usuarios desde un grupo de roles).
- Restaurar todos los roles predefinidos que se hayan eliminado haciendo clic en **Todas las acciones → Restaurar roles predeterminados**.

Privilegios predefinidos

Lenovo XClarity Administrator proporciona un conjunto de *privilegios* (permisos) que permite al usuario a realizar una acción específica. Los privilegios están organizados en categorías en función del tipo de acción.

Privilegios de acceso

Estos privilegios proporcionan permisos para modificar los modos criptográficos y SSL/TLS.

Nombre de privilegio	Descripción de privilegio	roles predeterminados
lxc-sec-apply-crypto-settings	Aplicar valores de criptografía	lxc-recovery, lxc-security-admin, lxc-supervisor

Privilegios de control de acceso

Estos privilegios proporcionan permisos para controlar el acceso a los recursos.

Nombre de privilegio	Descripción de privilegio	roles predeterminados
lxc-sec-modify-resource-access-control	Editar valores de control de acceso remoto	lxc-recovery, lxc-security-admin, lxc-supervisor

Privilegios de gestión de certificados

Estos privilegios proporcionan permisos para gestionar certificados de seguridad en Lenovo XClarity Administrator.

Nombre de privilegio	Descripción de privilegio	Roles predeterminados
lxc-sec-add-external-certificates	Añadir un certificado externo	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-add-trusted-certificates	Agregar un certificado de confianza	lxc-recovery, lxc-security-admin, lxc-supervisor

Nombre de privilegio	Descripción de privilegio	Roles predeterminados
lxc-sec-certificate-signing	Generar solicitud de firma de certificado	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-delete-external-certificates	Eliminar un certificado externo existente	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-delete-trusted-certificates	Eliminar un certificado existente	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-download-ca	Descargar certificado raíz de entidad de certificación	lxc-admin, lxc-hw-admin, lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-download-server-certificate	Descargar certificado de servidor	lxc-admin, lxc-hw-admin, lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-certificate-revocation-list	Modifica o reemplaza la lista de revocación de certificados	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-regenerate-ca	Volver a generar certificado raíz de entidad de certificación	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-regenerate-download-ca	Volver a generar certificado raíz de entidad de certificación	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-regenerate-server-certificate	Volver a generar certificado de servidor	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-resolve-untrusted-certificates	Resolver certificados no fiables	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-upload-server-certificate	Cargar certificado de servidor	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc_sec_view_certpol_settings	Ver valores de la política de certificados	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
lxc_sec_apply_certpol_settings	Aplicar valores de la política de certificados	lxc-security-admin, lxc-supervisor

Privilegios de supervisión y sucesos

Estos privilegios proporcionan permisos para gestionar los sucesos y alertas.

Nombre de privilegio	Descripción de privilegio	Roles predeterminados
lxc-event-audit	Gestionar evento y registros de auditoría	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-monitoring-create-edit-event-forwarders	Crear y modificar reenviadores de eventos	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-monitoring-create-edit-push-services	Crear y modificar los servicios de notificaciones automáticas	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-monitoring-remove-event-forwarders	Eliminar despachadores de sucesos	lxc-admin, lxc-hw-admin, lxc-supervisor

Nombre de privilegio	Descripción de privilegio	Roles predeterminados
lxc-monitoring-remove-push-services	Eliminar los servicios de notificaciones automáticas	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-monitoring-set-event-thresholds	Establecer umbrales de sucesos	lxc-admin, lxc-hw-admin, lxc-supervisor

Privilegios de actualizaciones de firmware

Estos privilegios proporcionan permisos para gestionar y aplicar las actualizaciones de firmware y los UpdateXpress System Packs.

Nombre de privilegio	Descripción de privilegio	roles predeterminados
lxc-fwUpdates-apply-assign-policy	Asignar una política de cumplimiento de firmware a dispositivos	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-apply-perform-updates	Realizar actualizaciones de firmware	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-policies-create-policies	Crear, copiar, editar e importar políticas de cumplimiento de firmware	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-policies-delete-policies	Eliminar políticas de cumplimiento	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-repository-delete-packages	Eliminar paquetes de actualización de firmware	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-repository-download-packages	Descargar e importar paquetes de actualización de firmware y el catálogo de actualización de los paquetes de actualización de firmware	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-repository-export-packages	Exportar paquetes de actualización de firmware	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor

Privilegios de grupo de recursos

Estos privilegios proporcionan permisos para utilizar grupos de recursos.

Nombre de privilegio	Descripción de privilegio	Roles predeterminados
lxc-resource-create-edit-group	Crear y modificar grupos de recursos	lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-resource-delete-group	Eliminar grupos de recursos	lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor

Privilegios de inventario

Estos privilegios proporcionan permisos para detectar y gestionar dispositivos y ver el inventario del dispositivo.

Nombre de privilegio	Descripción de privilegio	roles predeterminados
lxc-dm-manage-device	Gestionar chasis, servidores, almacenamiento y conmutadores	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-dm-modify-ip-settings	Habilitar o deshabilitar la comprobación de direcciones IP duplicadas en la misma subred	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-inventory-modify-device-power-state	Modificar estado de alimentación de botes, CMM, nodos, almacenamiento y conmutadores	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-inventory-modify-device-properties	Modificar propiedades de gabinetes, botes, chasis, CMM, nodos, almacenamiento y conmutadores	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-inventory-modify-node-pfa-config-settings	Modificar los valores de configuración de alertas de falla prevista (PFA)	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor

Privilegios de gestión de trabajos

Estos privilegios proporcionan permisos para gestionar trabajos (tareas).

Nombre de privilegio	Descripción de privilegio	Roles predeterminados
lxc-tasks-remove-jobs	Eliminar trabajos	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-tasks-schedule-jobs	Programar trabajos	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor

Privilegios de autenticación gestionada

Estos privilegios proporcionan permisos para gestionar la autenticación, incluidas las credenciales almacenadas.

Nombre de privilegio	Descripción de privilegio	roles predeterminados
lxc-sec-delete-stored-credentials	Eliminar las credenciales almacenadas	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-stored-credentials	Edtiar las credenciales almacenadas existentes	lxc-recovery, lxc-security-admin, lxc-supervisor

Privilegios de módulo de gestión v1

Estos privilegios están asociados con los bits de permisos LDAP (bitstrings) que se aplican a los módulos de gestión de los servidores de bastidor y a todo el chasis de Flex System (incluidos todos los dispositivos de ese chasis).

Lenovo XClarity Administrator no aplica estos permisos. Los permisos son aplicados por los dispositivos gestionados que utilizan una cuenta de uso de XClarity Administrator.

Si el dispositivo se gestiona mediante la *autenticación gestionada* (mediante el servidor de autenticación local para la autenticación), el servidor de autenticación local utiliza estos permisos para indicar a los dispositivos gestionados los permisos que debe otorgar al usuario cuando inicie sesión en el dispositivo.

Debe configurar los mismos permisos en un servidor LDAP externo. Cuando utilice un servidor LDAP externo con XClarity Administrator, asegúrese de agregar grupos en el servidor LDAP externo con nombres que

coincidan con los nombres de grupo de roles en XClarity Administrator y de que los usuarios LDAP externos se agreguen a uno o más de esos grupos. Los usuarios LDAP externos deben formar parte de un grupo de LDAP con un nombre que coincida con un grupo de roles XClarity Administrator que contenga roles asociados con las cadenas de bits del módulo de gestión. XClarity Administrator utiliza estos grupos para enlazar los usuarios LDAP externos a los grupos de roles en XClarity Administrator y a las cadenas de bits forzadas por el módulo de gestión. Luego, cuando un usuario inicia sesión en un dispositivo gestionado mediante una cuenta de usuario LDAP externa, el módulo de gestión sabe si debe otorgar privilegios de supervisor u operador de usuario.

Nota: Los privilegios del módulo de gestión v1 no se admiten para los conmutadores FlexSystem que no tienen habilitado el IOM seguro, conmutadores RackSwitch, dispositivos de almacenamiento y servidores ThinkServer.

Para obtener información acerca de los bits de permisos de LDAP para cada módulo de gestión, consulte la documentación en línea.
- Configuración de LDAP en la documentación en línea de CMM y CMM2
- Configuración de LDAP en la documentación en línea de IMM e IMM2
- Configuración de LDAP en la documentación en línea de XCC

Nombre de privilegio	Descripción de privilegio	roles predeterminados
mm-advanced-adaptor-configuration-v1	Configuración avanzada del adaptador	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-basic-configuration-v1	Configuración básica	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-clear-event-logs-v1	Borrar registros de sucesos	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-deny-always-v1	Rechazar siempre	lxc-admin, lxc-hw-admin, lxc-supervisor
mm-networking-and-security-v1	Redes y seguridad	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-power-and-restart-access-v1	Acceso de encendido/reinicio para los servidores y conmutadores Flex	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-remote-console-access-v1	Acceso de control remoto para servidores	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-remote-console-and-virtual-media-access-v1	Acceso de consola remota y medios virtuales para servidores	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-supervisor-v1	Acceso de supervisor	lxc-admin, lxc-hw-admin, lxc-supervisor
mm-user-account-management-v1	Gestión de usuarios	lxc-admin, lxc-hw-admin, lxc-recovery, lxc-security-admin, lxc-supervisor

Privilegios de módulo de gestión v2

Estos privilegios están asociados con los bits de permisos LDAP (bitstrings) que se aplican a los módulos de gestión de los dispositivos FlexSystem y ThinkSystem individuales en un chasis (chasis, servidores y conmutadores con Secure IOM habilitado).

Lenovo XClarity Administrator no aplica estos permisos. Los permisos son aplicados por los dispositivos gestionados que utilizan una cuenta de uso de XClarity Administrator.

Si el dispositivo se gestiona mediante la *autenticación gestionada* (mediante el servidor de autenticación local para la autenticación), el servidor de autenticación local utiliza estos permisos para indicar a los dispositivos gestionados los permisos que debe otorgar al usuario cuando inicie sesión en el dispositivo.

Debe configurar los mismos permisos en un servidor LDAP externo. Cuando utilice un servidor LDAP externo con XClarity Administrator, asegúrese de agregar grupos en el servidor LDAP externo con nombres que coincidan con los nombres de grupo de roles en XClarity Administrator y de que los usuarios LDAP externos se agreguen a uno o más de esos grupos. Los usuarios LDAP externos deben formar parte de un grupo de LDAP con un nombre que coincida con un grupo de roles XClarity Administrator que contenga roles asociados con las cadenas de bits del módulo de gestión. XClarity Administrator utiliza estos grupos para enlazar los usuarios LDAP externos a los grupos de roles en XClarity Administrator y a las cadenas de bits forzadas por el módulo de gestión. Luego, cuando un usuario inicia sesión en un dispositivo gestionado mediante una cuenta de usuario LDAP externa, el módulo de gestión sabe si debe otorgar privilegios de supervisor u operador de usuario.

Notas:

- También debe especificar los privilegios del módulo de gestión v1 para todo el chasis (consulte Privilegios de módulo de gestión v1).
- Los privilegios del módulo de gestión v2 no se admiten para los conmutadores FlexSystem que no tienen habilitado Secure IOM.
- Para chasis Lenovo ThinkSystem, asegúrese de que IMM2 esté configurado para permitir que el rol personalizado tenga “Administración de nodo”. Si desea que el rol personalizado tenga control de todos los dispositivos en el Lenovo ThinkSystem Chassis, asegúrese de que el IMM2 esté configurado para permitir que el rol personalizado tenga también “Alcance del nodo X”

Para obtener información acerca de los bits de permisos de LDAP para cada módulo de gestión, consulte la documentación en línea.
- Configuración de LDAP en la documentación en línea de CMM y CMM2
- Configuración de LDAP en la documentación en línea de IMM e IMM2
- Configuración de LDAP en la documentación en línea de XCC

Nombre de privilegio	Descripción de privilegio	Roles predeterminados
mm-blade-1-scope-v2	Alcance de nodo 1	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-2-scope-v2	Alcance de nodo 2	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-3-scope-v2	Alcance de nodo 3	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-4-scope-v2	Alcance de nodo 4	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-5-scope-v2	Alcance de nodo 5	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-6-scope-v2	Alcance de nodo 6	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-7-scope-v2	Alcance de nodo 7	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor

Nombre de privilegio	Descripción de privilegio	Roles predeterminados
mm-blade-8-scope-v2	Alcance de nodo 8	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-9-scope-v2	Alcance de nodo 9	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-10-scope-v2	Alcance de nodo 10	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-11-scope-v2	Alcance de nodo 11	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-12-scope-v2	Alcance de nodo 12	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-13-scope-v2	Alcance de nodo 13	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-14-scope-v2	Alcance de nodo 14	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-administration-v2	Administración de nodo	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-configuration-v2	Configuración de nodo	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-operator-v2	Operador de blade	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-remote-presence-v2	Presencia remota de nodo	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-chassis-administration-v2	Administración del chasis	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-chassis-configuration-v2	Configuración del chasis	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-chassis-log-management-v2	Gestión de cuenta de registro de chasis	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-chassis-operator-v2	Operador de chasis	lxc-admin, lxc-hw-admin, lxc-supervisor
mm-chassis-scope-v2	Alcance de chasis	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-chassis-user-account-management-v2	Gestión de usuarios	lxc-admin, lxc-hw-admin, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-deny-always-v2	Rechazar siempre	lxc-admin, lxc-hw-admin, lxc-supervisor
mm-io-module-1-scope-v2	Alcance de módulo de E/S 1	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-io-module-2-scope-v2	Alcance de módulo de E/S 2	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor

Nombre de privilegio	Descripción de privilegio	Roles predeterminados
mm-io-module-3-scope-v2	Alcance de módulo de E/S 3	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-io-module-4-scope-v2	Alcance de módulo de E/S 4	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-switch-administration-v2	Administración de conmutador	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-switch-configuration-v2	Configuración de conmutador	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-switch-operator-v2	Operador de conmutador	lxc-admin, lxc-hw-admin, lxc-supervisor
mm-supervisor-v2	Acceso de supervisor	lxc-admin, lxc-hw-admin, lxc-supervisor

Privilegios de servidor de gestión

Estos privilegios proporcionan permisos para actualizar el servidor de gestión.

Nombre de privilegio	Descripción de privilegio	roles predeterminados
lxc-mgmtserverupdates-delete-updates	Eliminar actualizaciones del servidor de gestión	lxc-admin, lxc-fw-admin, lxc-supervisor
lxc-mgmtserverupdates-download-updates	Descargar e importar actualizaciones del servidor de gestión y actualizar catálogo del servidor de gestión	lxc-admin, lxc-fw-admin, lxc-supervisor
lxc-mgmtserverupdates-perform-updates	Realizar actualizaciones del servidor de gestión	lxc-admin, lxc-fw-admin, lxc-supervisor

Privilegios de gestión de red

Estos privilegios proporcionan permisos para configurar valores de red.

Nombre de privilegio	Descripción de privilegio	Roles predeterminados
lxc-network-edit	Modificar acceso de red	lxc-admin, lxc-supervisor

Privilegios de despliegue del SO

Estos privilegios proporcionan permisos para gestionar y desplegar sistemas operativos.

Nombre de privilegio	Descripción de privilegio	Roles predeterminados
lxc-osdeploy-create-edit-remote-file-server	Crear y editar una entrada de servidor de archivo remoto	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osdeploy-create-import-export-edit-os-files	Crear, importar, exportar y editar imágenes de SO y archivos personalizados	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osdeploy-delete-os-files	Eliminar imágenes de SO y archivos personalizados	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osdeploy-delete-remote-file-server	Eliminar una entrada de servidor de archivo remoto	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor

Nombre de privilegio	Descripción de privilegio	Roles predeterminados
lxc-osdeploy-edit-global-settings	Editar información en el cuadro de diálogo de valores globales **Nota:** El cambio de los valores globales de la asignación de IP afecta a los valores de red; por lo tanto, para realizar cambios en los valores globales de la asignación de IP, también debe disponer de privilegios de **lxc-osdeploy-edit-settings-and-deploy-os-images**.	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osdeploy-edit-settings-and-deploy-os-images	Modificar valores de despliegue y desplegar imágenes de SO en uno o varios servidores	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor

Privilegios de actualización del controlador de SO

Estos privilegios proporcionan permisos para gestionar y aplicar actualizaciones del controlador de dispositivo del sistema operativo.

Nombre de privilegio	Descripción de privilegio	roles predeterminados
lxc-osDriverUpdates-apply-assign-uxsp	Asignar UXSP de controlador de dispositivos de SO a dispositivos	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osDriverUpdates-apply-check-authentication	Revisar la autenticación de SO	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osDriverUpdates-apply-check-compliance	Comprobar el cumplimiento de controlador de dispositivos de SO	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osDriverUpdates-apply-perform-updates	Realizar actualizaciones de controlador de dispositivos de SO	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osDriverUpdates-repository-delete-packages	Eliminar paquetes de actualización de controlador de dispositivos de SO	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osDriverUpdates-repository-download-packages	Descargar e importar paquetes de actualización de controlador de dispositivo de sistema operativo y actualizar catálogo UXSP de controlador de dispositivo de SO	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor

Privilegios de usuarios y grupos

Estos privilegios proporcionan permisos para gestionar las cuentas de usuario y grupos.

Nombre de privilegio	Descripción de privilegio	roles predeterminados
lxc-sec-apply-saml-settings	Aplicar configuración de SAML	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-delete-role-groups	Eliminar un grupo de roles	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-delete-roles	Eliminar un rol	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-delete-users	Eliminar un usuario	lxc-recovery, lxc-security-admin, lxc-supervisor

Nombre de privilegio	Descripción de privilegio	roles predeterminados
lxc-sec-edit-account-settings	Modificar valores de seguridad de cuenta	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-ldap-settings	Aplicar valores de LDAP	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-role-groups	Modificar un grupo de roles	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-roles	Modificar un rol	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-users	Modificar un usuario	lxc-recovery, lxc-security-admin, lxc-supervisor

Privilegios de configuración de servidor

Estos privilegios proporcionan permisos para aprovisionar o preaprovisionar servidores utilizando patrones de configuración.

Nombre de privilegio	Descripción de privilegio	Roles predeterminados
lxc-cp-edit-management-ip	Modificar las direcciones IP de gestión de chasis	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-edit-preferences	Definir preferencias de patrones de configuración	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-manage-address-pools	Gestionar grupos de direcciones	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-manage-patterns	Gestionar patrones	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-manage-placeholders	Gestionar marcadores	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-manage-profiles	Desplegar patrones, desplegar espacio reservado en chasis y gestionar perfiles	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-other-server-config	Restablecer el almacenamiento local y aplicar la operación de seguridad Intel Optane DCPMM	lxc-admin, lxc-hw-admin, lxc-supervisor

Privilegios de servicio

Estos privilegios proporcionan permisos para definir contactos de soporte para cada dispositivo gestionado, así como para recopilar los archivos de servicio y enviarlos al soporte de Lenovo, configurar el envío de una notificación automática a los proveedores de servicio cuando se producen ciertos sucesos de mantenimiento en dispositivos específicos y ver el estado del informe de servicio y la información de garantía y recolectar y reenviar datos de servicio.

Nombre de privilegio	Descripción de privilegio	Roles predeterminados
lxc-ss-alter-backup-credentials	Modificar credenciales FFDC de copia de seguridad	lxc-admin, lxc-hw-admin, lxc-service-admin, lxc-supervisor
lxc-ss-call-home	Realizar Llamar a casa	lxc-admin, lxc-hw-admin, lxc-supervisor

Nombre de privilegio	Descripción de privilegio	Roles predeterminados
lxc-ss-change-service-recovery-password	Cambio de la contraseña de recuperación de servicio	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-ss-change-service-tickets	Modificar informes de servicio	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-ss-remove-service-tickets	Eliminar informes de servicio	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-ss-run-service-forwarders	Ejecutar despachadores de servicios	lxc-admin, lxc-hw-admin, lxc-supervisor

Privilegios de configuración de conmutador

Estos privilegios proporcionan permisos para configurar los conmutadores y crear copias de seguridad y restaurar los datos de configuración del conmutador.

Nombre de privilegio	Descripción de privilegio	roles predeterminados
lxc-netcfg-template-management	Crear, modificar, eliminar y desplegar plantillas de configuración del conmutador y eliminar la implementación de una configuración del conmutador	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-swirm-config-management	Crear copia de seguridad, restaurar, eliminar, exportar e importar archivos de datos de configuración de conmutador	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-swirm-port-management	Modificar estado del puerto de conmutador	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor

Creación de un grupo de roles personalizado

Un *grupo de roles* es un conjunto de roles y un conjunto de usuarios que son miembros del mismo conjunto de roles. El nivel de acceso que se concede a cada usuario en el grupo de roles se basa en las funciones que están asignadas a ese grupo de roles. XClarity Administrator proporciona los siguientes grupos de roles predefinidos, que corresponden a cada uno de los roles predefinidos. También puede crear grupos de roles personalizados.

Acerca de esta tarea

Cada usuario de XClarity Administrator debe ser miembro al menos de un grupo de roles.

Los grupos de roles siguientes están predefinidos en XClarity Administrator.

- **LXC-SUPERVISOR**. Incluye los roles **lxc-supervisor**.
- **LXC-ADMIN**. Incluye el rol **lxca-admin**.
- **LXC-SECURITY-ADMIN**. Incluye el rol **lxc-security-admin**.
- **LXC-HW-ADMIN**. Incluye el rol **lxc-hw-admin**.
- **LXC-FW-ADMIN**. Incluye el rol **lxc-fw-admin**.
- **LXC-OS-ADMIN**. Incluye el rol **lxc-os-admin**.
- **LXC-SERVICE-ADMIN**. Incluye el rol **lxc-service-admin**.
- **LXC-HW-MANAGER**. Incluye el rol **lxc-hw-manager**.
- **LXC-OPERATOR**. Incluye los roles **lxc-operator**.

- **LXC-RECOVERY**. Incluye los roles **lxc-recovery**.

Los siguientes roles predefinidos están *reservados* y no se pueden usar para crear nuevos grupos de roles o asignarse a nuevos usuarios.
- **lxc-sysrdr**
- **lxc-sysmgr**

Procedimiento

Lleve a cabo los pasos siguientes para crear un grupo de roles.

Paso 1. En la barra de menús de XClarity Administrator , haga clic en **Administración → Seguridad**.

Paso 2. Haga clic en **Grupos de roles** en la sección Usuarios y grupos para mostrar el cuadro de diálogo Gestión de grupos.

Paso 3. Haga clic en el icono **Crear** ( ) para crear un grupo de roles. Se muestra el cuadro de diálogo Crear nuevo grupo de roles.

Paso 4. Escriba un nombre de grupo y una descripción.

Nota: Consejo: para el nombre de grupo, puede utilizar letras, números, espacios en blanco, guiones bajos, guiones y puntos.

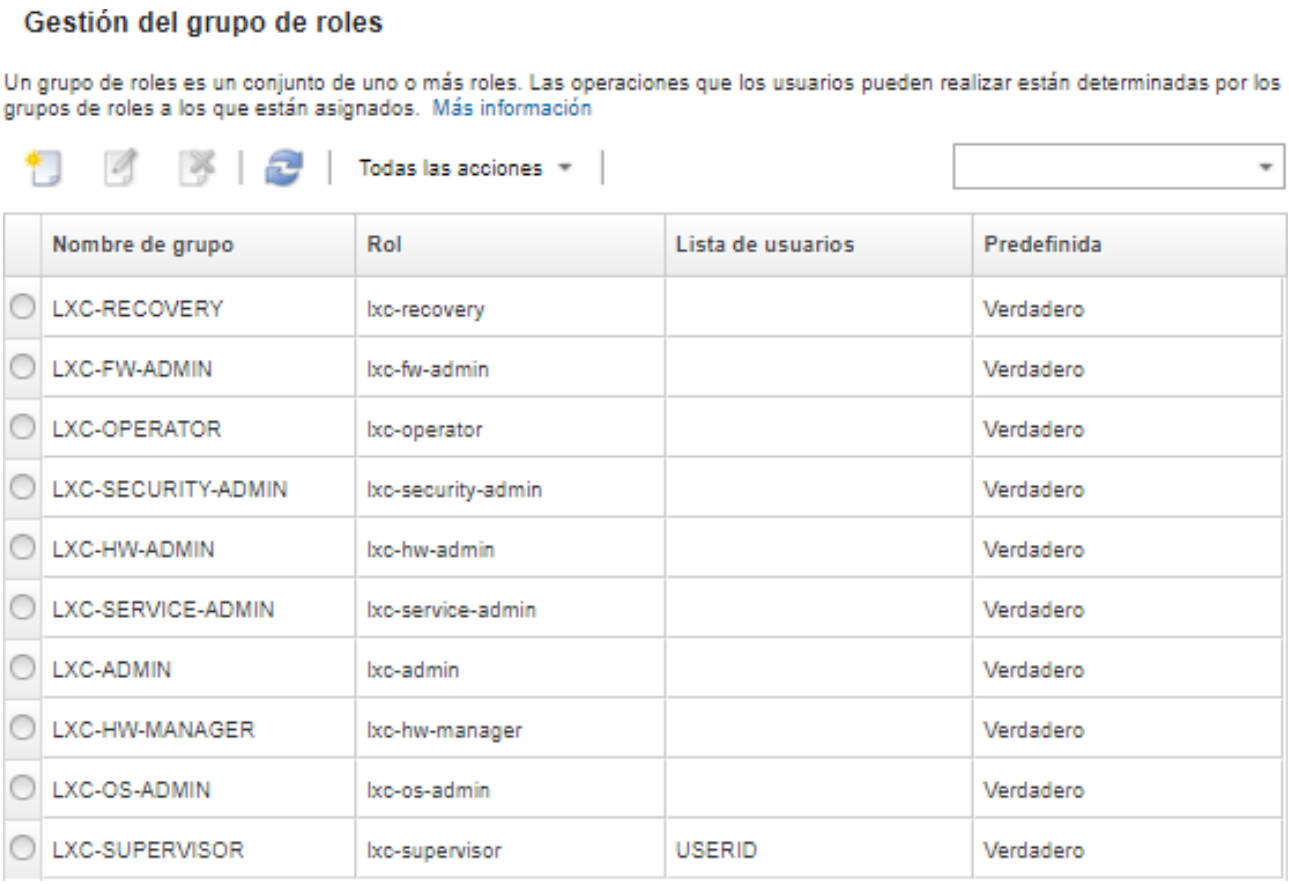
Paso 5. Seleccione uno o más roles para asignar a este grupo de roles.

Paso 6. Seleccione uno o varios usuarios como miembros de este grupo de roles.

Paso 7. Haga clic en **Crear**. El grupo de roles nuevo se añade a la tabla de la página Gestión de grupos.

Resultados

El grupo de roles se muestra en la tabla de grupos de roles. En la tabla se muestran los roles de autorización asociados y los miembros de cada grupo de roles.



Una vez que haya creado un grupo de roles, puede realizar las acciones siguientes en un grupo de roles seleccionado:

- Para agregar o eliminar roles que están asignados a este grupo de roles, haga clic en el ícono **Editar** ( ).
- Agregar o quitar usuarios como miembros del grupo de roles (consulte "Agregar y quitar varios usuarios desde un grupo de roles" en la página 58).
- Exportar información sobre los grupos de roles, incluidos los permisos de acceso pulsando **Todas las acciones → Exportar como CSV**.
- Eliminar el grupo de roles haciendo clic en el icono **Eliminar** ( ).No puede eliminar los grupos de roles predefinidos.

Después de crear, editar o eliminar un grupo de roles, el cambio se transfiere de inmediato a cada dispositivo administrado.

Agregar y quitar varios usuarios desde un grupo de roles

Puede cambiar la calidad de miembro en un grupo de roles al agregar o quitar varios usuarios.

Procedimiento

Lleve a cabo los pasos siguientes para agregar y quitar usuarios de un grupo de roles.

Paso 1. En la barra de menús de Lenovo XClarity Administrator , haga clic en **Administración → Seguridad**.

Paso 2. Haga clic en **Grupos de roles** en la sección Usuarios y grupos para mostrar el cuadro de diálogo Gestión de grupos.

Paso 3. Haga clic en el icono **Editar** ( ). Se muestra el cuadro de diálogo Editar grupo estático.

Paso 4. Haga clic en la lista desplegable **Lista de usuarios** y seleccione los usuarios que se van a incluir o borrar del grupo de roles.

Paso 5. Haga clic en **Guardar**. La columna **Lista de usuarios** muestra la calidad de miembro del usuario actual en el grupo de roles.

Gestión de acceso a dispositivos

El control de acceso a dispositivos está deshabilitado de forma predeterminada y no surte efecto hasta que se habilite

Cuando Lenovo XClarity Administrator gestiona los dispositivos por primera vez, un conjunto de grupos de roles predefinidos tienen permiso para acceder a los dispositivos de forma predeterminada. Este conjunto predefinido está vacío de forma predeterminada hasta que se configure.

Cambie los grupos de roles a los que se pueden acceder a los dispositivos gestionados específicos. Cuando se concede permiso a ciertos grupos de roles, solo los usuarios que son miembros de esos grupos de roles pueden ver y operar en esos dispositivos específicos.

Control de acceso a dispositivos específicos

Cuando Lenovo XClarity Administrator gestiona los dispositivos por primera vez, un conjunto de grupos de roles predefinidos tienen permiso para acceder a los dispositivos de forma predeterminada. Cambie los grupos de roles a los que se pueden acceder a los dispositivos gestionados específicos. Cuando se concede permiso a ciertos grupos de roles, solo los usuarios que son miembros de esos grupos de roles pueden ver y operar en esos dispositivos específicos.

Antes de empezar

Solo los usuarios con las autoridades **lxc-supervisor**, **lxc-security-admin** o **lxc-recovery** pueden realizar esta acción.

Acerca de esta tarea

Control de acceso está configurado en dispositivos individuales. No está configurado para contenedores, como bastidores y grupos de recursos.

Para los componentes en un chasis o alojamiento, los usuarios deben tener acceso al menos de solo lectura para el chasis o al alojamiento para los componentes de la vista de dicho chasis o del alojamiento. Si los usuarios no tiene como mínimo acceso de solo lectura al chasis o alojamiento, estos usuarios pueden ver los componentes en algunas vistas, pero no se garantiza que aparece en todas las vistas.

Los usuarios con autoridad de **lxc-supervisor** pueden ver y realizar acciones en todos los recursos, independientemente de si se encuentran en un grupo de roles a los que ha concedido acceso específicamente a dicho recurso. No se puede quitar el acceso a los recursos del grupo de roles **lxc-supervisor**.

Si un usuario no es miembro de un grupo de roles que tiene acceso a un dispositivo gestionado específico, el usuario no puede ver o realizar acciones en ese dispositivo específico. Esto incluye iniciar la interfaz web del controlador de gestión mediante Lenovo XClarity Administrator. En dispositivos Flex y System x, los usuarios tampoco pueden iniciar sesión directamente en un CMM o en un controlador de gestión para los cuales no tienen acceso.

Se utilizan los valores predeterminados de control de acceso para configurar los permisos de acceso a los dispositivos que gestiona inicialmente XClarity Administrator y durante el restablecimiento a los valores predeterminados de los permisos de acceso para un dispositivo específico. Cambiar los valores de control

de acceso predeterminados no modifica los permisos de acceso de los dispositivos que ya se estén gestionando.

Importante:

- Si un usuario es miembro de más de un grupo de roles y los grupos de roles se asignan a los distintos dispositivos, las acciones que pueden realizar los usuarios en cada dispositivo pueden diferir. Por ejemplo, si el usuario es miembro del grupo de roles predeterminado LXC-FW-ADMIN y LXC-OS-ADMIN y si, además de esto, se otorga acceso a LXC-FW-ADMIN al servidor A, pero no se otorga acceso a ese mismo servidor a LXC-OS-ADMIN, ese usuario podrá actualizar el firmware en el servidor A, pero no podría desplegar un sistema operativo en el mismo servidor. Si se otorgó acceso a LXC-OS-ADMIN al servidor B, pero no se otorgó acceso a LXC-FW-ADMIN al mismo servidor, entonces ese mismo usuario debiese poder desplegar un sistema operativo en el servidor B, pero no podría actualizar el firmware en dicho servidor.
- Cuando se limita el acceso a un dispositivo que tiene un recurso principal (por ejemplo, un servidor o un conmutador en del chasis de Flex), un usuario debe tener permisos al menos de solo lectura del recurso primario para interactuar completamente con el dispositivo. Si un usuario tiene acceso al menos de solo lectura para el dispositivo, pero no el primario, el usuario no podrá ver las vistas de inventario de dispositivos, pero es posible que pueda consultar acerca del dispositivo en algunas vistas, como los sucesos y trabajos.

  Por ejemplo, puede crear un grupo de roles para el principal y asignar ese grupo de roles del rol **lxc-operador**. Incluya todos los usuarios que deben tener acceso a alguno de los elementos secundarios (por ejemplo, un servidor o un conmutador en del chasis de Flex), en ese grupo de roles. Luego, incluya ese grupo de roles como uno de los grupos que tiene acceso al primario.

Procedimiento

Lleve a cabo los siguientes procedimientos para controlar el acceso a dispositivos específicos mediante la asociación de grupos de roles con estos dispositivos.

Paso 1. En el menú principal de Lenovo XClarity Administrator, haga clic en **Administración → Seguridad**.

Paso 2. Haga clic en **Vista de recursos** en el panel de navegación izquierdo. Aparece la página Vista de recursos.

Puede ordenar las columnas de la tabla para que sea más fácil encontrar dispositivos específicos. Además, puede seleccionar un tipo de dispositivo en el menú desplegable **Tipo de recurso**, seleccionar un rol de grupo en el menú desplegable **Grupos de roles**, seleccionar un grupo de recursos en el menú desplegable **Grupos de recursos** e introducir texto (como un nombre de recurso o de tipo) en el campo **Filtro** para obtener una lista de dispositivos limitada a solo aquellos que cumplen los criterios seleccionados.

Paso 3. Seleccione uno o varios dispositivos en los que desee controlar el acceso.

Paso 4. Haga clic en el icono **Editar** (). Se muestra el cuadro de diálogo Editar grupos de recursos con los dispositivos objetivo en el campo **Nombre de recurso**.

Paso 5. En la lista desplegable **Grupos de roles**, seleccione los Grupos de roles para los cuales desea acceder a los dispositivos objetivo.

Nota: Si el dispositivo tiene un recurso principal (por ejemplo, un servidor o un conmutador en un chasis de Flex), puede especificar el acceso para el recurso primario (columna izquierda) y el dispositivo (derecha).

Paso 6. Establezca **Acceso público** a `No`. Esto significa que solo los usuarios que son miembros de los grupos de roles seleccionados tienen acceso a los dispositivos objetivo.

Paso 7. Haga clic en **Guardar**.

Paso 8. Después de terminar la asignación de permisos, haga clic en el icono de alternación **Deshabilitado** para cambiar **Control de acceso a recursos** a habilitado.

Puede habilitar el control de acceso a recursos en cualquier momento, antes o después de configurar el acceso a dispositivos específicos. Cuando esta opción está habilitada, la configuración que se muestra en la tabla se aplica, lo que incluye denegar el acceso de todos los usuarios sin categoría de supervisor a todos los dispositivos que no tengan grupos configurados para acceder a ellos.

Después de finalizar

También puede controlar el acceso a dispositivos llevando a cabo las siguientes acciones:

- Cambie los permisos a los grupos de roles y a la configuración de acceso público predeterminados haciendo clic en el icono **Editar** () y, a continuación, haga clic en **Restablecer a valores predeterminados**.
- Cambie el grupo de roles y la configuración de acceso público predeterminados (consulte Cambiar los permisos predeterminados.).
- Deshabilite el control de acceso a recursos haciendo clic en el icono de alternación **Habilitado** para cambiar **Control de acceso a recursos** a deshabilitado. Esto significa que todos los grupos de roles pueden acceder a todos los dispositivos gestionados.

Deshabilitar el control de acceso a recursos

Se puede deshabilitar el control de acceso para todos los dispositivos o para dispositivos específicos, de modo que todos los usuarios puedan ver y operar esos dispositivos.

Acerca de esta tarea

Solo los usuarios con las autoridades **lxc-supervisor**, **lxc-security-admin** o **lxc-recovery** pueden realizar esta acción.

Procedimiento

Lleve a cabo los pasos siguientes para deshabilitar el control de acceso a los recursos.

- Para todos los dispositivos gestionados
  1. En el menú principal de Lenovo XClarity Administrator, haga clic en **Administración → Seguridad**.
  2. Haga clic en **Vista de recursos** en el panel de navegación izquierdo. Aparece la página Vista de recursos.
  3. Haga clic en el icono de alternación **Habilitado** para cambiar **Control de acceso a recursos** a deshabilitado.
- Para dispositivos gestionados específicos
  1. En el menú principal de XClarity Administrator, haga clic en **Administración → Seguridad**.
  2. Haga clic en **Vista de recursos** en el panel de navegación izquierdo. Aparece la página Vista de recursos.

     Puede ordenar las columnas de la tabla para que sea más fácil encontrar dispositivos específicos. Además, puede seleccionar un tipo de dispositivo en el menú desplegable **Tipo de recurso**, seleccionar un rol de grupo en el menú desplegable **Grupos de roles**, seleccionar un grupo de recursos en el menú desplegable **Grupos de recursos** e introducir texto (como un nombre de recurso o de tipo) en el campo **Filtro** para obtener una lista de dispositivos limitada a solo aquellos que cumplen los criterios seleccionados.

3. Seleccione uno o varios dispositivos a los que desee cambiar el acceso.
4. Haga clic en el icono **Editar** (). Se muestra el cuadro de diálogo Editar grupos de recursos con los dispositivos seleccionados en el campo **Nombre de recurso**.
5. Establezca **Acceso público** a `Yes`. Esto significa que todos los grupos de roles pueden acceder a los dispositivos objetivo, independientemente de los grupos de roles enumerados en la lista desplegable **Grupos de roles**.
6. Haga clic en **Guardar**.

Cambiar los permisos predeterminados

Hay dos valores que determinan si los grupos de roles pueden acceder a los dispositivos que gestiona Lenovo XClarity Administrator inicialmente: acceso público y grupos de roles. La configuración del acceso público determina si todos grupos de roles o solo un conjunto específico de ellos puede acceder a los dispositivos objetivo. De forma predeterminada, este valor se establece en `Yes`, lo que significa que todos los grupos de roles pueden acceder a los dispositivos objetivo. Puede cambiar el comportamiento predeterminado al cambiar la configuración del acceso público a `No` y, a continuación, seleccionar el conjunto de grupos de roles que pueden acceder a los dispositivos objetivo

Acerca de esta tarea

Solo los usuarios con las autoridades **lxc-supervisor**, **lxc-security-admin** o **lxc-recovery** pueden realizar esta acción.

Los usuarios con las autoridades **lxc-supervisor**, **lxc-security-admin** o **lxc-recovery** pueden tener acceso a todos los dispositivos gestionados. No puede quitar el acceso a todos los dispositivos de dichos grupos de roles.

Se utilizan los valores predeterminados de control de acceso para configurar los permisos de acceso a los dispositivos que gestiona inicialmente XClarity Administrator y durante el restablecimiento a los valores predeterminados de los permisos de acceso para un dispositivo específico. Cambiar los valores de control de acceso predeterminados no modifica los permisos de acceso de los dispositivos que ya se estén gestionando.

Procedimiento

Lleve a cabo los siguientes procedimientos para cambiar los controles de acceso predeterminados.

Paso 1. En el menú principal de XClarity Administrator, haga clic en **Administración → Seguridad**.

Paso 2. Haga clic en **Vista de recursos** en el panel de navegación izquierdo. Aparece la página Vista de recursos.

Puede ordenar las columnas de la tabla para que sea más fácil encontrar dispositivos específicos. Además, puede seleccionar un tipo de dispositivo en el menú desplegable **Tipo de recurso**, seleccionar un rol de grupo en el menú desplegable **Grupos de roles**, seleccionar un grupo de recursos en el menú desplegable **Grupos de recursos** e introducir texto (como un nombre de recurso o de tipo) en el campo **Filtro** para obtener una lista de dispositivos limitada a solo aquellos que cumplen los criterios seleccionados.

Paso 3. Haga clic en **Todas las acciones → Editar recursos predeterminados**. Se muestra el cuadro de diálogo Editar recursos predeterminados.

Paso 4. En la lista desplegable de recursos **Grupos de roles**, seleccione los grupos de roles que desea definir como el conjunto predeterminado.

Paso 5. Seleccione el valor de **Acceso público** predeterminado.

- **Sí**. Cuando se gestiona inicialmente un dispositivo, todos los grupos de roles pueden acceder a ese dispositivo, independientemente de los grupos de roles enumerados en la lista desplegable **Grupos de roles**.
- **No**. Cuando se gestiona inicialmente un dispositivo, solo los grupos de roles enumerados en la lista desplegable **Grupos de roles** pueden acceder a él de forma predeterminada.

Paso 6. Haga clic en **Guardar**.

Implementación de un entorno seguro

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

Acerca de esta tarea

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

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

- La seguridad física de su entorno es importante: limite el acceso a las salas y los bastidores donde se ubica el hardware de gestión de sistemas.
- Utilice un firewall basado en software para proteger su hardware de red y los datos de amenazas de seguridad desconocidas y emergentes, como virus y accesos no autorizados.
- No cambie los valores de seguridad predeterminados de los conmutadores de red ni de los módulos de paso a través. Los valores predeterminados de fábrica de estos componentes deshabilitan el uso de protocolos no seguros y habilitan el requisito de las actualizaciones de firmware firmadas.
- Las aplicaciones de gestión para los CMM, los controladores de gestión de la placa base, los FSP y los conmutadores solo permiten paquetes de actualización de firmware firmados para estos componentes, a fin de garantizar que solo se instale firmware de confianza.
- Solamente aquellos usuarios que estén autorizados para actualizar firmware deberían tener autoridad de actualización de firmware.
- Como mínimo, asegúrese de que instala actualizaciones de firmware críticas. Después de realizar cualquier cambio, realice siempre una copia de seguridad de la configuración.
- Asegúrese de que todas las actualizaciones relacionadas con la seguridad de los servidores DNS se instalen lo antes posible y se mantengan actualizadas.
- Pida a sus usuarios que no acepten certificados que no sean de confianza. Para obtener más información, consulte el apartado Trabajo con certificados de seguridad.
- Hay disponibles opciones a prueba de intrusos para el hardware de Flex System. Si el hardware está instalado en un bastidor sin cerrar o está ubicado en un área abierta, instale opciones a prueba de intrusos a fin de impedir e identificar las intrusiones. Consulte la documentación que se suministra con los productos de Flex System para obtener más información sobre las opciones a prueba de intrusos.
- Siempre que sea posible y le resulte práctico, coloque el hardware de gestión de sistemas en una submáscara aparte. Normalmente, solo los administradores deberían tener acceso al hardware de gestión de sistemas y no se debería conceder acceso a los usuarios básicos.
- Al elegir las contraseñas, no utilice expresiones que se puedan adivinar fácilmente, como “contraseña” o el nombre de su empresa. Mantenga las contraseñas en un lugar seguro y asegúrese de que el acceso a las mismas esté restringido. Implemente una política de contraseñas para su empresa.

Importante: Cambie siempre el nombre de usuario y la contraseña predeterminados. Las reglas de contraseñas complejas deberían ser obligatorias para todos los usuarios.

- Establezca contraseñas de encendido para los usuarios como forma de controlar quién tiene acceso a los datos y a los programas de configuración de los servidores. Consulte la documentación que se suministra los servidores para obtener más información sobre las contraseñas de encendido.
- Utilice varios niveles de autorización que estén disponibles para usuarios diferentes en su entorno. No permita que todos los usuarios trabajen con el mismo Id. de usuario de supervisor.
- Asegúrese de que su entorno cumple con los criterios de NIST 800-131A siguientes a fin de respaldar las comunicaciones seguras:
  - Utilizar la Capa de sockets seguros (SSL) sobre el protocolo TLS v1.2.
  - Utilizar funciones de algoritmos hash SHA-256 o más complejos para las firmas digitales y funciones de algoritmos hash SHA-1 o más complejos para otras aplicaciones.
  - Utilizar un sistema RSA-2048 o más complejo, o curvas elípticas aprobadas por NIST que tengan, como mínimo, 224 bits.
  - Utilizan un sistema de cifrado simétrico aprobado por NIST con claves que tengan una longitud mínima de 128 bits.
  - Utilizar generadores de números aleatorios aprobados por NIST.
  - Siempre que sea posible, permitir los mecanismos de intercambio de claves de Diffie-Hellman o de curvas elípticas de Diffie-Hellman.

  Para obtener más información sobre los valores criptográficos, consulte Configuración de valores de criptografía en el servidor de gestión. Para obtener más información sobre los valores de NIST, consulte Implementación de la conformidad con NIST SP 800-131A.

Cambio de los valores de seguridad de una cuenta de usuario

Los valores de seguridad 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 las opciones de los valores.

Procedimiento

Lleve a cabo los pasos siguientes para sobrescribir los valores de seguridad de la cuenta de usuario que se están aplicando.

Paso 1. En la barra de menús de XClarity Administrator , haga clic en **Administración → Seguridad**.

Paso 2. Haga clic en **Valores de seguridad de la cuenta** en la sección Usuarios y grupos para mostrar la página Gestión de usuarios.

Paso 3. Seleccione el nuevo valor para cada uno de los siguientes valores que tienen que cambiar.

Tabla 1. Valores de seguridad de la cuenta

Valor de seguridad	Descripción	Valores permitidos	Valores predeterminados
Periodo de caducidad de la contraseña	Cantidad de tiempo, en días que un usuario puede utilizar una contraseña antes de que tenga que cambiarla. Los valores más pequeños reducen la cantidad de tiempo en que los piratas informáticos pueden adivinar las contraseñas Si se establece en **0**, las contraseñas no caducan nunca. **Nota:** Este valor solo se aplica cuando las cuentas de usuarios se gestionan utilizando el servidor de autenticación local. No se usan cuando se utiliza el servidor de autenticación externo.	**0 – 365**	**90**
Periodo de advertencia de caducidad de la contraseña	Cantidad de tiempo, en días, antes de la fecha de caducidad de la contraseña en que los usuarios empiezan a recibir advertencias sobre la inminente caducidad de la contraseña de usuario Si se establece en **0**, los usuarios no reciben advertencias nunca. **Nota:** Este valor solo se aplica cuando las cuentas de usuarios se gestionan utilizando el servidor de autenticación local. No se usan cuando se utiliza el servidor de autenticación externo.	**0:** *valor de caducidad máximo de la contraseña*	**5**
Ciclo mínimo de reutilización de la contraseña	Número mínimo de veces que un usuario debe introducir una contraseña única cuando se cambia la contraseña antes de poder empezar a reutilizar contraseñas Si se establece en **0**, los usuarios pueden reutilizar las contraseñas inmediatamente.	**0 – 10**	**5**
Intervalo mínimo de cambio de contraseña	Cantidad mínima de tiempo, en horas, que debe transcurrir antes de que un usuario pueda volver a cambiar una contraseña una vez que la ha cambiado anteriormente. El valor especificado no puede superar el valor especificado en el periodo de caducidad de la contraseña. Si se establece en **0**, los usuarios pueden cambiar las contraseñas inmediatamente.	**0 – 1440**	**24**
Número máximo de errores de inicio de sesión	Número máximo de veces que un usuario puede intentar iniciar la sesión con una contraseña incorrecta antes de que la cuenta de usuario se bloquee. El número especificado en el periodo de bloqueo tras superar el número máximo de errores de inicio de sesión determina por cuanto tiempo está bloqueada la cuenta de usuario. Las cuentas que están bloqueadas no se pueden utilizar para acceder al sistema aunque se proporcione una contraseña válida. Si se establece en **0**, las cuentas no se bloquean nunca. El contador de errores de inicio se restablece a cero una vez que se ha iniciado sesión correctamente.	**0 – 100**	**20**

Tabla 1. Valores de seguridad de la cuenta (continuación)

Valor de seguridad	Descripción	Valores permitidos	Valores predeterminados
Periodo de bloqueo tras superar el número máximo de errores de inicio de sesión	Cantidad mínima de tiempo, en minutos, que debe transcurrir antes de que un usuario que ha sido bloqueado pueda intentar iniciar sesión de nuevo Si se establece en **0**, la cuenta se mantiene bloqueada hasta que un administrador la desbloquea expresamente. Un valor de 0 podría hacer que el sistema estuviera más expuesto a una grave negación de ataques al servicio, pues los intentos de error de inicio de sesión deliberados pueden dejar cuentas permanentemente bloqueadas. **Consejo:** cualquier usuario con el rol de Supervisor puede desbloquear una cuenta de usuario. Para obtener más información, consulte el apartado Desbloqueo de un usuario. **Nota:** Este valor solo se aplica cuando las cuentas de usuarios se gestionan utilizando el servidor de autenticación local. No se usan cuando se utiliza el servidor de autenticación externo.	**0 – 2880**	**60**
Tiempo de espera por inactividad de sesión web	Cantidad de tiempo, en minutos, que una sesión de usuario que se ha establecido con XClarity Administrator puede estar inactiva antes de que se cierre dicha sesión Si se establece en **0**, la sesión web no se cierra nunca. **Nota:** Cuando cambia este valor, solo las sesiones de usuario que se inician después de cambiar la configuración se ven afectadas.	**0 – 1440**	**1440**
Longitud mínima de la contraseña	Número mínimo de caracteres que se pueden utilizar para especificar una contraseña válida	**8 – 20**	**8**

Tabla 1. Valores de seguridad de la cuenta (continuación)

Valor de seguridad	Descripción	Valores permitidos	Valores predeterminados
Número reglas de complejidad que se deben seguir al crear una contraseña nueva	Número reglas de complejidad que se deben seguir al crear una contraseña nueva Las reglas se aplican comenzando con la regla 1 y hasta el número de reglas especificado. Por ejemplo, si la complejidad de la contraseña está configurada en 4, entonces se deben seguir las reglas 1, 2, 3 y 4. Si la complejidad de la contraseña está configurada en 2, entonces se deben seguir las reglas 1 y 2. XClarity Administrator admite las siguientes reglas de complejidad de contraseña. • (1) Debe contener al menos un carácter alfabético y no debe tener más de dos caracteres secuenciales, incluidas las secuencias de caracteres alfabéticos, dígitos y las teclas del teclado QWERTY (por ejemplo “abc”, “123” y “asd” no están permitidos). • (2) Debe contener al menos un número (0 - 9). • (3) Deben contener al menos *dos* de los siguientes caracteres. – Caracteres alfabéticos en mayúscula (A - Z) – Caracteres alfabéticos en minúscula (a - z) – Caracteres especiales ; @ _ ! ' $ & + • (4) No se debe repetir ni invertir el nombre de usuario. • (5) No debe contener más de dos caracteres iguales de forma consecutiva (por ejemplo, “aaa”, “111” y “...” no están permitidos). Si se establece en **0**, las contraseñas no se requieren para cumplir con ninguna regla de complejidad.	**0 – 5**	**4**
Máximo de sesiones activas simultáneas para un usuario específico	Número máximo de sesiones activas simultáneas para un usuario específico que se permiten a la vez Si se define en **0**, el número de sesiones activas permitidas para un usuario específico es ilimitado.	**1 – 20**	**3**
Obligar al usuario a cambiar la contraseña en el primer acceso	Indica si se requiere que el usuario cambie la contraseña cuando el usuario inicia sesión en XClarity Administrator por primera vez.	**Sí** o **No**	**Sí**

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

Después de finalizar

Cuando se ha guardado correctamente, los nuevos valores tienen efecto inmediatamente. Si cambia el valor del tiempo de espera por inactividad de sesión web, las sesiones activas se ven afectadas.

Si cambia las políticas de la contraseña, dichas políticas se aplicarán la próxima vez que el usuario inicie sesión o cambie la contraseña.

Configuración de valores de criptografía en el servidor de gestión

Puede configurar la versión de SSL/TLS y los valores de cifrado para el servidor de gestión.

Antes de empezar

Revise las consideraciones sobre criptografía antes de modificar los valores en el servidor de gestión (consulte Gestión criptográfica en la documentación en línea de XClarity Administrator).

Acerca de esta tarea

El *modo criptográfico* determina el grado de seguridad con el que se manejan las comunicaciones entre XClarity Administrator y todos los sistemas gestionados. Establece la longitud de las claves de cifrado que se van a utilizar si se han implementado comunicaciones seguras.

Nota: Independientemente del modo criptográfico que seleccione, siempre se utilizan generadores de bits aleatorios digitales aprobados por NIST y solo se utilizan claves de 128 bits o de mayor longitud para el cifrado simétrico.

Para cambiar el valor de seguridad de los dispositivos gestionados, consulte Configuración de los valores de seguridad para un servidor gestionado.

Procedimiento

Para cambiar los valores criptográficos en el servidor de gestión, lleve a cabo los pasos siguientes.

Paso 1. En la barra de menús de XClarity Administrator , haga clic en **Administración → Seguridad**.

Paso 2. Elija uno de los siguientes modos criptográficos para utilizar comunicaciones seguras:

- **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). 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 SP 800-131A.

Paso 3. Elija la versión mínima del protocolo TLS que se utilizará en las conexiones del cliente a otros servidores (como el servidor LDAP). Puede elegir la siguiente opción.

- **TLS1.2**. Aplica los protocolos de criptografía TLS v1.2.
- **TLS1.3**. Aplica los protocolos de criptografía TLS v1.3.

Paso 4. Elija la versión mínima del protocolo TLS a utilizar para conexiones de servidor (como el servidor web). Puede elegir la siguiente opción.

- **TLS1.2**. Aplica los protocolos de criptografía TLS v1.2.
- **TLS1.3**. Aplica los protocolos de criptografía TLS v1.3.

Paso 5. Elija la versión mínima del protocolo TLS para usar en el despliegue del sistema operativo XClarity Administrator y las actualizaciones de controladores de dispositivos de SO. Puede elegir la siguiente opción.

- **TLS1.2**. Aplica los protocolos de criptografía TLS v1.2.
- **TLS1.3**. Aplica los protocolos de criptografía TLS v1.3.

Nota: Solo se podrán desplegar y actualizar mediante XClarity Administrator aquellos sistemas operativos con un proceso de instalación que admita algoritmos criptográficos seleccionados o complejos.

Paso 6. Seleccione la longitud de la clave criptográfica y el algoritmo hash que se utilizará en todas las partes del certificado, incluido el certificado raíz de la CA, el certificado de servidor y la CSR para los certificados firmados externamente.

- **RSA de 2048 bits/SHA-256** (predeterminado)

  Este modo se puede usar cuando los dispositivos gestionados están en modo de compatibilidad, NIST SP 800-131A o seguridad estándar. Este modo *no* se puede usar cuando uno o más dispositivos gestionados están en el modo de **Seguridad estricta empresarial**.

- **RSA de 3072 bits/SHA-384**

  Este modo es necesario cuando los dispositivos gestionados están en el modo de **Seguridad estricta empresarial**.

  Importante: Solo los servidores con XCC2 admiten firmas de certificado RSA-3072/SHA-384. Después de configurar XClarity Administrator con un certificado basado en RSA-3072/SHA-384, se anula la gestión de los dispositivos que no sean XCC2. Para gestionar dispositivos que no sean XCC2, sea necesita una instancia de XClarity Administrator separada.

Paso 7. Haga clic en **Aplicar**.

Paso 8. Reinicie XClarity Administrator (consulte Reiniciar XClarity Administrator).

Paso 9. Si cambió la longitud de la clave criptográfica, vuelva a generar el certificado raíz de la entidad de certificación con la longitud de clave y el algoritmo hash correctos (consulte Regenerar o restaurar el certificado de servidor autofirmado de Lenovo XClarity Administrator o Desplegar certificados de servidor personalizado en Lenovo XClarity Administrator).

Después de finalizar

Si recibe una alerta de que el certificado de servidor no es de confianza para un dispositivo gestionado, consulte Resolución de un certificado de servidor no fiable.

Configuración de los valores de seguridad para un servidor gestionado

Puede configurar la versión de SSL/TLS y los valores de cifrado para los servidores gestionados.

Acerca de esta tarea

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

- 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.
  - Si falta o caduca la clave FoD del modo estricto en el XCC2, y si XCC2 utiliza un certificado TLS autofirmado, XCC2 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 XCC2 utiliza un certificado TLS personalizado, XCC2 permite la degradación y le advierte que debe importar un certificado de servidor basado en la criptografía del modo de **Seguridad estándar**.
- El modo **NIST SP 800-131A** no es compatible con servidores con XCC2.
- Si el modo criptográfico para XClarity Administrator está establecido en TLS v1.2, y si un servidor gestionado que usa autenticación gestionada tiene un modo de seguridad establecido en TLS v1.2, cambiar el modo de seguridad del servidor a TLS v1.3 mediante XClarity Administrator o XCC hará que el servidor esté fuera de línea de forma permanente.
- Si el modo criptográfico para XClarity Administrator está establecido en TLS v1.2 y se intenta gestionar un servidor con XCC cuyo modo de seguridad está establecido en TLS v1.3, el servidor no se podrá gestionar mediante la autenticación gestionada.

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 ThinkEdge SE350/SE450
- Servidores Lenovo System x

Procedimiento

Para cambiar los valores de seguridad de servidores gestionados específicos, lleve a cabo los pasos siguientes:

Paso 1. En el menú de XClarity Administrator, haga clic en **Hardware → Servidores**. Se muestra la página Servidores con una vista de tabla de todos los servidores gestionados.

Paso 2. Seleccione uno o más servidores.

Paso 3. Configure el modo de seguridad.

1. Haga clic en **Todas las acciones → Seguridad → Establecer el modo de seguridad del sistema** para mostrar el cuadro de diálogo Establecer modo de seguridad del sistema.

   El cuadro de diálogo muestra la cantidad de servidores que se pueden configurar en cada modo. Desplace el cursor por encima de cada número para mostrar un elemento emergente con la lista de los nombres de servidores correspondientes.

2. Seleccionar modo de seguridad. Puede presentar uno de los valores siguientes.

   - **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 *no es* compatible con servidores con XCC2.

- **Seguridad estándar**. (Únicamente servidores con XCC2) Este es el modo de seguridad predeterminado para servidores con XCC2. 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**. (solo servidores con XCC2) Este es el modo más seguro. 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 del certificado RSA-3072/SHA-384 para servidores en el modo de **Seguridad estricta empresarial**.

  Importante:

  – La clave de característica bajo demanda de XCC2 se debe instalar en cada uno de los servidores con XCC2 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 RSA3072/SHA384. Si XClarity Administrator utiliza un certificado externo firmado, XClarity Administrator debe generar una CSR basada en RSA3072/SHA384 y ponerse en contacto con la CA externa para firmar un nuevo certificado de servidor basado en RSA3072/SHA384.

  – Cuando XClarity Administrator utiliza un certificado basado en RSA3072/SHA384, 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 RSA2048/SHA384.

3. Haga clic en **Aplicar**.

Paso 4. Configure la versión mínima de TLS.

1. Haga clic en **Todas las acciones → Seguridad → Establecer versión de TLS del sistema** para mostrar el cuadro de diálogo Establecer versión TLS del sistema.
2. Seleccione la versión mínima del protocolo TLS que se usará en las conexiones del cliente a otros servidores (como las conexiones de cliente LDAP a un servidor LDAP). El valor se configura en los dispositivos seleccionados que admiten este valor. Puede elegir la siguiente opción.

   - **TLS1.2**. Aplica los protocolos de criptografía TLS v1.2.
   - **TLS1.3**. Aplica los protocolos de criptografía TLS v1.3.

   Nota: Los dispositivos System x y CMM solo admiten TLS v1.2.

3. Haga clic en **Aplicar**.

Trabajo con 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.

Antes de empezar

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

Acerca de esta tarea

El certificado 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.

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

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

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

- **Certificado del servidor**. Durante el arranque inicial, se generan una clave única y un certificado autofirmado. Estos se usan como la Entidad de certificación de raíz predeterminada, que se puede

gestionar en la página de Autoridad de certificación en los valores de seguridad de XClarity Administrator. No es necesario volver a generar el certificado de raíz a menos que se haya comprometido la clave o si su organización tiene una política que todos los certificados se deben reemplazar periódicamente (consulte Regenerar o restaurar el certificado de servidor autofirmado de Lenovo XClarity Administrator).

También durante la configuración inicial, se genera una clave separada y se crea y se firma un certificado de servidor, un certificado se crea que está firmado por la autoridad de certificación interna. Este certificado utilizado como el certificado de servidor de XClarity Administrator predeterminado. Se regenera automáticamente cada vez que XClarity Administrator detecta que las direcciones de red (las direcciones IP o DNS) se han modificado para asegurarse de que el certificado contiene las direcciones correctas para el servidor. Se puede personalizar y se generara a demanda (consulte Regenerar o restaurar el certificado de servidor autofirmado de Lenovo XClarity Administrator).

Puede elegir utilizar un certificado de servidor firmado externamente en lugar del certificado de servidor autofirmado predeterminado generando una solicitud de firma de certificado (CSR), teniendo la CSR firmada por una entidad de certificación raíz de certificado privada o comercial y luego importando la cadena de certificado completa en XClarity Administrator (consulte Desplegar certificados de servidor personalizado en Lenovo XClarity Administrator).

Si elige usar el certificado de servidor autofirmado predeterminado, se recomienda que importe el certificado del servidor en su navegador web como entidad de confianza de raíz para evitar los mensajes de error del certificado en su navegador (consulte Importación del certificado de la Entidad de certificación en un navegador web).

- **Certificado de despliegue de SO**. El servicio de despliegue del sistema operativo usa un certificado separado para asegurarse de que el instalador del sistema operativo pueda conectarse de forma segura al servicio de despliegue durante el proceso de instalación del sistema operativo. Si se ha comprometido la clave, puede regenerarla reiniciando el servidor de gestión.

Los clientes de XClarity Administrator utilizan la siguiente categoría (almacenes de confianza) de certificados.

- **Certificados de confianza**.

  Este almacén de confianza gestiona certificados que se usan para establecer una conexión segura con los recursos locales cuando XClarity Administrator actúa como un cliente. Ejemplos de recursos locales son dispositivos gestionados, software local al reenviar sucesos y un servidor LDAP externo.
- **Certificados de servicios externos**. Este almacén de confianza gestiona certificados que se usan para establecer una conexión segura con dispositivos externos cuando XClarity Administrator actúa como un cliente. Ejemplos de servicios externos son los servicios del soporte de Lenovo en línea que se usan para recuperar información de garantía o crear informes de servicio, software externo (como Splunk) al que se pueden reenviar sucesos y servidores de notificaciones automáticas de Apple y Google si las notificaciones automáticas de Lenovo XClarity Mobile están habilitadas para un dispositivo iOS o Android. Contiene certificados de confianza preconfigurados de entidades de certificación raíz de ciertos proveedores de entidades de certificación conocidas a nivel mundial y de confianza común, (como Digicert y Globalsign).

  Cuando configure XClarity Administrator para usar una característica que requiere una conexión con otro servicio externo, consulte la documentación para determinar si necesita agregar manualmente un certificado a este almacén de confianza.

  Tenga en cuenta que los certificados en este almacén de confianza al establecer conexiones con otros servicios (como LDAP) a menos que también los agregue al almacén de confianza de Certificados de confianza principal. Eliminar certificados de este almacén de confianza evita una operación satisfactoria de estos servicios.

XClarity Administrator admite firmas del certificado RSA-3072/SHA-384, RSA-2048/SHA-256 y ECDSA p256/SHA-256. Otros algoritmos como SHA-1 superior o SHA hash se pueden admitir dependiendo de la configuración. Considere el modo criptográfico seleccionado en XClarity Administrator (consulte

Configuración de valores de criptografía en el servidor de gestión), los valores de seguridad seleccionados para servidores gestionados (Configuración de los valores de seguridad para un servidor gestionado) y las capacidades de otros software y dispositivos en su entorno. Los certificados ECDSA que se basan en algunas curvas elípticas (incluidos los p256), pero no se admiten todas las curvas elípticas en la página de certificados de confianza y en la cadena de firma del certificado de XClarity Administrator, pero *no* se admiten actualmente para su uso por el certificado de servidor de XClarity Administrator.

Nota: XClarity Administrator utiliza firmas del certificado RSA- 3072/SHA-384 para servidores con XCC2 en modo estricto.

Instalación de un certificado de servidor firmado externamente y personalizado

Puede optar por utilizar un certificado de servidor firmado por una entidad de certificación (CA) privada o comercial.

Antes de empezar

Asegúrese de que la Entidad de certificación de raíz es aquella generada por su organización y que se utiliza para firmar certificados dentro de esa organización o de una entidad de confianza conocida mundialmente (consulte Página web de la lista de entidades de certificación de confianza).

Asegúrese de que se admiten los algoritmos para las claves y las firmas del certificado raíz de la CA. Solo se admiten las firmas RSA-3072/SHA-384 y RSA-2048/SHA-256. No se admiten las firmas RSA-PSS en este momento.

Asegúrese de que todos los dispositivos gestionados tengan instalado el firmware más reciente antes de iniciar cualquier tarea que pueda afectar a las conexiones entre los dispositivos gestionados. Para actualizar el firmware en dispositivos gestionados, consulte Actualización de firmware en dispositivos gestionados.

Asegúrese de que XClarity Administrator esté comunicando satisfactoriamente con todos los dispositivos gestionados pulsando **Hardware** y luego pulsando el tipo de dispositivo (chasis o servidor). Se muestra una página con una vista de tabla de todos los dispositivos gestionados de ese tipo. Si cualquier dispositivo tiene un estado de “Fuera de línea”, asegúrese de que la conectividad de red esté funcionando entre el servidor de gestión y el dispositivo y resuelva los problemas de certificados de servidor de confianza si es necesario (consulte Resolución de un certificado de servidor no fiable).

Acerca de esta tarea

Al instalar un certificado de servidor firmado externamente personalizado en XClarity Administrator o en un controlador de gestión o CMM, debe indicar el conjunto de certificados que contiene toda la cadena de firma de la entidad de certificación CA.

Al instalar un certificado de servidor personalizado en un chasis o servidor que no está gestionado mediante XClarity Administrator, debe instalar el conjunto de certificados en el CMM antes de instalarlo en todos los controladores de gestión del CMM.

Al instalar un certificado de servidor personalizado en un chasis gestionado, primero debe agregar la cadena de firma de la CA al almacén de confianza de XClarity Administrator, después instalar el certificado de servidor en cada controlador de gestión y CMM y, finalmente, cargar el certificado de servidor a XClarity Administrator. Tenga en cuenta que esto puede omitirse fácilmente al confiar o agregar todos los certificados de CA raíz, pero no todas las cadenas de certificados de cada dispositivo gestionado. El número de certificados importados debe ser igual al número de certificados de CA raíz (certificados de CA raíz + todos certificados de CA intermediarias). Para obtener más información, consulte el apartado Despliegue de certificados de servidor personalizados en dispositivos gestionados.

Debe añadir el certificado raíz de la CA y todos los certificados intermedios, uno cada vez, al almacén de confianza de XClarity Administrator. El orden no importa. Cada certificado debe instalarse una vez, de modo que si todos los dispositivos utilizan la misma CA y los mismos certificados intermedios, la CA y cada certificado intermedio debe instalarse en el almacén de confianza de XClarity Administrator una vez. Si se utiliza más de una CA o una CA intermediaria, asegúrese de que cada certificado raíz de la CA o certificados intermedios que se utilizan en la cadena de firma de un dispositivo gestionado se importen siguiendo estos pasos.

Consejo: si el nuevo certificado de servidor no está firmado por un tercero de confianza, la próxima vez que se conecte a XClarity Administrator, el navegador mostrará un mensaje de seguridad y un cuadro de diálogo que le pide que acepte el nuevo certificado en el navegador. Para evitar los mensajes de seguridad, puede importar un certificado de servidor descargado en la lista de certificados de confianza del navegador web. Para obtener más información sobre cómo importar certificados de servidor, consulte Importación del certificado de la Entidad de certificación en un navegador web.

Desplegar certificados de servidor personalizado en Lenovo XClarity Administrator

Puede elegir generar una solicitud de firma de certificado (CSR) para firmar con la autoridad de certificación de su organización o una autoridad de certificación de terceros. El CSR crea una cadena de certificado completa que se puede importar y utilizar en lugar de los certificados firmados internamente únicos predeterminados.

Antes de empezar

Asegúrese de que los detalles del certificado incluyan los siguientes requisitos.

- El uso de clave debe contener
  - Acuerdo clave
  - Firma digital
  - Cifrado de clave
- El uso de clave mejorada debe contener
  - Autenticación de servidor (1.3.6.1.5.5.7.3.1)
  - Autenticación de cliente (1.3.6.1.5.5.7.3.2)

Acerca de esta tarea

Atención: Si NIST SP 800-131A está habilitado (consulte Implementación de la conformidad con NIST SP 800-131A) y está utilizando o planea utilizar certificados personalizados o firmados externamente en un NIST, todos los certificados de la cadena deben basarse en las funciones hash SHA-256.

Después de cargar el certificado de servidor, XClarity Administrator intenta suministrar el nuevo certificado de la CA a todos los dispositivos gestionados. Si el proceso de aprovisionamiento se realiza correctamente, XClarity Administrator comienza a utilizar el nuevo certificado de servidor de inmediato. Si el proceso falla, se entregan mensajes de error que le indican que debe corregir los problemas en forma manual antes de aplicar el certificado de servidor importado recientemente. Después de corregir los errores, realice la instalación del certificado previamente cargado.

Nota: Si XClarity Administrator utilizaba ya un certificado firmado por la misma entidad raíz, la CA no necesita que se envíen a los dispositivos y XClarity Administrator comienza a utilizar el certificado de inmediato.

Después de cargar un certificado en XClarity Administrator versión 1.1.0 y anterior, el servidor web se reinicia y automáticamente cierra todas las sesiones del explorador. XClarity Administrator versión 1.1.1 y posterior se inicia con el nuevo certificado sin cerrar las sesiones existentes. Las nuevas sesiones se establecen utilizando el nuevo certificado. Para ver el nuevo certificado en uso, reinicie el navegador web.

Procedimiento

Para generar y desplegar un certificado de servidor personalizado firmado externamente en Lenovo XClarity Administrator, complete los pasos siguientes.

Paso 1. Crear y descargar una solicitud de firma de certificado (CSR) para XClarity Administrator.

a. En la barra de menús de XClarity Administrator, haga clic en **Administración → Seguridad** para mostrar la página Seguridad.

b. Haga clic en **Certificado de servidor** en la sección Gestión de certificados para mostrar la página Certificado de servidor.

c. Haga clic en la pestaña **Generar solicitud de firma de certificado (CSR)**.

d. Rellene los campos de la solicitud.
- País o región
- Estado o provincia
- Ciudad o localidad
- Organización
- Unidad organizativa (opcional)
- Nombre común

Atención: Seleccione un nombre común que coincida con la dirección IP o el nombre de host que XClarity Administrator utiliza para conectar con el dispositivo gestionado. Si no selecciona el valor correcto, se podrían producir conexiones no fiables.

e. Personalice los nombres alternativos de asunto (SAN) que se añaden a la extensión X.509 “subjectAltName” cuando se genera el CSR.

De forma predeterminada, XClarity Administrator define automáticamente los nombres alternativos de asunto (SAN) para CSR según la dirección IP y el nombre de host que se detectó mediante las interfaces de red del sistema operativo invitado de XClarity Administrator. Puede personalizar, eliminar o agregar a estos valores SAN.

El nombre que especifique debe ser válido para el tipo seleccionado:
- **directoryName** (por ejemplo, `cn=lxca-example,ou=dcg,dc=company,dc=com`)
- **dNSName** (por ejemplo, `lxca-example.dcg.company.com`)
- **ipAddress** (por ejemplo, `192.0.2.0`)
- **registeredID** (por ejemplo, `1.2.3.4.55.6.5.99`)
- **rfc822Name** (por ejemplo, `example@company.com`)
- **uniformResourceIdentifier** (por ejemplo, `https://lxca-dev.dcg.company.com/example`)

Nota: Todas las SAN que se enumeran en la tabla se validan, guardan y añaden a CSR solo después de que genere CSR en el paso siguiente.

f. Haga clic en **Generar archivo CSR**. El certificado de servidor se muestra en el cuadro de diálogo Solicitud de firma de certificado.

g. Haga clic en **Guardar en archivo** para guardar el certificado de servidor en el servidor host.

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

Paso 3. Cargue el certificado de servidor firmado externamente en XClarity Administrator. El contenido del certificado debe ser un conjunto que contiene el certificado raíz de la CA, el certificado intermedio y el certificado de servidor.

a. En la barra de menús de XClarity Administrator, haga clic en **Administración → Seguridad** para mostrar la página Seguridad.

b. Haga clic en **Certificado de servidor** en la sección Gestión de certificados.

c. Haga clic en la pestaña **Cargar certificado**.

d. Haga clic en **Cargar certificado** para mostrar el cuadro de diálogo Cargar certificado.

e. Especifique un archivo de conjunto de certificados, en formato PEM, DER o PKCS7 o pegue el conjunto de certificados en formato PEM.

f. Haga clic en **Cargar** para cargar el certificado de servidor y almacenarlo en el almacén de confianza de XClarity Administrator.

Despliegue de certificados de servidor personalizados en dispositivos gestionados

Puede desplegar certificados de servidor personalizados en dispositivos gestionados cargando e instalando el conjunto de certificados firmados externamente utilizando el CMM y el controlador de gestión de dichos dispositivos.

Antes de empezar

Asegúrese de que esté instalado el firmware más reciente en todos los dispositivos gestionados (consulte Actualización de firmware en dispositivos gestionados).

Cuando vaya a generar una solicitud de firma de certificado (CSR) para certificados personalizados, asegúrese de que selecciona un nombre común que coincida con la dirección IP o nombre de host que se utiliza para identificar el dispositivo. Si no selecciona el valor correcto, se podrían producir conexiones no fiables.

Asegúrese de obtener un conjunto de certificados que contenga toda la cadena de firma, desde el certificado de servidor final hasta el certificado raíz (base) de la entidad de certificación (CA) de confianza, que se puede utilizar para verificar toda la cadena de confianza del certificado.

No cambie el certificado de servidor de Lenovo XClarity Administrator mientras un dispositivo gestionado esté “fuera de línea”. Debe reparar la conexión antes de modificar Lenovo XClarity Administrator, si no puede ser necesario realizar pasos adicionales para reparar los problemas de conectividad (consulte Resolución de un certificado de servidor no fiable).

Acerca de esta tarea

Esta sección contiene las recomendaciones para garantizar la comunicación satisfactoria entre Lenovo XClarity Administrator y los dispositivos gestionados. Para obtener instrucciones detalladas acerca de cómo generar un CSR e importar un certificado firmado, consulte la documentación del dispositivo.

Si Lenovo XClarity Administrator está gestionando uno o varios chasis, servidores de bastidor y servidores de torre, los certificados firmados internamente de Lenovo XClarity Administrator predeterminados están instalados en Lenovo XClarity Administrator y en dispositivos gestionados, puede desplegar un certificado de servidor personalizado.

Si el certificado de servidor firmado externamente está instalado en el dispositivo *antes* de que intente gestionar el dispositivo mediante Lenovo XClarity Administrator, no se necesita realizar ningún paso adicional. Para desplegar un certificado de servidor personalizado a los dispositivos gestionados por Lenovo XClarity Administrator, debe realizar uno de los siguientes pasos para garantizar la conectividad continua entre el servidor de gestión y los dispositivos gestionados.

Procedimiento

Use una de las siguientes opciones para desplegar un certificado de servidor firmado externamente y personalizado para gestionar chasis o servidores.

- Si Lenovo XClarity Administrator utiliza un certificado firmado por la misma entidad de certificación que los dispositivos gestionados, realice los pasos de Desplegar certificados de servidor personalizado en

Lenovo XClarity Administrator *antes* de instalar los certificados en los dispositivos gestionados. La instalación de la cadena de certificados de Lenovo XClarity Administrator de la misma CA asegura que la cadena de certificados se encuentra en el almacén de confianza de Lenovo XClarity Administrator y de que Lenovo XClarity Administrator puede confiar en los dispositivos después de que los certificados firmados externamente estén instalados allí.

- Añada los certificados firmados externamente en las cadenas de firma de la CA al almacén de confianza de Lenovo XClarity Administrator.

  Debe añadir el certificado raíz de la CA y todos los certificados intermedios, uno cada vez, al almacén de confianza de Lenovo XClarity Administrator. El orden no importa. Cada certificado debe instalarse una vez, de modo que si todos los dispositivos utilizan la misma CA y los mismos certificados intermedios, la CA y cada certificado intermedio debe instalarse en el almacén de confianza de Lenovo XClarity Administrator una vez. Si se utiliza más de una CA o una CA intermediaria, asegúrese de que cada certificado raíz de la CA o certificados intermedios que se utilizan en la cadena de firma de un dispositivo gestionado se importen siguiendo estos pasos.

  Nota: No añada los certificados de servidor finales que no son de la CA durante estos pasos.

  Lleve a cabo estos pasos para cada certificado del conjunto.

  1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Administración → Seguridad** para mostrar la página Seguridad.
  2. Haga clic en **Certificados de confianza** en la sección Gestión de certificados del área de navegación izquierda.
  3. Haga clic en el icono de **Crear** ( ) para mostrar el cuadro de diálogo Añadir certificado.
  4. Especifique un archivo de certificados en formato PEM o DER o pegue el certificado en formato PEM.
  5. Haga clic en **Crear** para crear el certificado.

  Una vez instalada la cadena de firma de la CA, Lenovo XClarity Administrator comprueba la confianza de las conexiones con los servidores CIM del CMM y del controlador de gestión donde está instalado el certificado de servidor firmado externamente.
- Importe los certificados firmados externamente en los dispositivos gestionados.

  Nota: Si los certificados necesarios no están presentes en el almacén de confianza de Lenovo XClarity Administrator, la conectividad se pierde entre Lenovo XClarity Administrator y el dispositivo gestionado. Realice los pasos de Resolución de un certificado de servidor no fiable para reparar la conexión.

  Importante: Esta opción implica pérdida de conectividad temporal; por lo tanto se recomienda una de las opciones anteriores.

Regenerar o restaurar el certificado de servidor autofirmado de Lenovo XClarity Administrator

Puede generar un nuevo certificado de la entidad de certificación o de servidor para sustituir los certificados autofirmados actuales o para reinstalar un certificado generador por Lenovo XClarity Administrator si XClarity Administrator utiliza actualmente un certificado de servidor firmado externamente personalizado. El nuevo certificado de servidor autofirmado se utiliza a continuación en los servidores de autenticación, HTTPS y CIM de XClarity Administrator. También se suministra automáticamente a todos los dispositivos gestionados.

Antes de empezar

Cuando vuelva a generar o cargar el certificado XClarity Administrator, XClarity Administrator se reiniciará.

Si se genera un nuevo certificado de CA, el nuevo certificado de CA se despliega automáticamente al almacén de confianza en cada controlador de gestión de CMM y de placa base, para que todos los chasis

gestionados, servidores de bastidor y servidores de torre mantengan conexiones de confianza de autenticación con el servidor. Si ocurre un error mientras se despliega el certificado raíz de la CA, descárguelo desde la página de la entidad de certificación e impórtela manualmente en el almacén de confianza de cualquier dispositivo gestionado al que no haya aprovisionado correctamente antes de generar un nuevo certificado de servidor.

Si desea volver a generar el certificado de la CA, reserve una hora para volver a generar la CA, solucione cualquier error de aprovisionamiento y regenere el certificado del servidor dentro de un período de tiempo.

Después de generar un nuevo certificado raíz de la CA, pueden producirse errores de comunicación o es posible que no pueda iniciar sesión en un dispositivo hasta después de que se regenere y está firmado el certificado de servidor.

Importante: Para XClarity Administrator versión 1.1.1 y anterior, debe importar el certificado raíz de la CA al almacén de confianza de cada CMM y controlador de gestión. Consulte la documentación del CMM y controlador de gestión para obtener más información acerca de la importación del certificado raíz de la CA

Procedimiento

Lleve a cabo los pasos siguientes para restaurar un certificado de servidor autofirmado en XClarity Administrator.

Nota: El certificado de servidor que está actualmente en uso en XClarity Administrator, ya sea autofirmado o externamente firmado, permanece en uso hasta que se regenere y está firmado el nuevo certificado de servidor.

Paso 1. **Opcional:** genere un nuevo certificado raíz de la CA.

a. En la barra de menús de XClarity Administrator, haga clic en **Administración → Seguridad** para mostrar la página Seguridad.

b. Haga clic en **Entidad de certificación** en la sección Gestión de certificados.

c. Haga clic en **Volver a generar certificado raíz de entidad de certificación**.

Si la clave y el certificado de CA se regeneran correctamente, se muestra un cuadro de diálogo que muestra el estado de trabajos a aprovisionar con ese certificado como un certificado de confianza LDAP a todos los CMM y controladores de gestión (para servidores convergidos, NeXtScale y System x). Este cuadro de diálogo, así como la página de supervisión del trabajo, muestran si el trabajo de aprovisionamiento de cada trabajo se realizó correctamente o no.

Si cualquiera de los trabajos de aprovisionamiento fallan, complete los pasos siguientes para descargar el certificado raíz de la CA, luego importe manualmente el certificado raíz como un certificado LDAP de confianza en cualquier dispositivo donde el trabajo haya fallado.

Paso 2. **Opcional:** descargue el certificado raíz de la CA al sistema host e impórtelo a su navegador web.

a. En la barra de menús de XClarity Administrator, haga clic en **Administración → Seguridad** para mostrar la página Seguridad.

b. Haga clic en **Entidad de certificación** en la sección Gestión de certificados.

c. Haga clic en **Descargar certificado raíz de entidad de certificación**. Se muestra el certificado raíz actual de la CA en el cuadro de diálogo Certificado raíz de la entidad de certificación.

d. Haga clic en **Guardar en archivo** para guardar el certificado raíz de la CA en el sistema host.

e. Siga las instrucciones para su navegador web y el navegador web de otros usuarios que tienen acceso a XClarity Administrator para importar el certificado como una entidad de confianza de raíz.

Paso 3. Vuelva a generar un nuevo certificado de servidor y firme el certificado con el nuevo certificado raíz de la CA.

a. Desde la página Seguridad, haga clic en **Certificado de servidor** en la sección Gestión de certificados.

b. Haga clic en la pestaña **Volver a generar certificado de servidor**.

c. Rellene los campos de la página Volver a generar certificado de servidor:
- País o región
- Estado o provincia
- Ciudad o localidad
- Organización
- Unidad de organización
- Nombre común
- No válido antes de la fecha
- No válido antes de la hora
- No válido después de la fecha
- No válido después de la hora

d. Haga clic en **Volver a generar certificado**.

e. Si va a volver a generar certificados autofirmados en los CMM gestionados y en los controladores de gestión (para servidores Converged, NeXtScale, ThinkSystem y System x), después de volver a generar los certificados en cada dispositivo, importe el certificado nuevo de dispositivo en el almacén de confianza de XClarity Administrator (consulte Resolución de un certificado de servidor no fiable). Como alternativa, puede descargar manualmente el certificado desde el dispositivo e importarlo en XClarity Administrator en la página Certificados de confianza.

Para XClarity Administrator versión 1.1.0 y anterior, el servidor web reinicia y completa automáticamente todas las sesiones del navegador después de volver a generar un certificado. Para XClarity Administrator versión 1.1.1 y posterior, XClarity Administrator comienza a utilizar el nuevo certificado sin finalizar las sesiones existentes. Las nuevas sesiones se establecen utilizando el nuevo certificado. Para ver el nuevo certificado en uso, reinicie el navegador web.

Paso 4. Si va a volver a generar certificados autofirmados en los CMM gestionados y en los controladores de gestión (para servidores Converged, NeXtScale, ThinkSystem y System x), después de volver a generar los certificados en cada dispositivo, importe el certificado nuevo de dispositivo en el almacén de confianza de XClarity Administrator (consulte Resolución de un certificado de servidor no fiable). Como alternativa, puede descargar manualmente el certificado desde el dispositivo e importarlo en XClarity Administrator en la página Certificados de confianza.

Resolución de un certificado de servidor no fiable

El certificado de servidor que se utiliza para establecer una conexión segura con un dispositivo gestionado puede pasar a ser no fiable. Si el problema se debe a una versión de nivel inferior del certificado raíz de la CA del dispositivo o del certificado autofirmado del dispositivo en el almacén de confianza de Lenovo XClarity Administrator, XClarity Administrator puede resolver el certificado de servidor no fiable.

Acerca de esta tarea

Si un dispositivo gestionado pasa a ser no fiable, XClarity Administrator impide la comunicación con dicho dispositivo, de modo que no podrá realizar operaciones de gestión o inventario en dicho dispositivo.

Procedimiento

Para resolver un certificado de servidor no fiable de un dispositivo gestionado, lleve a cabo los pasos siguientes.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Hardware** y, a continuación, haga clic en el tipo de dispositivo (**Chasis**, **Servidor**, **Almacenamiento** o **Conmutador**). Se muestra una página con una vista de tabla de todos los dispositivos gestionados de ese tipo.

Paso 2. Seleccione un dispositivo específico en el estado “Fuera de línea”.

Paso 3. Haga clic en **Todas las acciones → Seguridad → Resolver certificados no fiables**.

Paso 4. Haga clic en **Instalar certificado**.

XClarity Administrator recupera el certificado actual del dispositivo objetivo. Si ese certificado difiere del certificado de confianza del dispositivo en el almacén de confianza de XClarity Administrator, el nuevo certificado se coloca en el almacén de confianza de XClarity Administrator y sustituye al certificado anterior de dicho dispositivo.

Si esto no solucionan el problema, asegúrese de que la conectividad de red esté funcionando entre XClarity Administrator y el dispositivo.

Descargando el certificado de servidor

Puede descargar una copia del certificado de servidor actual, en formato PEM o DER, en su sistema local. A continuación, puede importar el certificado a su navegador web u otras aplicaciones (como Lenovo XClarity Mobile o Lenovo XClarity Integrator).

Procedimiento

Lleve a cabo los pasos siguientes para descargar el certificado de servidor.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Administración → Seguridad** para mostrar la página Seguridad.

Paso 2. Haga clic en **Certificado de servidor** en la sección Gestión de certificados. Se muestra la página Certificado de servidor.

Paso 3. Haga clic en la pestaña **Descargar certificado**.

Paso 4. Haga clic en **Descargar certificado**.

Paso 5. Pulse **Guardar como DER** o **Guardar como PEM** para guardar el certificado de servidor como un archivo DER o PEM en su sistema local.

Importación del certificado de la Entidad de certificación en un navegador web

Para evitar recibir mensajes de advertencia del navegador web al acceder a Lenovo XClarity Administrator, puede descargar una copia del certificado actual de la Entidad de certificación (CA), en formato PEM o DER, en su sistema local e importar ese certificado de servidor a la lista de certificados de confianza del navegador web.

Acerca de esta tarea

XClarity Administrator admite firmas del certificado RSA-3072/SHA-384, RSA-2048/SHA-256 y ECDSA p256/SHA-256. Otros algoritmos como SHA-1 superior o SHA hash se pueden admitir dependiendo de la configuración. Considere el modo criptográfico seleccionado en XClarity Administrator (consulte Configuración de valores de criptografía en el servidor de gestión), los valores de seguridad seleccionados para servidores gestionados (Configuración de los valores de seguridad para un servidor gestionado) y las capacidades de otros software y dispositivos en su entorno. Los certificados ECDSA que se basan en algunas curvas elípticas (incluidos los p256), pero no se admiten todas las curvas elípticas en la página de certificados de confianza y en la cadena de firma del certificado de XClarity Administrator, pero *no* se admiten actualmente para su uso por el certificado de servidor de XClarity Administrator.

Nota: XClarity Administrator utiliza firmas del certificado RSA- 3072/SHA-384 para servidores con XCC2 en modo estricto.

Procedimiento

Para descargar el certificado de servidor, lleve a cabo los pasos siguientes.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Administración → Seguridad** para mostrar la página Seguridad.

Paso 2. Haga clic en **Entidad de certificación** en la sección Gestión de certificados. Aparece la página Entidad de certificación.

Paso 3. Haga clic en **Descargar certificado raíz de entidad de certificación**.

Paso 4. Haga clic en **Guardar como DER** o **Guardar como PEM** para guardar el certificado de servidor como un archivo DER o PEM en su sistema local.

Paso 5. Importe el certificado que ha descargado en la lista de certificados de confianza de la autoridad raíz del navegador.

- **Firefox:**
  1. Abra el navegador y haga clic en **Herramientas → Opciones → Avanzado**.
  2. Haga clic en la pestaña **Certificados**.
  3. Haga clic en **Ver certificados**.
  4. Haga clic en **Importar** y vaya a la ubicación donde se descargó el certificado.
  5. Seleccione el certificado y haga clic en **Abrir**.
- **Internet Explorer:**
  1. Abra el navegador y haga clic en **Herramientas → Opciones de Internet → Contenido**.
  2. Haga clic en **Certificados** para ver una lista de todos los certificados de confianza actuales.
  3. Pulse **Importar** para mostrar el asistente Importar certificado.
  4. Complete el asistente para importar el certificado.

Adición y sustitución de una lista de revocación de certificados

Una *lista de revocación de certificados* es una lista de certificados que se han revocado y ya no son de confianza. Se puede revocar un certificado si la CA lo ha emitido incorrectamente o si la clave está en peligro, se ha perdido o ha sido robada.

Procedimiento

Lleve a cabo los pasos siguientes para agregar una nueva lista de revocación de certificados o para sustituir una existente.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Administración → Seguridad** para mostrar la página Seguridad.

Paso 2. Haga clic en **Listas de revocación de certificados** en la sección Gestión de certificados del área de navegación izquierda. Se muestra la página Listas de revocación de certificados donde se incluyen todas las listas de revocación de certificados.

Paso 3. Haga clic en **Añadir/Reemplazar CLR** para agregar una lista de revocación de certificados o para seleccionar una lista de revocación de certificados y haga clic en **Añadir/Reemplazar CLR** para sustituir la CRL.

Paso 4. Especifique un archivo de lista de revocación de certificados, en formato PEM o DER o pegue el certificado en formato PEM.

Paso 5. Pulse **Crear** para crear una lista de revocación de certificados.

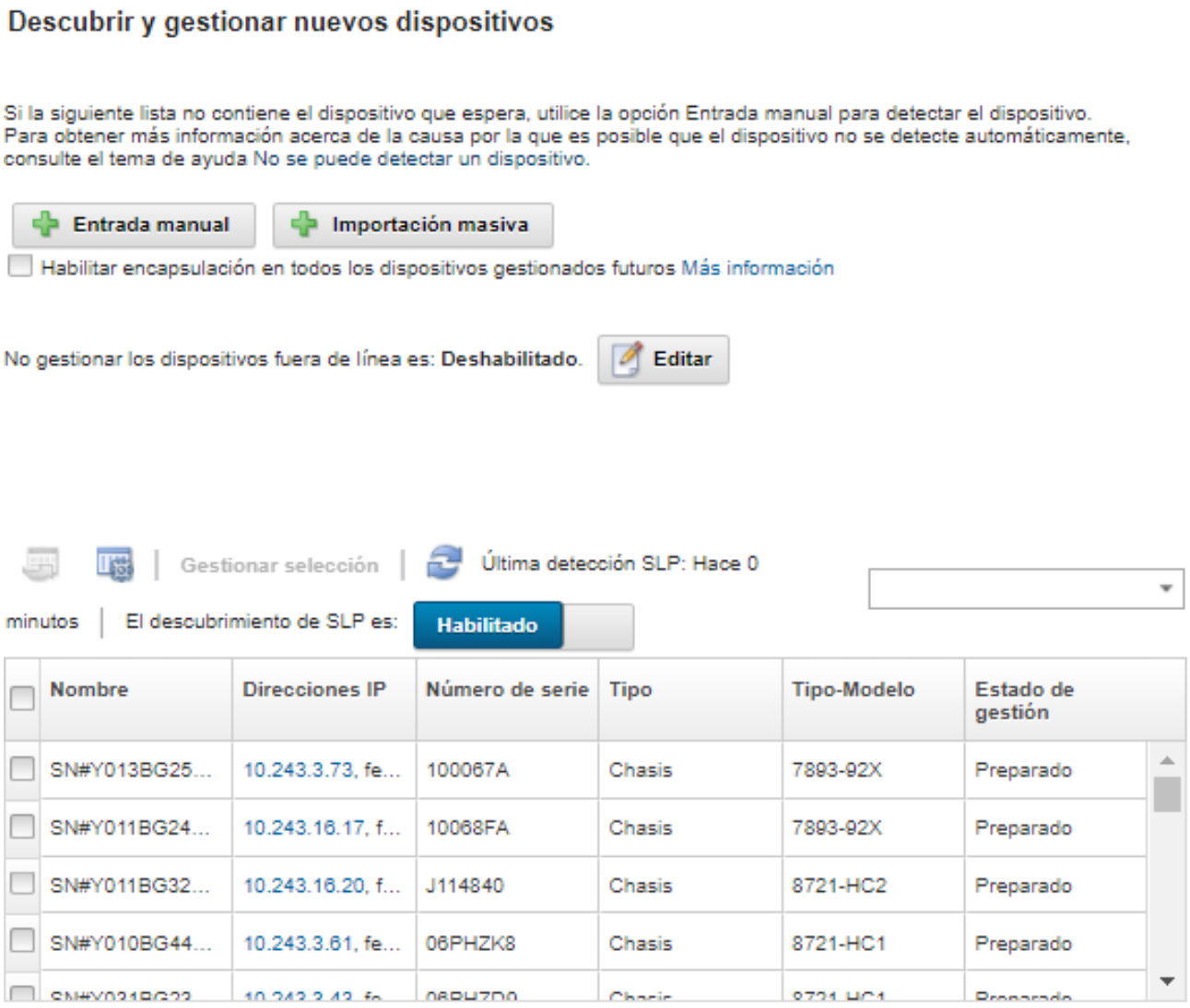
Habilitar encapsulación

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.

Puede habilitar o deshabilitar la encapsulación globalmente para todos los dispositivos durante el proceso de gestión seleccionando la casilla de verificación **Habilitar encapsulación en todos los dispositivos gestionados futuros** en la página Detectar y gestionar dispositivos nuevos. La encapsulación está deshabilitado de forma predeterminada.



También puede habilitar o deshabilitar la encapsulación individualmente para los dispositivos gestionados específicos en cualquier momento navegando a la página de resumen del dispositivo, seleccionando el dispositivo y **Acciones → Habilitar encapsulación** o **Acciones → Deshabilitar 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 archivo lenovoMgrAlert.mib y la Recuperación de la gestión con un CMM después de un error en el servidor de gestión.

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

Implementación de la conformidad con NIST SP 800-131A

Si debe cumplir con NIST SP 800-131A, puede empezar a trabajar para conseguir un entorno que se ajuste plenamente a las normas utilizando Lenovo XClarity Administrator.

Acerca de esta tarea

En la publicación especial 800-131A del Instituto Nacional de Estándares y Tecnología (NIST SP 800-131A) se especifica la forma en que deben gestionarse las comunicaciones seguras. El estándar fortalece los algoritmos e incremente las longitudes de las claves para mejorar la seguridad. El estándar NIST SP 800-131A requiere que los usuarios estén formados para cumplir estrictamente con ella.

Notas: En la actualidad, los siguientes componentes de Flex System no son compatibles con NIST SP 800-131A. Las comunicaciones entre XClarity Administrator o el CMM y estos componentes no cumplen con estos estándares:

- Conmutador escalable Flex System EN4023 de 10 Gb
- Conmutador Ethernet Flex System EN6131 de 40 Gb
- Conmutador SAN Flex System FC3171 de 8 Gb
- Conmutador escalable SAN Flex System FC5022 de 16 Gb
- Conmutador InfiniBand IB6131 Flex System

Nota: Cuando se utiliza un proveedor de identidad SAML para la autenticación, XClarity Administrator utiliza SHA-1 para incluir la firma en los metadatos. El uso del algoritmo SHA-1 para las firmas digitales no es compatible con NIST SP 800-131A.

Procedimiento

Lleve a cabo los pasos siguientes para implementar la conformidad con NIST SP 800-131A.

Paso 1. Asegúrese de que sus dispositivos cumplen los siguientes criterios:

- Utilizar la Capa de sockets seguros (SSL) sobre el protocolo TLS v1.2.
- Utilizar funciones de algoritmos hash SHA-256 o más complejos para las firmas digitales y funciones de algoritmos hash SHA-1 o más complejos para otras aplicaciones.
- Utilizar un sistema RSA-2048 o más complejo, o curvas elípticas aprobadas por NIST que tengan, como mínimo, 224 bits.
- Utilizan un sistema de cifrado simétrico aprobado por NIST con claves que tengan una longitud mínima de 128 bits.
- Utilizar generadores de números aleatorios aprobados por NIST.
- Siempre que sea posible, permitir los mecanismos de intercambio de claves de Diffie-Hellman o de curvas elípticas de Diffie-Hellman.

Paso 2. Configure los valores criptográficos en Lenovo XClarity Administrator. Hay dos valores que están relacionados con la conformidad con NIST SP 800-131A:

- El *modo SSL/TLS* especifica los protocolos que deben utilizarse para las comunicaciones seguras. XClarity Administrator admite un valor de **Servidor y cliente de TLS 1.2** para restringir el protocolo de criptografía a TLS 1.2, tanto en XClarity Administrator como en todos los dispositivos gestionados.
- El *modo criptográfico* establece la longitud de las claves que deben utilizarse si se han implementado comunicaciones seguras. Puede definir el modo criptográfico como **NIST SP 800-131A**. No obstante, es posible que no pueda desplegar algunos sistemas operativos mediante XClarity Administrator, dado que algunos instaladores de sistemas operativos no admiten los valores restringidos. Para la compatibilidad con el despliegue del sistema operativo, puede decidir si va a permitir una excepción para el despliegue del sistema operativo.

Cuando cambia la configuración criptográfica, XClarity Administrator aprovisiona los nuevos valores a todos los dispositivos gestionados e intenta solucionar los nuevos certificados en esos dispositivos.

Nota: Debe reiniciar manualmente Lenovo XClarity Administrator después de que los valores criptográficos se cambien para que los cambios entren en vigor y para restaurar cualquier servicio perdido (consulte Reiniciar XClarity Administrator).

Para obtener más información sobre estos valores, consulte Configuración de valores de criptografía en el servidor de gestión.

Paso 3. Utilice un navegador web que admita el protocolo TLS1.2 y las funciones de algoritmos hash SHA-256 y habilite estos valores en el navegador web.

Nota: Si utiliza o planea utilizar certificados personalizados o firmados externamente, todos los certificados de la cadena deben basarse en las funciones hash SHA-256.

Paso 4. Utilice protocolos cifrados para todas las comunicaciones. No habilite protocolos no cifrados, como Telnet, FTP y VNC para las comunicaciones remotas con los dispositivos gestionados de XClarity Administrator.

Uso de las herramientas de VMware

El paquete de herramientas de VMware se instala en la máquina virtual y en el sistema operativo invitado cuando instala Lenovo XClarity Administrator en entornos basados en VMware ESXi. Este paquete proporciona un subconjunto de las herramientas de VMware que admiten la copia de seguridad y la migración optimizadas de dispositivos virtuales, al tiempo que preservan el estado y la continuidad de la aplicación.

Para obtener información acerca de la utilización de las herramientas de VMware, consulte Uso de la utilidad de configuración de las herramientas de VMware en el sitio web del centro de documentación de VMware vSphere.

Configuración del acceso de red

Cuando configura Lenovo XClarity Administrator inicialmente, puede configurar hasta dos interfaces de red. Además, debe especificar qué interfaces se deben utilizar para desplegar sistemas operativos. Después de la configuración inicial, puede modificar estos valores.

Antes de empezar

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.
- Cuando se ejecuta XClarity Administrator como un contenedor.
  - Solo puede habilitar o deshabilitar la comprobación de direcciones IP duplicadas, modificar los roles de interfaz de red y modificar los valores del proxy. El resto de los valores de red (incluidos la dirección IP, la puerta de enlace y DNS) se definen en la configuración del contenedor.
  - Asegúrese de que la red macvlan esté configurada en el sistema host.

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, 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 acerca de las interfaces de red de XClarity Administrator, incluidas las limitaciones de la dirección IPv6, consulte Consideraciones de red en la documentación en línea de XClarity Administrator.

Procedimiento

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

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Administración → Acceso de red**. Se muestran los valores de red actuales.

Paso 2. Opcionalmente, puede habilitar la comprobación de direcciones IP duplicadas en la misma subred haciendo clic en el icono de alternación **Verificación de dirección IP duplicada**.

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.

Paso 3. Haga clic en **Editar acceso de red** para mostrar la página Editar acceso de red.

Paso 4. 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 5. (XClarity Administrator solo como dispositivo virtual) Modifique 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 IPv6 en la documentación en línea de XClarity Administrator.

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 6. (XClarity Administrator solo como dispositivo virtual) Opcionalmente, modifique 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.

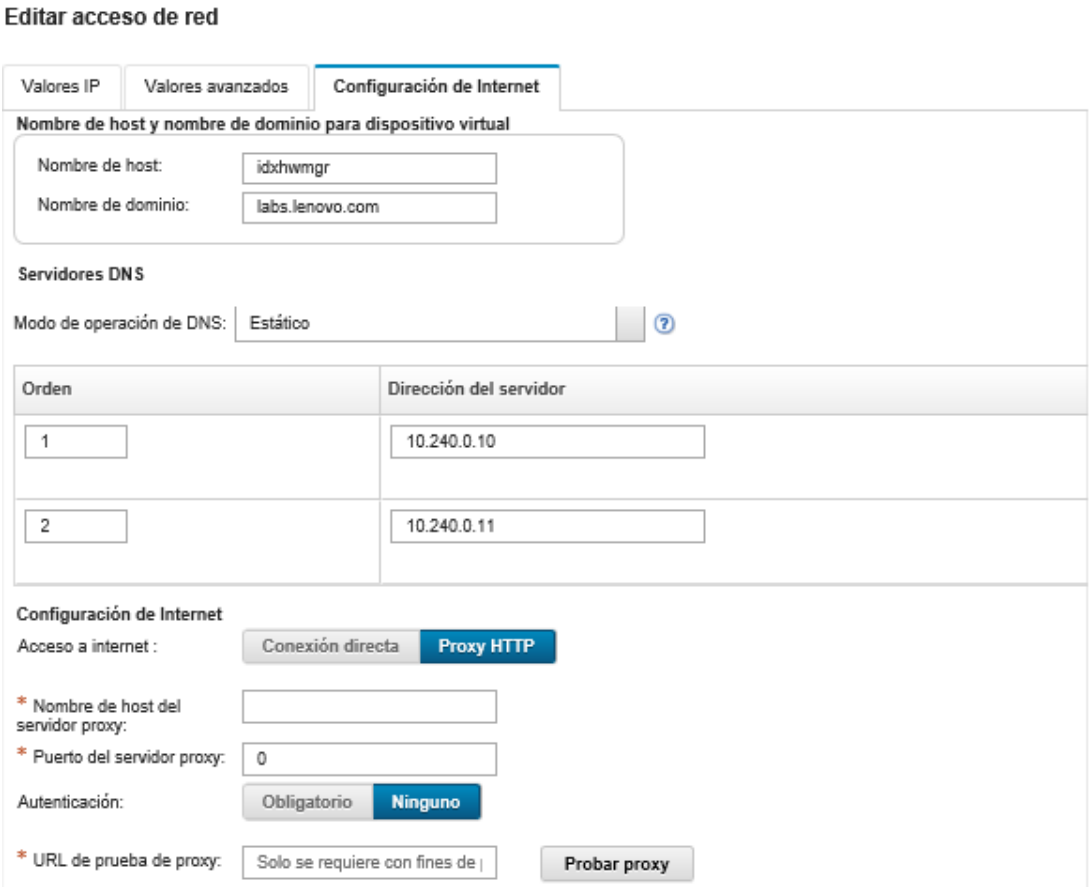
5. Especifique la dirección de la puerta de enlace a la que deben dirigirse los paquetes.

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

Paso 7. También puede modificar los valores de DNS y proxy.

Cuando se configura como XClarity Administrator un contenedor, solo se pueden modificar los valores del proxy desde la interfaz web. Los valores DNS se definen en el contenedor.

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 y XCC2, 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).

También puede quitar la información de FQDN y DNS del servidor de gestión de los servidores gestionados con IMM2, XCC y XCC2 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 8. Haga clic en **Reiniciar** para reiniciar el servidor de gestión.

Paso 9. Haga clic en **Probar conexión** para verificar los valores de red.

Establecimiento de la fecha y la hora

Puede establecer la fecha y hora que va a utilizar para Lenovo XClarity Administrator.

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.

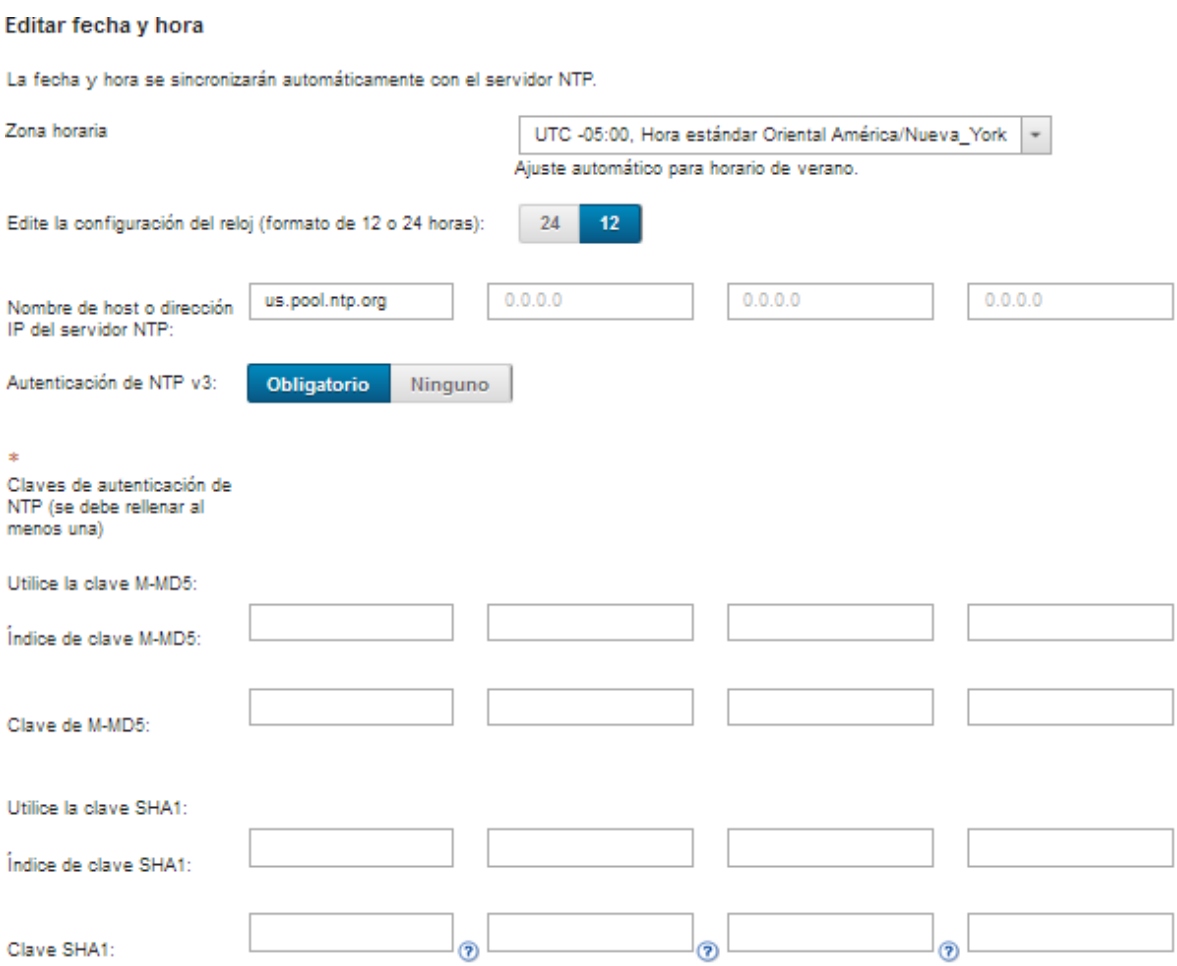
- Para ESXi, siga las instrucciones del VMware: página web de deshabilitar la sincronización de hora.
- Para Hyper-V, desde el Administrador de Hyper-V, haga clic con el botón derecho en XClarity Administrator máquina virtual y luego haga clic en **Configuración**. En el cuadro de diálogo, haga clic en **Gestión > Servicios de integración** en el panel de navegación y luego desactive **Sincronización de hora**.

Procedimiento

Lleve a cabo los pasos siguientes para establecer la fecha y la hora de XClarity Administrator.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Administración → Fecha y hora**. Aparece la página Fecha y hora. Esta página muestra la fecha y la hora actuales de XClarity Administrator.

Paso 2. Haga clic en **Editar fecha y hora** para mostrar la página Editar fecha y hora.



Paso 3. 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 4. Haga clic en **Guardar**.

Establecer preferencias de inventario

Puede especificar preferencias de inventario para dispositivos gestionados, lo que incluye la propiedad que se utiliza para visualizar el nombre del dispositivo.

Procedimiento

Lleve a cabo los pasos siguientes para configurar las preferencias de inventario para los dispositivos gestionados.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Administración → Preferencia de inventario**. Aparecerá la página Preferencias de Inventario.

Paso 2. Seleccione la propiedad que se utilizará para el nombre del dispositivo que se muestra en la interfaz de usuario de Lenovo XClarity Administrator. Puede seleccionar una de las siguientes propiedades.
- **Secuencia predefinida (predeterminado)**
- **Nombre definido por el usuario**
- **Nombre de host de DNS**
- **Nombre de host**
- **Dirección IPv4**
- **Número de serie**

Si se seleccionó **Secuencia predefinida**, el nombre del dispositivo a visualizar se elige en función de la secuencia de propiedades de la lista anterior. Por ejemplo, si un dispositivo tiene un nombre definido por el usuario, se muestra ese nombre. Si un dispositivo no tiene un nombre definido por el usuario, entonces se muestra el nombre de host de DNS. Si un dispositivo no tiene un nombre definido por el usuario o un nombre de host de DNS, se muestra el nombre de host.

Nota: Al seleccionar un valor distinto al predeterminado, se cambia el nombre de la propiedad seleccionada que se muestra en la interfaz de usuario de Lenovo XClarity Administrator en todos los dispositivos. El nombre definido por el usuario que se asigna al dispositivo no cambia.

Paso 3. Opcionalmente, haga clic en **Habilitar** para optar por ordenar cuadrículas (tablas) utilizando el valor que se seleccionó para el nombre del dispositivo.

Paso 4. Seleccione la preferencia orden de numeración de bastidor, ya sea de arriba abajo (por ejemplo, 1 a 52) o abajo a arriba (por ejemplo, 52 a 1).

Nota: El cambio de la preferencia de orden de números no cambia la ubicación de un dispositivo en el bastidor.

Paso 5. Haga clic en **Aplicar**.

Después de finalizar

Puede definir preferencias de umbral para generar alertas y sucesos cuando un valor, como la duración de una SSD en un servidor ThinkSystem o ThinkServer, supera un nivel crítico o de advertencia (consulte Configuración de preferencias de umbral para generar alertas y sucesos).

Configuración de preferencias de umbral para generar alertas y sucesos

Puede definir preferencias de umbral para generar alertas y sucesos cuando un valor, como la duración de una SSD en un servidor ThinkSystem o ThinkServer, supera un nivel crítico o de advertencia.

Procedimiento

Lleve a cabo los pasos siguientes para reenviar archivos de servicio específicos al proveedor de servicio.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Supervisión → Alertas** para mostrar la página Alertas.

Paso 2. Haga clic en el icono **Valores del umbral** ( ) para mostrar el cuadro de diálogo Valores del umbral.

Paso 3. Modifique los umbrales de advertencia o críticos para la vida restante de SSD en los servidores ThinkSystem y ThinkServer.

La vida restante de los SSD se calcula usando recuentos SMART del proveedor. Los valores predeterminados son un 30 % para el umbral de advertencia y un 20 % del umbral crítico.

Paso 4. Seleccione la alternación **Habilitado** para generar alertas y sucesos cuando se alcanza el umbral de cada uno.

Paso 5. Haga clic en **Aplicar**.

Configuración de notificaciones automáticas de problemas al Lenovo Soporte (Llamar a casa)

Puede crear un despachador de servicio que envíe automáticamente datos del servicio para que cualquier dispositivo gestionado en Lenovo Soporte utilice Llamar a casa cuando se reciben ciertos sucesos de mantenimiento, como una memoria no recuperable, desde dispositivos gestionados específicos, para que se pueda abordar el problema. Este servicio despachado se denomina “Predeterminado Llamar a casa.”

Lenovo está comprometido con la seguridad. Cuando está habilitado, Llamar a casa LenovoCentro de soporte cuando un dispositivo notifica un error de hardware o cuando elige iniciar una Llamar a casa manual. Los datos de servicio que normalmente se cargarían manualmente al soporte de Lenovo se envían automáticamente al LenovoCentro de soporte a través de HTTPS utilizando TLS 1.2 o posterior; los datos profesionales no se transmiten nunca. El acceso a los datos de servicio en el LenovoCentro de soporte está restringido al personal de servicio autorizado.

Antes de empezar

Atención: Debe aceptar el Declaración de privacidad de Lenovo antes de poder transferir datos al soporte de Lenovo.

Asegúrese de que todos los puertos que Lenovo XClarity Administrator requiere (incluidos los que se necesitan para la opción Llamar a casa) estén disponibles antes de habilitar la opción Llamar a casa. Para obtener más información sobre los puertos, consulte Disponibilidad de puertos en la documentación en línea de XClarity Administrator.

Asegúrese de que exista una conexión a las direcciones de Internet requeridas por Llamar a casa. Para obtener más información acerca de los firewall, consulte Firewall y servidores proxy en la documentación en línea de XClarity Administrator.

Si XClarity Administrator accede a Internet mediante un proxy HTTP, asegúrese de que el servidor proxy esté configurado para usar la autenticación básica y que no esté configurado como un proxy de terminación. Para obtener más información acerca de la configuración de proxy, consulte Configuración del acceso de redConfiguración del acceso de red en la documentación en línea de XClarity Administrator.

Después de configurar Llamar a casa, el despachador de servicio de **Llamar a casa de Lenovo predeterminado** se agrega a la página Despachadores de servicios. Puede editar este de despachador para configurar valores adicionales, incluido qué dispositivos se asocian a este despachador. Todos los dispositivos coinciden de manera predeterminada. Si no se especifica ningún dispositivo, Llamar a casa *no* reenviará notificaciones de problemas al soporte de Lenovo.

Acerca de esta tarea

Un *despachador de servicio* define información acerca del lugar al que deben enviarse los archivos de datos del servicio cuando se produce un suceso de mantenimiento. Puede definir hasta 50 despachadores de servicio.

- **Si un despachador de servicio de Llamar a casa no está configurado**, puede abrir manualmente un informe de servicio y enviar los archivos de servicio al LenovoCentro de soporte; para ello, siga las

instrucciones del Página Web de nueva solicitud de servicio. Para obtener más información acerca de cómo descargar los archivos de servicio, consulte Descarga de los archivos de diagnóstico de Lenovo XClarity Administrator y Recopilación y descarga de archivos de diagnóstico para un dispositivo en la documentación en línea de XClarity Administrator.

- **Si un despachador de servicio de Llamar a casa está configurado pero no está habilitado**, en cualquier momento puede abrir *manualmente* un informe de servicio y utilizar la función Llamar a casa para recopilar y transferir los archivos de servicio al LenovoCentro de soporte. Para obtener más información, consulte Apertura de un informe de servicio en la XClarity Administrator documentación en línea.
- **Si un despachador de servicio de Llamar a casa está configurado y habilitado**, XClarity Administrator recopila *automáticamente* datos del servicio, abre un informe de servicio y transfiere los archivos de servicio al LenovoCentro de soporte cuando se produce un suceso que se debe reparar, para así resolver el problema.

  Importante: Al habilitar un Llamar a casa despachador de servicio en Lenovo XClarity Administrator, Llamar a casa se deshabilita en cada dispositivo gestionado para evitar que se produzca duplicación de registros de problemas. Si tiene pensado dejar de utilizar Lenovo XClarity Administrator para gestionar sus dispositivos, o si pretende deshabilitar la función Llamar a casa en XClarity Administrator, puede volver a habilitar Llamar a casa en todos los dispositivos gestionados desde XClarity Administrator en lugar de volver a habilitar Llamar a casa en un momento posterior para dispositivo final individual.Para obtener información acerca de cómo volver a habilitar Llamar a casa en todos los dispositivos gestionados cuando el despachador de servicio de Llamar a casa está deshabilitado, consulte Nueva habilitación de Llamar a casa en todos los dispositivos gestionados en la documentación en línea de XClarity Administrator.Para los servidores con XCC2, XClarity Administrator guarda los datos del servicio en dos archivos del repositorio.

  – **Archivo de servicio**. (.zip) Este archivo contiene información de servicio e inventario en un formato de fácil lectura. Este archivo se envía automáticamente al LenovoCentro de soporte cuando ocurre un suceso que se debe reparar.
  – **Archivo de depuración**. (.tzz) El archivo contiene toda la información del servicio, el inventario y los registros de depuración para uso del soporte de Lenovo. Si se necesita información adicional para resolver un problema, puede enviar manualmente este archivo al soporte de Lenovo.

  Para otros dispositivos, XClarity Administrator guarda los datos del servicio (incluida la información del servicio, el inventario y los registros de depuración) en un solo archivo de servicio en el repositorio. Este archivo se envía al LenovoCentro de soporte cuando ocurre un suceso que se debe reparar.

  Aunque XClarity Administrator admite Llamar a casa para dispositivos ThinkAgile y ThinkSystem, el controlador de gestión de la placa base para algunos dispositivos ThinkAgile y ThinkSystem no incluye soporte para Llamar a casa. Por lo tanto, no puede habilitar ni deshabilitar la función Llamar a casa en esos mismos dispositivos. La función Llamar a casa solo puede habilitarse para estos dispositivos en el nivel XClarity Administrator.

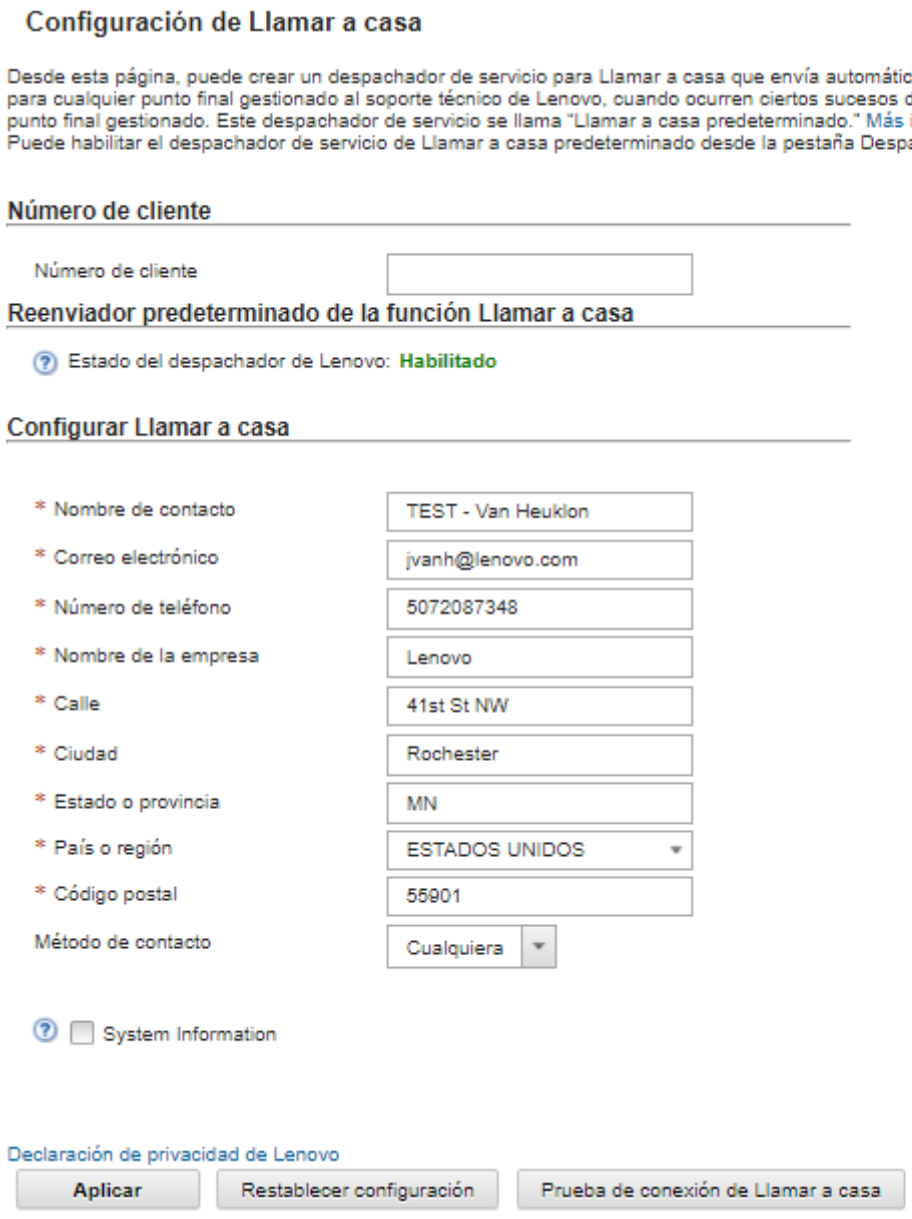
  La función Llamar a casa se suprime para los sucesos repetidos de cualquier dispositivo si hay un informe de servicio abierto para un suceso en ese dispositivo. La función Llamar a casa también se suprime para los sucesos similares de cualquier dispositivo ThinkAgile y ThinkSystem si hay un informe de servicio abierto para un suceso en ese dispositivo. Los sucesos ThinkAgile y ThinkSystem son cadenas de 16 caracteres en el siguiente formato *xx<2_char_reading_type><2_char_sensor_type>xx<2_char_entity_ID>xxxxxx* (por ejemplo, `806F010D0401FFFF`). Los sucesos son similares si tienen el mismo tipo de lectura, tipo de sensor e ID. de entidad. Por ejemplo, si hay un informe de servicio abierto para 806F010D0401FFFF de sucesos en un dispositivo ThinkAgile o ThinkSystem específico, se suprimen los sucesos que se producen en ese dispositivo con identificadores de sucesos como *xx*`6F01`*xx*`04`*xxxxxx*, donde *x* es cualquier carácter alfanumérico.

Para obtener información acerca de cómo ver los informes de servicio que se han abierto automáticamente con un despachador de servicio de Llamar a casa, consulte Visualización de estados e informes de servicio en la documentación en línea de XClarity Administrator.

Procedimiento

Lleve a cabo los pasos siguientes para configurar un despachador de servicio de Llamar a casa.

- Configure Llamar a casa para todos los dispositivos gestionados (actuales y futuros):
  1. En la barra de menús de XClarity Administrator, haga clic en **Administración → Servicio y soporte**.
  2. Haga clic en **Configuración de Llamar a casa** en el panel de navegación izquierdo para mostrar la página Configuración de Llamar a casa.



  3. (Opcional) Especifique el número de cliente de Lenovo predeterminado para utilizarlo al notificar problemas con XClarity Administrator.

Consejo: Puede encontrar su número de cliente en el correo electrónico de prueba de derecho que recibió cuando compró Lenovo XClarity Pro.

4. Rellene la información de contacto y ubicación.
5. Seleccione el método de contacto preferido por el soporte de Lenovo.
6. (Opcional) Rellene la información del sistema.
7. Haga clic en **Aplicar**.

   Se crea un despachador de servicio de Llamar a casa con el nombre “Llamar a casa predeterminado” para todos los dispositivos gestionados utilizando la información de contacto especificada.
8. Habilite y pruebe el despachador de servicio de “Llamar a casa predeterminado”.
   a. Haga clic en **Despachador de servicio** en el panel de navegación izquierdo para mostrar la página Despachadores de servicio.
   b. Seleccione **Habilitar** en la columna **Estado** para el despachador de servicio de “Llamar a casa predeterminado”.
   c. Seleccione el despachador de servicio de “Llamar a casa predeterminado” y haga clic en **Comprobar despachadores de servicio** para generar un suceso de prueba para el despachador de servicio y comprobar si XClarity Administrator es capaz de comunicarse con el centro de soporte de Lenovo.

      Puede supervisar el progreso de la prueba haciendo clic en **Supervisión → Trabajos** en la barra de menús de XClarity Administrator.

      Nota: Antes de poder probarlo, el despachador de servicio debe estar habilitado

- Configure Llamar a casa para los dispositivos gestionados específicos:
  1. En la barra de menús de XClarity Administrator, haga clic en **Administración → Servicio y soporte**.
  2. Haga clic en **Despachadores de servicio** en el panel de navegación izquierdo para mostrar la página Despachadores de servicio.
  3. Haga clic en el icono de **Crear despachador de servicio** ( ) para mostrar el cuadro de diálogo Nuevo despachador de servicio.
  4. Haga clic en la pestaña **General**.

   a. Seleccione **Llamar a casa** como el despachador de servicio:
   b. Introduzca el nombre del despachador de servicio y una descripción.
   c. Especifique el número de reintentos de notificaciones automáticas. El valor predeterminado es 2.

d. Especifique el número mínimo de minutos entre reintentos. El valor predeterminado es 2.

e. (Opcional) Haga clic en **Requiere inspección de datos de servicio** si desea inspeccionar los archivos de datos de servicio antes de que se transfieran y, opcionalmente, especifique la dirección de correo electrónico de contacto al cual se le notificará cuando se deban inspeccionar archivos de servicio.

5. Haga clic en la pestaña **Específico** y llene la información de contacto y sistema.

   Consejo: Para utilizar la misma información de contacto y ubicación que está configurada en la página Configuración de Llamar a casa, seleccione **Configuración general** en el menú desplegable **Configuración**.

6. Haga clic en la pestaña **Dispositivos** y seleccione los dispositivos gestionados y grupos de recursos para los que desea que este despachador de servicio reenvíe archivos de servicio.

   Consejo: Para reenviar los archivos del servicio de todos los dispositivos gestionados (actuales y futuros), seleccione la casilla de verificación **Igualar todos los dispositivos**.

7. Haga clic en **Crear**. El despachador de servicio se agrega a la página Servicio y soporte.
8. En la página Despachadores de servicio, seleccione **Habilitar** en la columna **Estado** para habilitar el despachador de servicio.
9. Seleccione el despachador de servicio y haga clic en **Comprobar despachadores de servicio** para generar un suceso de prueba para el despachador de servicio y comprobar si XClarity Administrator es capaz de comunicarse con el centro de soporte de Lenovo.

   Puede supervisar el progreso de la prueba haciendo clic en **Supervisión → Trabajos** en la barra de menús de XClarity Administrator.

   Nota: Antes de poder probarlo, el despachador de servicio debe estar habilitado.

Después de finalizar

En la página Servicio y soporte, también puede realizar las acciones siguientes:

- Si se selecciona **Requiere inspección de datos de servicio** y se recibió un suceso de mantenimiento desde uno de los dispositivos gestionados asociado al despachador de servicio, debe inspeccionar los archivos de servicio antes de que se reenvíen al proveedor de servicio. Para obtener más información, consulte Transferencia de archivos de diagnóstico al soporte de Lenovo en la XClarity Administrator documentación en línea.
- Determine si Llamar a casa está habilitado o deshabilitado en el dispositivo gestionado haciendo clic en **Acciones del punto final** en el panel izquierdo y verificando el estado en la columna **Llamar a casa Estado**.

  Consejo: si aparece “Estado desconocido” en la columna Estado de **Llamar a casa** actualice el navegador web para que muestre el estado correcto.
- Defina la información de contacto y ubicación de soporte para un dispositivo gestionado específico; para ello, haga clic en la pestaña **Acciones del punto final** en el panel de navegación izquierdo , seleccione el dispositivo y, a continuación, haga clic en el icono **Crear perfil de contacto** ( ) o **Editar perfil de contacto** ( ). La información de contacto y ubicación para el dispositivo gestionado se incluye en el informe de servicio que Llamar a casa envía al LenovoCentro de soporte. Si se especifica una información de contacto y ubicación única para un dispositivo gestionado, dicha información se incluye en el informe de servicio. De lo contrario, se usa la información general que se especifica para la configuración de XClarity Administrator Llamar a casa (en la página **Llamar a casa Configuración** o la página **Despachadores de servicio**). Para obtener más información, consulte el apartado LenovoCentro de soporte. Para obtener más información, consulte Definición de los contactos de soporte para un dispositivo en la XClarity Administrator documentación en línea.

- Visualice los informes de servicio enviados al LenovoCentro de soporte haciendo clic en **Estado del informe de servicio**, en el panel de navegación izquierda. Esta página muestra los informes de servicio que un despachador de servicio de Llamar a casa ha abierto automática o manualmente, como el estado y los archivos de servicio que se han transmitido al LenovoCentro de soporte. Para obtener más información, consulte Visualización de estados e informes de servicio en la XClarity Administrator documentación en línea.
- Recopile los datos del servicio de un dispositivo específico; para ello, haga clic en la pestaña **Acciones del punto final** en el panel de navegación izquierda, seleccione el dispositivo y, a continuación, haga clic en el icono **Recopilar datos del servicio** (). Para obtener más información, consulte Recopilación y descarga de archivos de diagnóstico para un dispositivo en la XClarity Administrator documentación en línea.
- Abra manualmente un informe de servicio en el LenovoCentro de soporte, recopile los datos de servicio de un dispositivo específico y envíelos al LenovoCentro de soporte; para ello, haga clic en la pestaña **Acciones del punto final** en el panel de navegación izquierdo, seleccione el dispositivo y, a continuación, haga clic en **Todas las acciones → Realizar Llamar a casa** manualmente.Si el LenovoCentro de soporte requiere datos adicionales, el Lenovo Soporte podría pedirle que vuelva a recopilar los datos de servicio de ese mismo u otro dispositivo.

  Para obtener más información, consulte Apertura de un informe de servicio en la XClarity Administrator documentación en línea.
- Reestablezca Llamar a casa en todos los dispositivos gestionados al hacer clic en **Acciones del punto final** en el panel de navegación izquierdo y luego haga clic en **Todas las acciones → Habilitar Llamar a casa en todos los dispositivos**.

  Al habilitar un Llamar a casa despachador de servicio en Lenovo XClarity Administrator, Llamar a casa se deshabilita en cada dispositivo gestionado para evitar que se produzca duplicación de registros de problemas. Si tiene pensado dejar de utilizar Lenovo XClarity Administrator para gestionar sus dispositivos, o si pretende deshabilitar la función Llamar a casa en XClarity Administrator, puede volver a habilitar Llamar a casa en todos los dispositivos gestionados desde XClarity Administrator en lugar de volver a habilitar Llamar a casa en un momento posterior para dispositivo final individual.

  Para obtener más información, consulte Nueva habilitación de Llamar a casa en todos los dispositivos gestionados en la documentación en línea de XClarity Administrator.

Configurar notificación automática de problemas para un proveedor de servicio de preferencia

Puede configurar Lenovo XClarity Administrator para que envíe automáticamente los archivos de diagnóstico de un conjunto específico de dispositivos gestionados a su proveedor de servicio de preferencia (incluido el soporte de Lenovo mediante la función Llamar a casa) cuando se reciban determinados sucesos de mantenimiento desde dispositivos gestionados (como un error irrecuperable de memoria), de manera que se pueda abordar y solucionar el problema.

Antes de empezar

Atención: Debe aceptar el Declaración de privacidad de Lenovo antes de poder transferir datos al soporte de Lenovo.

Asegúrese de que todos los puertos que XClarity Administrator requiere (incluidos los que se necesitan para Llamar a casa) estén disponibles antes de configurar el despachador de servicio. Para obtener más información sobre los puertos, consulte Disponibilidad de puertos en la documentación en línea de XClarity Administrator.

Asegúrese de que exista una conexión a las direcciones de Internet requeridas por el proveedor de servicio.

Si elige utilizar Lenovo Soporte, asegúrese de que exista una conexión a las direcciones de Internet requeridas por Llamar a casa. Para obtener más información acerca de los firewall, consulte Firewall y servidores proxy en la documentación en línea de XClarity Administrator.

Si XClarity Administrator accede a Internet mediante un proxy HTTP, asegúrese de que el servidor proxy esté configurado como un proxy de no terminación. Para obtener más información acerca de la configuración de proxy, consulte Configuración del acceso de redConfiguración del acceso de red en la documentación en línea de XClarity Administrator .

Acerca de esta tarea

Un *despachador de servicio* define información acerca del lugar al que deben enviarse los archivos de datos del servicio cuando se produce un suceso de mantenimiento. Puede definir hasta 50 despachadores de servicio

Para cada despachador de servicio, puede elegir transferir automáticamente los datos del servicio al soporte de Lenovo (lo que se denomina *Llamar a casa*), a la Herramienta de carga de Lenovo o a otro proveedor de servicio mediante SFTP. Para obtener información acerca de cómo un despachador de servicio para Llamar a casa, consulte Configuración de notificaciones automáticas de problemas al Lenovo Soporte (Llamar a casa) y Configurar notificación automática de problemas para un proveedor de servicio de preferencia. Para obtener información acerca de cómo un despachador de servicio para 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.

Si se configura y habilita un despachador de servicio para SFTP, XClarity Administrator recopila *automáticamente* datos de servicio y transfiere los archivos de servicio al sitio SFTP especificado para su proveedor de servicio de preferencia.

Para los servidores con XCC2, XClarity Administrator guarda los datos del servicio en dos archivos del repositorio.

- **Archivo de servicio**. (.zip) Este archivo contiene información de servicio e inventario en un formato de fácil lectura. Este archivo se envía automáticamente a su proveedor de servicio de preferencia cuando ocurre un suceso que se debe reparar.
- **Archivo de depuración**. (.tzz) El archivo contiene toda la información del servicio, el inventario y los registros de depuración para uso del soporte de Lenovo. Si se necesita información adicional para resolver un problema, puede enviar manualmente este archivo al soporte de Lenovo.

Para otros dispositivos, XClarity Administrator guarda los datos del servicio (incluida la información del servicio, el inventario y los registros de depuración) en un solo archivo de servicio en el repositorio. Este archivo se envía a su proveedor de servicio de preferencia cuando ocurre un suceso que se debe reparar.

Nota: Si se configuran múltiples despachadores de servicio de SFTP para el mismo dispositivo, solo uno de los despachadores de servicio transfieren datos de servicio. La dirección y el puerto que se utilizan dependen de qué despachador de servicio se activa primero.

Procedimiento

Lleve a cabo los pasos siguientes para definir y habilitar un despachador de servicio.

Paso 1. En la barra de menús de XClarity Administrator , haga clic en **Administración → Servicio y soporte**. Se abre la página Servicio y soporte.

Paso 2. Haga clic en **Despachadores de servicio** en el panel de navegación izquierdo para mostrar la página Despachadores de servicio.

Paso 3. Haga clic en el icono de **Crear despachador de servicio** ( ) para mostrar el cuadro de diálogo Nuevo despachador de servicio.

Paso 4. Haga clic en la pestaña **General**.

1. Seleccione **SFTP** para el despachador de servicio:
2. Introduzca el nombre del despachador de servicio y una descripción.
3. Especifique el número de reintentos de notificaciones automáticas. El valor predeterminado es 2.
4. Especifique el número mínimo de minutos entre reintentos. El valor predeterminado es 2.
5. (Opcional) Haga clic en **Requiere inspección de datos de servicio** si desea inspeccionar los archivos de servicio antes de que se transfieran y, opcionalmente, especifique la dirección de correo electrónico de contacto al cual se le notificará cuando se deban inspeccionar archivos de servicio.

Paso 5. Haga clic en la pestaña **Específico** y llene la siguiente información:
- Dirección IP y número de puerto del servidor SFTP
- Id. de usuario y contraseña para la autenticación en el servidor SFTP

Paso 6. Haga clic en la pestaña **Dispositivo** y seleccione los dispositivos gestionados y grupos de recursos para los que desea que este despachador de servicio reenvíe datos de servicio.

Consejo: para reenviar los datos del servicio de todos los dispositivos gestionados (actuales y futuros), seleccione la casilla de verificación **Igualar todos los dispositivos**.

Paso 7. Haga clic en **Crear**. El despachador de servicio se agrega a la página Servicio y soporte

Paso 8. En la página Servicio y soporte, seleccione **Habilitar** en la columna **Estado** para habilitar el despachador de servicio.

Paso 9. Para evitar que los sucesos de mantenimiento que se encuentran en la lista de sucesos excluidos abran automáticamente informes de problemas, seleccione **No** en la opción junto a la pregunta **¿Desea que los sucesos excluidos abran el informe de problemas?**

Paso 10. Seleccione el despachador de servicio y haga clic en **Comprobar despachadores de servicio** para generar un suceso de prueba para el despachador de servicio y comprobar si XClarity Administrator es capaz de comunicarse con cada proveedor de servicio.

Nota: Antes de poder probarlo, el despachador de servicio debe estar habilitado.

Después de finalizar

En la página Servicio y soporte, también puede realizar las acciones siguientes:

- Si se selecciona **Requiere inspección de datos de servicio** y se recibió un suceso de mantenimiento desde uno de los dispositivos gestionados asociado al despachador de servicio, debe inspeccionar los archivos de servicio antes de que se reenvíen al proveedor de servicio. Para obtener más información, consulte Inspección de archivos de diagnóstico en la XClarity Administrator documentación en línea .
- Modifique la información del despachador de servicio al hacer clic en la pestaña **Despachadores de servicio** en el panel de navegador izquierdo y el icono **Editar despachador de servicio** ().
- Habilite o deshabilite un proveedor de servicio al hacer clic en **Despachadores de servicio** y seleccionar **Habilitar** o **Deshabilitar** en la columna **Estado**.
- Elimine el proveedor de servicio al hacer clic en **Despachadores de servicio** y en el icono **Eliminar despachador de servicio** ().
- Defina la información de contacto y ubicación de soporte para un dispositivo gestionado específico; para ello, haga clic en la pestaña **Acciones del punto final** en el panel de navegación izquierdo , seleccione el dispositivo y, a continuación, haga clic en el icono **Crear perfil de contacto** () o **Editar perfil de contacto** (). La información de contacto y ubicación para el dispositivo gestionado se incluye en el registro de problemas que Llamar a casa crea en LenovoCentro de soporte. Si se especifica una información de contacto y ubicación única para un dispositivo gestionado, dicha información se incluye en el registro de problemas. De lo contrario, se utiliza la información general que se especifica para la configuración de Llamar a casa de XClarity Administrator (en la página **Configuración de Llamar a casa** o la página **Despachadores de servicio**). Para obtener más información, consulte Definición de los contactos de soporte para un dispositivo en la XClarity Administrator documentación en línea.
- Recopile los datos del servicio de un dispositivo específico; para ello, haga clic en **Acciones del punto final**, seleccione el dispositivo y, a continuación, haga clic en el icono **Recopilar datos del servicio** (). Para obtener más información, consulte Recopilación y descarga de archivos de diagnóstico para un dispositivo en la XClarity Administrator documentación en línea.

Para obtener más información acerca de estas tareas de servicio y soporte, consulte Trabajo con servicio y soporte en la documentación en línea de XClarity Administrator.

Conectar XClarity Administrator como concentrador al portal TruScale

Puede conectarse Lenovo XClarity Administrator como un concentrador de gestión al portal Lenovo TruScale.

Antes de empezar

Atención: Estos pasos de configuración están pensados solo para los representantes del servicio de Lenovo.

Procedimiento

Para conectar XClarity Administrator al portal TruScale, realice los pasos siguientes.

Paso 1. En la barra del menú XClarity Administrator, haga clic en **Administración → Configuración de concentrador** para mostrar la página Configuración de concentrador.

Paso 2. Cree una clave de registro haciendo clic en **Generar solicitud de registro**. Se muestra el cuadro de diálogo Generar solicitud de registro.

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

Paso 4. Haga clic en **Instalar clave de registro** para mostrar el cuadro de diálogo Instalar clave de registro.

Paso 5. Pegue la clave de registro en el campo **Clave de registro**.

Paso 6. Haga clic en **Enviar**.

Después de finalizar

Puede desinstalar la clave de registro haciendo clic en **Restablecer configuración**.

Creación de copia de seguridad, restauración y migración de los datos del sistema y de configuración

Puede utilizar Lenovo XClarity Administrator para realizar la copia de seguridad y la restauración de los valores y datos del sistema y los archivos importados, como imágenes del sistema operativo, actualizaciones de firmware y controladores de dispositivos de SO.

Copia de seguridad de Lenovo XClarity Administrator

Si ya dispone de procedimientos de copia de seguridad para hosts virtuales, asegúrese de que sus procedimientos incluyen Lenovo XClarity Administrator.

Antes de empezar

Atención: Asegúrese de notificar a todos los usuarios activos antes de iniciar el proceso de copia de seguridad. XClarity Administrator está inactivo durante el procedimiento para evitar la modificación de datos. Por lo tanto, no se puede acceder a XClarity Administrator mientras se está ejecutando el proceso de copia de seguridad.

Asegúrese de que el certificado de la entidad de certificación se haya descargado desde el dispositivo virtual XClarity Administrator y que se haya importado al navegador web (consulte Importación del certificado de la Entidad de certificación en un navegador web).

Asegúrese de que todos los trabajos en ejecución estén completos y que no hay ningún trabajo pendiente. Si hay trabajos en ejecución, puede elegir detener los trabajos en ejecución y continuar con la creación de la copia de seguridad.

Asegúrese de que los servidores de DNS se configuren correctamente, de lo contrario es posible que SMTP y NTP no funcionen correctamente después de restaurar una copia de seguridad.

Asegúrese de que haya suficiente espacio disponible en el servidor de gestión para la copia de seguridad. Si no es así, libere espacio en disco al eliminar recursos de , lo que incluye copias de seguridad anteriores, que no son necesarios (consulte XClarity Administrator en la documentación en línea de Gestión del espacio en el disco duro) o cree una nueva copia de seguridad sin incluir el sistema operativo, los archivos de actualización de firmware y controladores de dispositivo de SO.

Asegúrese de que el despliegue del SO esté configurado en la interfaz de red adecuada, eth1 o eth0, si desea realizar una copia de seguridad de las imágenes del SO (consulte Configuración del acceso de red).

Acerca de esta tarea

Realice siempre una copia de seguridad de XClarity Administrator después de realizar la configuración inicial y tras efectuar cambios significativos en la configuración, incluidos los siguientes:

- Antes de actualizar XClarity Administrator
- Al gestionar chasis o servidores de bastidor nuevos
- Cuando añada usuarios a XClarity Administrator
- Al crear y desplegar nuevos patrones de configuración

Asegúrese de realizar una copia de seguridad de XClarity Administrator de forma periódica.

Se recomienda descargar copias de seguridad en su sistema local. Si el sistema operativo del host se apaga de forma inesperada, puede que no pueda autenticarse con XClarity Administrator después de reiniciar el sistema operativo del host. Para resolver este problema, restaure XClarity Administrator de la última copia de seguridad en su sistema local (consulte Restauración de Lenovo XClarity Administrator).

Procedimiento

Complete los pasos siguientes para crear una copia de seguridad de XClarity Administrator.

Paso 1. Desde la barra de menús de XClarity Administrator, haga clic en **Administración → Crear copia de seguridad y restaurar datos**. Se muestra la página de Crear copia de seguridad y restaurar datos.

Paso 2. Haga clic en el icono **Crear copia de seguridad** (). Se muestra el cuadro de diálogo Crear copia de seguridad de datos y valores.

Paso 3. Ingrese una descripción de esta copia de seguridad.

Paso 4. Elija la ubicación donde desea crear la copia de seguridad. Esto puede ser el repositorio local o un recurso compartido remoto.

La copia de seguridad se crea en el repositorio local de forma predeterminada. Para copiar una copia de seguridad del repositorio local en un recurso compartido remoto, haga clic en el icono **Copia de seguridad** ().

Si elige un recurso compartido remoto, la copia de seguridad se crea primero en el repositorio local. A continuación, la copia de seguridad se copia al recurso remoto seleccionado y se elimina la copia local. Para obtener más información, consulte Gestión de remote shares.

Paso 5. Opcionalmente, seleccione esta opción para incluir las imágenes de sistemas operativos, las actualizaciones de firmware, y los controladores de dispositivos de SO.

Paso 6. Especifique la frase de paso de cifrado de la copia de seguridad.

Atención: Registre la frase de paso de cifrado. La frase de paso es necesaria para restaurar la copia de seguridad en esta u otra instancia de XClarity Administrator. Si olvida la frase de paso, no existe manera de recuperarla.

Paso 7. Haga clic en **Crear copia de seguridad** para crear una copia de seguridad de los datos y valores de inmediato, o bien haga clic en **Programación** para programar esta copia de seguridad para que se ejecute posteriormente.

Atención: Si elige crear una copia de seguridad inmediatamente, no cierre ni actualice la pestaña del navegador web o la ventana antes de que finalice el proceso. De lo contrario, es posible que se genere la copia de seguridad.

Generar la copia de seguridad puede tardar varios minutos. Una barra de progreso muestra el estado del trabajo.

Si elige crear la copia de seguridad en una carpeta remota compartida, puede supervisar el progreso desde la página trabajos (consulte Supervisión de trabajos).

Si se programa una copia de seguridad, se apaga el servidor de gestión temporalmente durante el proceso de copia de seguridad. Una vez que conecte el servidor de gestión, puede supervisar el estado del proceso de copia de seguridad en la página trabajos.

Paso 8. Inicie sesión en XClarity Administrator para continuar la gestión de los dispositivos.

Después de finalizar

En la página de Crear copia de seguridad y restaurar datos, puede realizar las siguientes acciones:

- Para copiar XClarity Administrator Copias de seguridad hacia o desde un remote share, haga clic en el icono **Copia de seguridad** ().
- Para eliminar copias de seguridad seleccionadas desde el repositorio local o remote shares que ya no se necesitan, haga clic en el icono **Eliminar copia de seguridad** ().
- Restaure los datos del sistema y los valores para este servidor de gestión (consulte Restauración de Lenovo XClarity Administrator).
- Importe o exporte las copias de seguridad del sistema local al hacer clic en el icono **Importar copia de seguridad** () o el icono **Exportar copia de seguridad** (), respectivamente.
- Inserte la copia de seguridad seleccionada en otra instancia de XClarity Administrator (consulte Migración de datos y de configuración del sistema a otra instancia de XClarity Administrator).

Restauración de Lenovo XClarity Administrator

Puede utilizar datos la copia de seguridad de datos y valores para restaurar Lenovo XClarity Administrator a un estado anterior.

Antes de empezar

Atención: Asegúrese de notificar a todos los usuarios activos antes de iniciar el proceso de copia de seguridad. XClarity Administrator está inactivo durante el procedimiento para evitar la modificación de datos. Por lo tanto, no se puede acceder a XClarity Administrator mientras se está ejecutando el proceso de copia de seguridad.

Descargue el certificado de la entidad de certificación desde el dispositivo virtual de XClarity Administrator e importe el certificado al navegador web (consulte Importación del certificado de la Entidad de certificación en un navegador web).

Asegúrese de que todos los trabajos en ejecución estén completos y que no hay ningún trabajo pendiente.

Solo es posible restaurar una copia de seguridad a la misma versión de XClarity Administrator que se utilizó para crear dicha copia de seguridad.

Acerca de esta tarea

Atención:

- Se perderán todos los cambios hechos posteriormente a la fecha de creación de la copia de seguridad.
- Para restaurar datos, el dispositivo virtual se restablece a su estado original. Antes de restaurar los datos de la copia de seguridad, se eliminan todos los valores actuales, inventarios de dispositivos y archivos (imágenes de sistema operativo, actualizaciones de firmware y controladores de dispositivo de SO). Los datos y valores de la copia de seguridad no se mezclan con los datos actuales y valores del dispositivo virtual. Si no desea restaurar el inventario del dispositivo de restauración, las imágenes de sistema operativo, las actualizaciones de firmware y los controladores de dispositivos de SO, solo estarán presentes los datos predeterminados de XClarity Administrator después de que se complete la operación de restauración.

La restauración de una copia de seguridad no elimina las copias de seguridad en la instancia de XClarity Administrator.

Restaurar una copia de seguridad no cambia los datos o la configuración de los dispositivos gestionados. Por ejemplo, si anula la gestión de un dispositivo y, a continuación, restaura una copia de seguridad anterior cuando el dispositivo era gestionado por XClarity Administrator, es posible que tenga problemas de conectividad con el dispositivo, una vez completada la operación de restauración. Asimismo, si gestiona un dispositivo y, a continuación, restaura una copia de seguridad anterior cuando el dispositivo aún no es gestionado, es posible que deba modificar manualmente la configuración del dispositivo para deshacer el estado gestionado o utilizar la opción **Forzar** al intentar gestionarlo en XClarity Administrator nuevamente.

Procedimiento

Lleve a cabo los pasos siguientes para restaurar XClarity Administrator.

Paso 1. Desde la barra de menús de XClarity Administrator, haga clic en **Administración → Crear copia de seguridad y restaurar datos**. Se muestra la página de Crear copia de seguridad y restaurar datos.

Paso 2. Si se exportó el paquete de copia de seguridad a su sistema local y lo elimina del XClarity Administrator, lleve a cabo los pasos siguientes.

a. Desde la página de Copia de seguridad y restauración, haga clic en el icono **Importar copia de seguridad** () para mostrar el cuadro de diálogo Importar copia de seguridad.

b. Haga clic en **Examinar** para buscar la copia de seguridad que exportó desde una instancia de XClarity Administrator.

c. Haga clic en **Importar** para cargar la copia de seguridad en XClarity Administrator.

La importación de la copia de seguridad puede tardar varios minutos. Una barra de progreso muestra el estado del trabajo.

Atención: Si cierra o actualiza la pestaña del navegador web o la ventana antes de que finalice la carga, es posible que falle el proceso.

d. Una vez que se complete la importación, especifique la frase de paso de cifrado para la copia de seguridad.

Nota: Si no tiene la frase de paso de cifrado, debe crear una nueva copia de seguridad del XClarity Administrator origen (consulte Copia de seguridad de Lenovo XClarity Administrator).

Paso 3. Seleccione la copia de seguridad a restaurar y, a continuación, haga clic en el icono **Restaurar copia de seguridad** (). Se muestra el diálogo Restaurar datos.

Paso 4. Especifique la frase de paso de cifrado de la copia de seguridad.

Paso 5. Haga clic en **Confirmar**.

Paso 6. En el cuadro de diálogo Confirmar restauración de datos, asegúrese de que la información en el cuadro de diálogo sea correcta.

Paso 7. En el cuadro de diálogo Opciones de restauración, puede escoger de forma opcional imágenes de sistema operativo, actualizaciones de firmware, controladores de dispositivos de SO, valores de red y el inventario de dispositivos.

Atención: Asegúrese de leer atentamente todas las advertencias que aparezcan en este cuadro de diálogo.

Paso 8. Haga clic en **Confirmar** para comenzar la restauración de datos.

La restauración de los datos y de la configuración puede tardar varios minutos. Una barra de progreso muestra el estado del trabajo.

Una vez completado el proceso de restauración, se redirigirá a la página de inicio de sesión.

Atención: Si cierra o actualiza la pestaña del navegador web o la ventana antes de que finalice el proceso, es posible que no se pueda cargar el paquete.

Paso 9. Inicie sesión en XClarity Administrator para continuar la gestión de los dispositivos.

Migración de datos y de configuración del sistema a otra instancia de XClarity Administrator

Puede emigrar los datos de sistema y de valores de la copia de seguridad un nuevo Lenovo XClarity Administrator que se encuentre en la red misma o en una red distinta.

Antes de empezar

El servidor de gestión de destino debe ser una *nueva* instancia de XClarity Administrator en la misma versión que el servidor de gestión que se usó para crear el respaldo y debe estar en el Asistente de configuración inicial, sin pasos completados. Para obtener más información, consulte Instalación y configuración de XClarity Administrator en la XClarity Administrator documentación en línea.

Asegúrese de notificar a todos los usuarios activos antes de iniciar el proceso de copia de seguridad. XClarity Administrator está inactivo durante el procedimiento para evitar la modificación de datos. Por lo tanto, no se puede acceder a XClarity Administrator mientras se está ejecutando el proceso de copia de seguridad.

Descargue el certificado de la entidad de certificación desde el XClarity Administrator e importe el certificado al navegador web (consulte Gestión del espacio en el disco duro en la documentación en línea de XClarity Administrator).

Las copias de seguridad en el repositorio de copia de seguridad del servidor de gestión de origen no se migren al servidor de gestión de destino. Antes de migrar los datos y valores, exporte cualquier copia de seguridad que necesite en su sistema local.

Acerca de esta tarea

Los cambios realizados al servidor de gestión de origen después de la copia de seguridad no se migran al servidor de gestión de destino.

Restaurar una copia de seguridad no cambia los datos o la configuración de los dispositivos gestionados. Por ejemplo, si anula la gestión de un dispositivo y, a continuación, restaura una copia de seguridad anterior cuando el dispositivo era gestionado por XClarity Administrator, es posible que tenga problemas de conectividad con el dispositivo, una vez completada la operación de restauración. Asimismo, si gestiona un dispositivo y, a continuación, restaura una copia de seguridad anterior cuando el dispositivo aún no es gestionado, es posible que deba modificar manualmente la configuración del dispositivo para deshacer el estado gestionado o utilizar la opción **Forzar** al intentar gestionarlo en XClarity Administrator nuevamente.

Notas: Cuando XClarity Administrator se ejecuta como un contenedor, otro contenedor puede utilizar los volúmenes creados en el host para un contenedor como volúmenes. Una vez que los volúmenes se enlazan al nuevo contenedor (de destino), ya no se pueden utilizar en el contenedor inicial (de origen).

1. Configuración del archivo `docker-compose.yml` que el contenedor de destino utilice la misma dirección IP y nombre de contenedor que el contenedor de origen.
2. Detenga el contenedor de origen mediante el siguiente comando.
   ```
   docker-compose -p ${CONTAINER_NAME} down
   ```
3. Inicie el contenedor de destino mediante el siguiente comando, donde <*env_filename*> se encuentra el nombre del archivo de variables de entorno. Cuando se inicia el contenedor de destino, los volúmenes

se enlazan al contenedor XClarity Administrator de destino y XClarity Administrator utiliza los datos del sistema y los valores de dichos volúmenes.
COMPOSE_HTTP_TIMEOUT=300 `docker-compose -p ${CONTAINER_NAME} --env-file <ENV_FILENAME> up -d`

Procedimiento

Lleve a cabo los pasos siguientes para restaurar XClarity Administrator.

Paso 1. Si el XClarity Administrator de origen y de destino están en la misma red, complete los pasos siguientes.

a. Desde la barra de menús de XClarity Administrator, haga clic en **Administración → Crear copia de seguridad y restaurar datos**. Se muestra la página de Crear copia de seguridad y restaurar datos.

b. Haga clic en el icono **Insertar copia de seguridad** () para mostrar el cuadro de diálogo Insertar datos.

c. Especifique la dirección IP actual del destino del XClarity Administrator.

d. Haga clic en **Continuar** para cargar la copia de seguridad en el destino XClarity Administrator.

Generar la copia de seguridad puede tardar varios minutos. Una barra de progreso muestra el estado del trabajo.

Atención: Si cierra o actualiza la pestaña del navegador web o la ventana antes de que finalice la carga, es posible que no se pueda cargar el paquete.

Paso 2. Si el XClarity Administrator de origen y de destino *no están* en la misma red, complete los pasos siguientes.

a. Desde la barra de menús del XClarity Administrator de origen, haga clic en **Administración → Crear copia de seguridad y restaurar datos**. En la página Crear copia de seguridad y restaurar datos, haga clic en el icono **Exportar copia de seguridad** () para exportar la copia de seguridad en el sistema local.

La exportación de la copia de seguridad puede tardar varios minutos.

b. Copiar la copia de seguridad exportada desde el servidor de gestión de origen a un sistema en la misma red que el servidor de gestión de destino.

c. Desde la página del asistente en el XClarity Administrator de destino, haga clic en el icono **Importar copia de seguridad** () para mostrar el cuadro de diálogo Importar datos y valores.

d. Haga clic en **Examinar** para buscar la copia de seguridad que exportó desde el XClarity Administrator de origen.

e. Haga clic en **Cargar** para importar la copia de seguridad en el destino XClarity Administrator.

La importación de la copia de seguridad puede tardar varios minutos. Una barra de progreso muestra el estado del trabajo.

Atención: Si cierra o actualiza la pestaña del navegador web o la ventana antes de que finalice la carga, es posible que falle el proceso.

Paso 3. Una vez que se complete la importación, especifique la frase de paso de cifrado para la copia de seguridad.

Nota: Si no tiene la frase de paso de cifrado, debe crear una nueva copia de seguridad del XClarity Administrator origen (consulte Copia de seguridad de Lenovo XClarity Administrator.

Paso 4. En el cuadro de diálogo Confirmar restauración de datos, asegúrese de que toda la información sea correcta.

Paso 5. Haga clic en **Confirmar** para comenzar a cargar los datos del sistema y los valores.

Paso 6. En el cuadro de diálogo Opciones de restauración, puede escoger de forma opcional imágenes de sistema operativo, actualizaciones de firmware, controladores de dispositivos de SO, valores de red y el inventario de dispositivos.

Atención: Asegúrese de leer atentamente todas las advertencias que aparezcan en este cuadro de diálogo.

Paso 7. Si elige importar los valores de red o del inventario de dispositivos, apague el servidor de gestión fuente del XClarity Administrator fuente al hacer clic en **Administración → Apagar servidor de gestión → Apagar**.

Confirme que el dispositivo virtual fuente se apagó antes de continuar

Paso 8. En el XClarity Administrator de destino , haga clic en **Confirmar** para comenzar a cargar los datos y valores del paquete.

Si elige importar valores de red, una vez completada la migración de las direcciones IP del XClarity Administrator fuente, se reasignará al XClarity Administrator de destino.

Atención: Si el XClarity Administrator fuente utiliza DHCP, debe enlazar la dirección MAC de XClarity Administrator de destino para la dirección de IP de XClarity Administrator fuente correspondiente en el servidor DHCP. Espere al menos 15 minutos después de que el servidor DHCP se modifique antes de continuar.

Paso 9. Espere a que se complete la barra de progreso de Carga de datos y valores de paquete.

Una vez completado el proceso de migración de datos, se redirigirá a la página de inicio de sesión.

Atención: Si cierra o actualiza la pestaña del navegador web o la ventana antes de que finalice la carga, es posible que falle el proceso.

Paso 10. Inicie sesión en el XClarity Administrator objetivo para continuar la gestión de los dispositivos.

Gestión del espacio en el disco duro

Para gestionar la cantidad de espacio en disco que usa Lenovo XClarity Administrator, mueva grandes archivos de datos que no se necesitan inmediatamente a un remote share o elimine recursos que ya no son necesarios.

Acerca de esta tarea

Para determinar la cantidad de espacio en el disco usado actualmente, haga clic en **Panel** en la barra de menú de XClarity Administrator. El uso de espacio en disco en el repositorio y remote shares se lista en la sección Actividad de XClarity Administrator.

Procedimiento

Lleve a cabo uno o más de los pasos siguientes para liberar espacio de disco moviendo los archivos a un recurso compartido remoto y eliminando los recursos innecesarios.

- **Eliminar recursos innecesarios**

  Puede eliminar rápidamente los archivos del repositorio local que ya no se necesitan siguiendo los pasos que se indican a continuación.

1. En la barra de menús de XClarity Administrator, haga clic en **Administración → Limpieza de disco** para mostrar la página Limpieza de disco.
2. Seleccione los archivos que desea eliminar. El encabezado de la sección identifica la cantidad de espacio que se liberará al eliminar los archivos.
   - **Archivos asociados al sistema operativo**

     Puede eliminar las imágenes del SO, los archivos de opciones de arranque y los archivos de software.
   - **Actualizaciones de firmware**

     Puede eliminar los archivos de carga útil para todos los controladores de dispositivos del SO que están asociados con UpdateXpress System Packs (UXSP) y los controladores de dispositivos individuales con el estado Descargado.

     Se puede eliminar archivos de carga útil para actualizaciones de firmware individuales con estado Descargado que no se usan en una política de cumplimiento de firmware.

     Puede eliminar los archivos de carga para actualizaciones de servidor de gestión que están en estado Descargado.

     Nota: Cuando el repositorio de actualizaciones de firmware está ubicado en una unidad compartida remota, no puede utilizar la función de limpieza del disco para eliminar actualizaciones de firmware individuales y UXSP.
   - **Archivo de datos del servicio**

     Cuando se produce un suceso de servicio en un dispositivo, se recopilan automáticamente los datos del servicio para dicho dispositivo. Se capturan automáticamente datos de servicio del servidor de gestión cada vez que se produce una excepción en XClarity Administrator. Se recomienda eliminar periódicamente estos archivos si XClarity Administrator y los dispositivos gestionados se están ejecutando sin problemas.

     Cuando las actualizaciones de servidor de gestión se aplican correctamente, archivos los de actualización se extraen automáticamente del repositorio.
3. Haga clic en **Eliminar selección**.
4. Revise la lista de los archivos que ha seleccionado y haga clic en **Eliminar**.

- **Mover paquetes de actualización de firmware a un repositorio remoto**

  De forma predeterminada, Lenovo XClarity Administrator utiliza un repositorio local (interno) para almacenar actualizaciones de firmware. Puede liberar espacio en el disco que está disponible para el repositorio local de XClarity Administrator usando una unidad compartida remota sobre sistema de archivos SSH (SSHFS) montada como repositorio remoto. A continuación, puede utilizar los archivos de actualización de firmware directamente desde el repositorio remoto para mantener el cumplimiento del firmware en sus dispositivos. Para obtener más información, consulte Uso de un repositorio remoto para actualizaciones de firmware.

  Cuando cambie la ubicación de repositorio de actualizaciones de firmware, puede elegir copiar todas las actualizaciones de firmware desde el repositorio original en el nuevo repositorio.

  Los archivos de actualización de firmware del repositorio original *no* se limpian automáticamente después de cambiar de ubicación.

  Consejo: el repositorio de actualizaciones remotas se puede compartir en varios servidores de gestión de XClarity Administrator.

  Para mover las actualizaciones de firmware a un repositorio remoto de actualizaciones de firmware, realice los pasos siguientes.

1. Añada un recurso compartido remoto a XClarity Administrator (consulte Gestión de remote shares).
2. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Actualizaciones de firmware: Repositorio** . Se muestra la página del repositorio de actualizaciones de firmware.
3. Haga clic en **Todas las acciones → Cambiar ubicación de repositorio** para mostrar el cuadro de diálogo Ubicación de repositorio de intercambio.
4. Seleccione la carpeta compartida remota que acaba de crear en la lista desplegable **Ubicación de repositorio**.
5. Seleccione **Copiar paquetes de actualización desde el repositorio actual en el nuevo repositorio** para copiar los archivos de actualización de firmware en la nueva ubicación de repositorio antes de cambiar la ubicación de repositorio.
6. Haga clic en **Aceptar**.

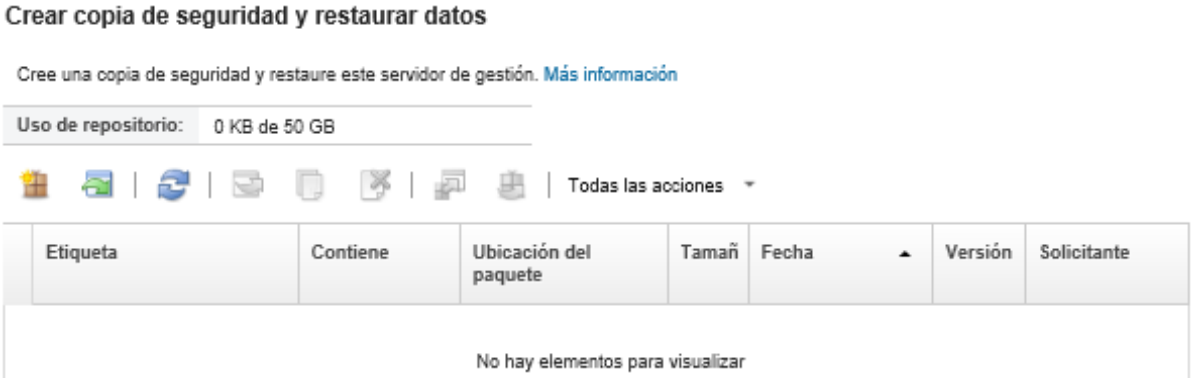
   Se crea un trabajo para copiar los paquetes de actualización de firmware en el nuevo repositorio. Puede supervisar el progreso del trabajo haciendo clic en **Supervisión → Trabajos** en la barra de menús de XClarity Administrator.
7. Limpie los archivos de actualización de firmware en el repositorio local.
   a. Cambie la ubicación al repositorio local haciendo clic en **Todas las acciones → Cambiar ubicación de repositorio**, seleccione el **Repositorio local** para la ubicación de repositorio y, a continuación, haga clic en **Aceptar**.
   b. Haga clic en la pestaña **Actualizaciones individuales**, haga clic en la casilla de verificación seleccionar todo en la tabla para seleccionar todas las actualizaciones de firmware y, a continuación, haga clic en el icono **Eliminar paquetes de actualización completos** ()
   c. Haga clic en la pestaña **UpdateXpress System Pack (UXSP)**, haga clic en la casilla de verificación Seleccionar todo en la tabla para seleccionar todos los UXSP y, a continuación, haga clic en el icono **Eliminar UXSP y políticas asociadas** ()
   d. Cambie la ubicación al repositorio de vuelta al repositorio remoto haciendo clic en **Todas las acciones → Cambiar ubicación de repositorio**, seleccione el nuevo repositorio remoto para la ubicación de repositorio y, a continuación, haga clic en **Aceptar**.

- **Mueva las copias de seguridad de XClarity Administrator a un recurso compartido remoto**

  Para liberar espacio de disco que se encuentra disponible para el repositorio local de XClarity Administrator, mueva copias de seguridad de XClarity Administrator a un remote share. Sin embargo, no puede utilizar los archivos directamente en un remote share. Para utilizar los archivos, debe moverlos de vuelta al repositorio local de XClarity Administrator. Para obtener más información sobre los requisitos, consulte remote shares, consulte Gestión de remote shares.

  Importante: Se recomienda descargar copias de seguridad en su sistema local o copiar copias de seguridad a un recurso compartido remoto antes de eliminar las copias de seguridad en XClarity Administrator.

1. Desde la barra de menús de XClarity Administrator, haga clic en **Administración → Crear copia de seguridad y restaurar datos** para mostrar la página Crear copia de seguridad y restaurar datos.



   La columna **Ubicación de paquete** identifica si la copia de seguridad está almacenada localmente en el repositorio local de XClarity Administrator o en un remote share.

2. Seleccione la copia de seguridad y haga clic en el icono **Copiar copia de seguridad** ( ) para mostrar el cuadro de diálogo Copiar copia de seguridad.
3. Elija la remote share para almacenar la copia de seguridad.
4. Haga clic en **Copiar**.
5. Supervise el progreso de la copia en la página Trabajos. Cuando la copia esté completa, vuelva a seleccionar la copia de seguridad y haga clic en el icono **Eliminar copia de seguridad** ( ) para mostrar el cuadro de diálogo Eliminar copia de seguridad.
6. Seleccione “Local” para conocer la ubicación.
7. Haga clic en **Eliminar**.

Gestión de remote shares

Puede montar remote shares y luego mover archivos de datos grandes, como copias de seguridad y actualizaciones de firmware de Lenovo XClarity Administrator, desde el repositorio local hasta la unidad compartida remota para gestionar el espacio en disco disponible para el servidor de gestión.

Antes de empezar

Cuando se ejecuta XClarity Administrator como un contenedor, los usos compartidos remotos se montan en el contenedor utilizando el archivo yml durante la instalación (consulte Instalación de XClarity Administrator en entornos con base VMware ESXi en la documentación en línea de XClarity Administrator).

Cuando se ejecuta XClarity Administrator como un dispositivo virtual, debe tener la autoridad **lxc-supervisor** para montar o desmontar un remote share.

Asegúrese de tener una red estable y de alta velocidad entre el servidor de archivo y XClarity Administrator.

Los usos compartidos remotos no se admiten cuando se ejecuta XClarity Administrator como un contenedor.

Acerca de esta tarea

Debe utilizar acciones remotas separadas para almacenar copias de seguridad y actualizaciones de firmware de XClarity Administrator.

No puede utilizar los archivos de copia de seguridad de XClarity Administrator directamente desde el recurso compartido remoto. Para utilizar los archivos de copia de seguridad, debe moverlos de vuelta al repositorio local.

Actualmente, solo se admite SSHFS.

Procedimiento

Para añadir un remote share cuando ejecute XClarity Administrator como un dispositivo virtual, lleve a cabo los siguientes pasos.

1. En la barra de menús de XClarity Administrator, haga clic en **Administración → Recurso compartido remoto**. Se muestra la página Recurso compartido remoto.
2. Haga clic en el icono **Crear** ( ) para crear un recurso compartido remoto. Se muestra el cuadro de diálogo Crear recurso compartido remoto.
3. Especifique la dirección IP del servidor de archivos que aloja las remote share.
4. Especifique las credenciales almacenadas a utilizar para acceder a la remote share.

   Consejo: para crear una credencial almacenada, consulte Gestión de credenciales almacenadas.
5. Especifique el punto de montaje (directorio local) en el servidor de gestión que se utilizará para montar el recurso compartido remoto.

   Importante: La ruta debe comenzar con “/mnt”.
6. Especifique la ruta compartida (ruta de servidor remota) a montar como el recurso compartido remoto en el servidor de gestión.
7. Haga clic en **Crear**.

Después de finalizar

- Desmonte el recurso compartido remoto seleccionando el recurso compartido remoto y haciendo clic en el icono **Eliminar** ( ).
- Mueva los archivos de copia de seguridad de XClarity Administrator desde y hacia un recurso compartido remoto (consulte Gestión del espacio en el disco duro).
- Configure XClarity Administrator para que use un recurso compartido remoto como repositorio de actualizaciones de firmware (consulte Uso de un repositorio remoto para actualizaciones de firmware).

Cambiar el idioma de la interfaz de usuario

Puede cambiar el idioma de la interfaz de usuario después iniciar sesión.

Procedimiento

Desde la barra de título de Lenovo XClarity Administrator, haga clic en el menú de acciones de usuario (ADMIN_USER) y haga clic en **Cambiar idioma**. Seleccione el idioma a visualizar y, a continuación, haga clic en **Cerrar**.

Nota: El sistema de ayuda se muestra en el mismo idioma que se establece para la interfaz de usuario.

Apagar XClarity Administrator

Cuando se apaga Lenovo XClarity Administrator, se pierde la conectividad con Lenovo XClarity Administrator.

Antes de empezar

Debe tener autoridad de **lxc-supervisor** o **lxc-admin** para apagar un dispositivo virtual XClarity Administrator.

Asegúrese de que no hay trabajos en ejecución actualmente. Cualquier trabajo que esté en ejecución en la actualidad se cancela durante el proceso de apagado. Para ver el registro de trabajos, consulte Supervisión de trabajos.

Procedimiento

Lleve a cabo los pasos siguientes para apagar Lenovo XClarity Administrator

- **Contenedores**

  Ejecute los siguientes comandos para detener el contenedor.
  ```
  docker-compose -p ${CONTAINER_NAME} down
  ```
- **Dispositivos virtuales**
  1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Administración → Apagar servidor de gestión**.

     Se muestra un cuadro de diálogo de confirmación con una lista de los trabajos que están actualmente en ejecución. Cuando apaga XClarity Administrator, los trabajos se cancelan.
  2. Haga clic en **Apagar**.

Después de finalizar

Para reiniciar XClarity Administrator después de una operación de apagado, consulte Reiniciar XClarity Administrator.

Reiniciar XClarity Administrator

Puede reiniciar Lenovo XClarity Administrator desde la interfaz web o desde el hipervisor después de una operación de apagado.

Antes de empezar

Debe tener autoridad de **lxc-supervisor** o **lxc-admin** para reiniciar XClarity Administrator.

Asegúrese de que no hay trabajos en ejecución actualmente. Cualquier trabajo que esté en ejecución en la actualidad se cancela durante el proceso de reinicio. Para ver el registro de trabajos, consulte Supervisión de trabajos.

Acerca de esta tarea

Existen ciertas situaciones que requieren un reinicio de Lenovo XClarity Administrator:
- Al volver a generar un certificado de servidor
- Al cargar un nuevo certificado de servidor

Procedimiento

Lleve a cabo uno de los siguientes procedimientos para reiniciar Lenovo XClarity Administrator.

- **Contenedores**

Ejecute los siguientes comandos para detener y luego iniciar el contenedor, donde <*env_filename*> es el nombre del archivo de variables del entorno.

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

- **Dispositivos virtuales**
  - Reinicie Lenovo XClarity Administrator desde la interfaz web:
    1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Administración → Apagar servidor de gestión**.

       Se muestra un cuadro de diálogo de confirmación con una lista de los trabajos que están actualmente en ejecución. Cuando reinicia Lenovo XClarity Administrator, los trabajos se cancelan.
    2. Haga clic en **Reiniciar**.

       Cuando se apaga Lenovo XClarity Administrator, se pierde la conectividad con Lenovo XClarity Administrator.
    3. Espere unos minutos para que Lenovo XClarity Administrator se reinicie y, a continuación, vuelva a iniciar sesión.
  - Reinicie Lenovo XClarity Administrator desde el hipervisor después de una operación de apagado:.
    - Microsoft Hyper-V
      1. En el Panel de Server Manager, haga clic en **Hyper-V**.
      2. Haga clic en con el botón derecho del ratón en el servidor y haga clic en **Administrador de Hyper-V**.
      3. Haga clic en con el botón derecho en la máquina virtual y, a continuación, haga clic en **Iniciar**. Cuando se inicia la máquina virtual, se enumeran las direcciones IPv4 e IPv6 para cada interfaz, tal como se muestra en el ejemplo siguiente.

         El puerto de gestión eth0 de XClarity Administrator usa una dirección IP DHCP de forma predeterminada. Al final del proceso de arranque de XClarity Administrator, puede elegir establecer una dirección IP estática para el puerto de gestión eth0 al establecer 1 cuando se le solicite, tal como se muestra en el ejemplo siguiente. El mensaje emergente está disponible por 150 segundos, hasta que se muestre el indicador de inicio de sesión. Para continuar con la ventana emergente de inicio de sesión sin demora, escriba x en el indicador.

         Importante:

         - Al modificar los valores de dirección IP estática, tiene un máximo de 60 segundos para especificar los valores nuevos. Asegúrese de tener a mano la información de IP necesaria antes de continuar.
           - Para valores de IPv4, debe tener la dirección IP, la máscara de subred y la dirección IP de la puerta de enlace
           - Para valores de IPv6, debe tener la dirección IP y la longitud de prefijo
         - Si no está utilizando un servidor DHCP, puede utilizar un archivo de configuración para especificar los valores IP del puerto de gestión eth0 de XClarity Administrator que desea utilizar para acceder a XClarity Administrator. Para obtener más información, consulte la sección “Qué debe hacer a continuación”, más adelante.
         - Si se cambia los valores de la dirección IP de la consola, XClarity Administrator se reinicia para aplicar los valores nuevos.
         - No se requiere ninguna acción para iniciar sesión. Ignore el mensaje de inicio de sesión de la consola. La interfaz de la consola no es para el uso del cliente.

- Puede que aparezca el mensaje `TCP: eth0: controlador tiene e sospecha de implementación, puede estar en peligro el rendimiento de TCP` en la consola de. El rendimiento de la máquina virtual no se ven afectados, por lo que puede ignorar esta advertencia.

Atención: Si cambia la dirección IP del puerto de gestión de XClarity Administrator después de gestionar dispositivos, es posible que cause que los dispositivos entren en estado fuera de línea en XClarity Administrator. Si elige cambiar la dirección IP después de que XClarity Administrator esté actualizado y funcionando, asegúrese de que se anule la gestión de todos los dispositivos antes de cambiar la dirección IP.

```
----------------------------------------
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
  … …
```

4. Inicie sesión en Lenovo XClarity Administrator (consulte Inicio de sesión en XClarity Administrator).

– VMware ESXi

1. Conéctese al host a través de VMware vSphere Client.
2. Haga clic en con el botón derecho del ratón en la máquina virtual y, a continuación, haga clic en **Alimentación → Encender**.
3. Haga clic en la pestaña **Consola**. Cuando se inicia la máquina virtual, se enumeran las direcciones IPv4 e IPv6 para cada interfaz, tal como se muestra en el ejemplo siguiente.

   El puerto de gestión eth0 de XClarity Administrator usa una dirección IP DHCP de forma predeterminada. Al final del proceso de arranque de XClarity Administrator, puede elegir establecer una dirección IP estática para el puerto de gestión eth0 al establecer 1 cuando se le solicite, tal como se muestra en el ejemplo siguiente. El mensaje emergente está disponible por 150 segundos, hasta que se muestre el indicador de inicio de sesión. Para continuar con la ventana emergente de inicio de sesión sin demora, escriba x en el indicador.

   Importante:

   - Al modificar los valores de dirección IP estática, tiene un máximo de 60 segundos para especificar los valores nuevos. Asegúrese de tener a mano la información de IP necesaria antes de continuar.
     – Para valores de IPv4, debe tener la dirección IP, la máscara de subred y la dirección IP de la puerta de enlace
     – Para valores de IPv6, debe tener la dirección IP y la longitud de prefijo
   - Si no está utilizando un servidor DHCP, puede utilizar un archivo de configuración para especificar los valores IP del puerto de gestión eth0 de XClarity Administrator que desea

utilizar para acceder a XClarity Administrator. Para obtener más información, consulte la sección “Qué debe hacer a continuación”, más adelante.

- Si se cambia los valores de la dirección IP de la consola, XClarity Administrator se reinicia para aplicar los valores nuevos.
- No se requiere ninguna acción para iniciar sesión. Ignore el mensaje de inicio de sesión de la consola. La interfaz de la consola no es para el uso del cliente.
- Puede que aparezca el mensaje `TCP: eth0: controlador tiene e sospecha de implementación, puede estar en peligro el rendimiento de TCP` en la consola de. El rendimiento de la máquina virtual no se ven afectados, por lo que puede ignorar esta advertencia.

Atención: Si cambia la dirección IP del puerto de gestión de XClarity Administrator después de gestionar dispositivos, es posible que cause que los dispositivos entren en estado fuera de línea en XClarity Administrator. Si elige cambiar la dirección IP después de que XClarity Administrator esté actualizado y funcionando, asegúrese de que se anule la gestión de todos los dispositivos antes de cambiar la dirección IP.

```
----------------------------------------
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
  … …
```

4. Inicie sesión en Lenovo XClarity Administrator (consulte Inicio de sesión en XClarity Administrator).

Después de finalizar

Cuando Lenovo XClarity Administrator se reinicia, recopila el inventario para cada dispositivo gestionado. Espere entre 30 y 45 minutos, dependiendo del número de dispositivos gestionados, antes de intentar realizar actualizaciones de firmware, despliegues del patrón de configuración o despliegues del sistema operativo.

Capítulo 3. Supervisión de dispositivos y las actividades

Puede supervisar los dispositivos y las actividades mediante los registros de panel, de alertas y de auditoría y los registros de trabajos.

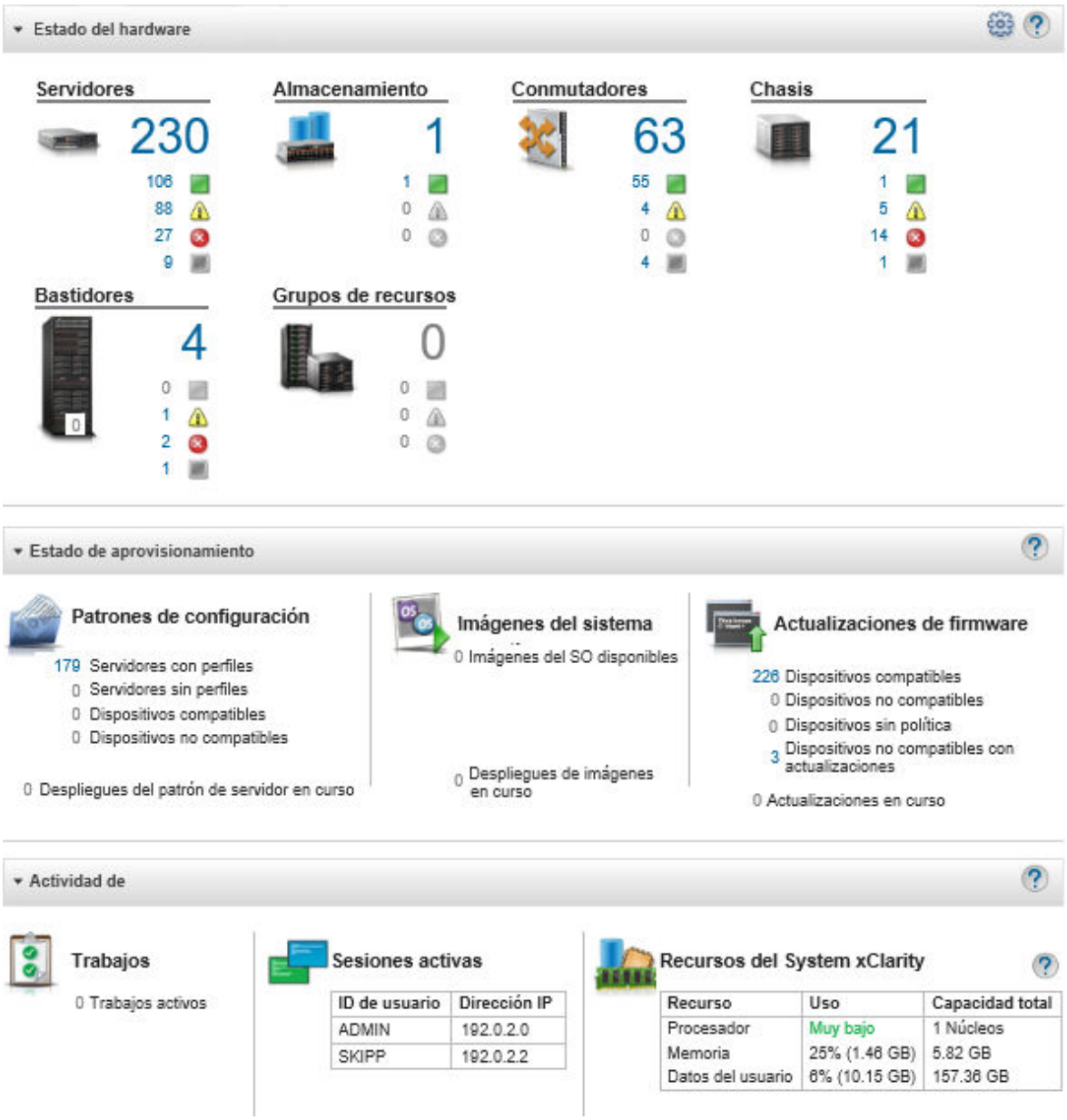
Visualización de un resumen del estado de su entorno

El panel de mandos muestra el estado de todos los dispositivos gestionados, una visión general de todas las tareas relacionadas con el aprovisionamiento, información acerca de los recursos y las actividades de Lenovo XClarity Administrator.

Más información: XClarity Administrator: supervisión

Procedimiento

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Panel**.



Paso 2. Expanda la sección de estado del hardware, estado de aprovisionamiento o actividad del administrador para obtener más información sobre cada una de estas áreas.

Visualización de un resumen del estado de hardware

En el área de estado del hardware se muestra el estado de todos los dispositivos gestionados.

Procedimiento

Para obtener más información acerca de todos los dispositivos de ese tipo, haga clic en el número que aparece debajo del tipo de dispositivo.

Para ver más información únicamente acerca de los dispositivos de este tipo y estado, haga clic en el icono o el número junto a cada icono de estado.

- **Servidores**. Muestra el número total de servidores (nodos de cálculo, servidores de bastidor y servidores de torre) gestionados por XClarity Administrator y el número de servidores con estado normal, de advertencia y crítico. Para obtener más información, consulte el apartado Visualización del estado de un servidor gestionado.
- **Storage**. Muestra el número total de dispositivos de almacenamiento gestionados por XClarity Administrator y el número de dispositivos de almacenamiento con estado normal, de advertencia y crítico. Para obtener más información, consulte el apartado Visualización del estado de los dispositivos de almacenamiento.
- **Conmutadores**. Muestra el número total de conmutadores RackSwitch y Flex System gestionados por XClarity Administrator y el número de conmutadores con estado normal, de advertencia y crítico. Para obtener más información, consulte Visualización del estado de los conmutadores
- **Chasis**. Muestra el número total de chasis de Flex gestionados por XClarity Administrator y el número de chasis de Flex con estado normal, de advertencia y crítico. Para obtener más información, consulte el apartado Visualización del estado de un chasis gestionado.
- **Bastidores**. Muestra el número de bastidores creados en XClarity Administrator y el número de bastidores con dispositivos con estado normal, de advertencia y crítico. Para obtener más información, consulte el apartado Visualización del estado de los dispositivos de un bastidor.
- **Grupos de recursos**. Muestra el número de grupos de recursos que gestionan XClarity Administrator y el número de grupos de recursos con dispositivos que tienen los estados normal, advertencia y crítico como su estado más elevado. Para obtener más información, consulte el apartado Visualización de estado de dispositivos en un grupo de recursos.

Para personalizar los recursos de hardware que se muestran en el panel, haga clic en el icono **Personalizar** ( ). También puede elegir los tipos de dispositivos que desea mostrar u ocultar. También puede elegir si desea agregar servidores en un resumen único, mostrar resúmenes separados para cada tipo de servidor (bastidor y torre, servidores Flex System, ThinkServer y NeXtScale) u omitir tipos específicos de servidores.

Visualización de un resumen del estado de aprovisionamiento

En el área de estado de aprovisionamiento se muestra un resumen de todas las tareas que están asociadas a los dispositivos de aprovisionamiento.

Procedimiento

- **Patrones de configuración**. Muestra detalles sobre el número de servidores que tienen perfiles, lo que incluye las siguientes estadísticas.

Nota: Cuando el servidor de gestión no es compatible con la licencia, todos los valores son 0 (consulte Instalación de licencia de habilitación de funciones completas en la documentación en línea de XClarity Administrator).

- El número de servidores que cumplen con sus perfiles de servidor. Puede hacer clic en el número para mostrar la página Patrones de configuración: perfiles de servidor con una lista de servidores en conformidad con su perfil.
- El número de servidores que no cumplen con sus perfiles de servidor. Puede hacer clic en el número para mostrar la página Patrones de configuración: perfiles de servidor con una lista de servidores que no están en conformidad con su perfil.
- El número de dispositivos para los que se desconoce el estado de conformidad. Puede hacer clic en el número para mostrar la página Patrones de configuración: Perfiles de servidor con una lista de servidores con conformidad desconocida.

  Nota: Se desconoce el estado de conformidad, normalmente después de la implementación parcial de un perfil, cuando Lenovo XClarity Administrator no se recopiló la información de configuración del servidor. Actualice el inventario del servidor o vuelva a visitar la página de detalles del perfil del servidor para forzar la recopilación de la información de configuración del servidor.
- El número de servidores asignados a un perfil de servidor. Puede hacer clic en el número para mostrar la página Patrones de configuración: Perfiles de servidor con una lista de servidores con perfiles.
- El número de servidores no asignados a un perfil de servidor. Puede hacer clic en el número para mostrar la página Patrones de configuración: Patrones de servidor con una lista de patrones de servidor que se pueden desplegar en servidores sin perfil.
- El número de patrones de servidor que actualmente se está desplegando.

Para ver los datos de tendencia para los patrones de configuración, haga clic en **Ver datos de tendencia** (consulte Supervisión de tendencias existentes en el estado de aprovisionamiento).

Para obtener más información sobre los patrones de configuración y los perfiles de servidor, consulte Configuración de servidores mediante el uso de patrones de configuración.

- **Imágenes del sistema operativo**. Muestra los detalles acerca de los despliegues del sistema operativo, incluidas las siguientes estadísticas.

  Nota: Cuando el servidor de gestión no es compatible con la licencia, todos los valores son 0 (consulte Instalación de licencia de habilitación de funciones completas en la documentación en línea de XClarity Administrator).

  - La cantidad de imágenes de SO en el repositorio. Puede hacer clic en el número para mostrar la página desplegar sistemas operativos: gestionar imágenes de SO con una lista de sistemas operativos.
  - El número de implementaciones de SO actuales que están en progreso. Puede hacer clic en el número para mostrar la página desplegar sistemas operativos: implementar imágenes de SO con una lista de dispositivos para los que se está instalando un sistema operativo.
- **Actualizaciones de firmware**. Muestra detalles sobre las actualizaciones de firmware, incluye las siguientes estadísticas.
  - El número de dispositivos conformes. Puede hacer clic en el número para mostrar la página Actualizaciones de firmware: Aplicar/Activar con una lista de los dispositivos conformes.
  - El número de dispositivos no conformes. Puede hacer clic en el número para mostrar la página Actualizaciones de firmware: Aplicar/Activar con una lista de los dispositivos no conformes.
  - El número de dispositivos que no tienen una política asignada de la política de cumplimiento de firmware. Puede hacer clic en el número para mostrar la página Actualizaciones de firmware: Aplicar/Activar con una lista de los dispositivos sin una política de cumplimiento.

En esta página, puede asignarle a cada dispositivo una política de cumplimiento de firmware al seleccionar una política en el menú desplegable de la columna **Política de cumplimiento asignada**.

- El número de dispositivos que no admiten las actualizaciones. Puede hacer clic en el número para mostrar la página Actualizaciones de firmware: Aplicar / Activar con una lista de dispositivos en los que no se admiten las actualizaciones.
- El número de actualizaciones en progreso.
- El número de dispositivos con firmware pendiente. Puede hacer clic en el número para mostrar la página Actualizaciones de firmware: Aplicar / Activar con una lista de dispositivos en los que las actualizaciones tienen la activación pendiente.

Para ver los datos de tendencia para las actualizaciones de firmware, haga clic en **Ver datos de tendencia** (consulte Supervisión de tendencias existentes en el estado de aprovisionamiento).

Para obtener más información sobre las actualizaciones de firmware y las políticas de conformidad, consulte Actualización de firmware en dispositivos gestionados.

Visualización de un resumen de actividad de Lenovo XClarity Administrator

El área de Actividad de XClarity Administrator muestra información sobre trabajos activos, sesiones activas y recursos del sistema en XClarity Administrator.

Procedimiento

- **Trabajos**. Muestra el número de trabajos activos que están en curso en la actualidad. Para obtener más información sobre los trabajos, consulte Supervisión de trabajos.
- **Sesiones activas**. Muestra el Id. de usuario y la dirección IP de cada sesión activa de XClarity Administrator. Para obtener más información sobre los usuario, consulte Gestión de cuentas de usuario.
- **Uso de recursos**. Muestra el uso del procesador, el uso de memoria y la capacidad del disco en el sistema host y los archivos compartidos remotos. Para obtener más información acerca de los recursos de sistema, consulte Supervisión de los recursos del sistema.

Supervisión de los recursos del sistema

Desde la página Panel puede determinar el uso del procesador, así como el uso de la memoria y la capacidad del disco en el sistema host.

Antes de empezar

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
- 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.

Procedimiento

En la barra de menús de Lenovo XClarity Administrator, haga clic en **Panel**.

El uso de recursos del sistema host aparece en la sección Actividad de XClarity Administrator.

Procesador

La medición del uso indica el número de procesos de XClarity Administrator que están accediendo al mismo tiempo a los procesadores del host.

Consejo: en ocasiones, la medición del uso puede subir a Alto o Muy alto. Si el uso permanece en uno de estos niveles durante más de 30 minutos, compruebe el registro de trabajos para ver si hay trabajos con un tiempo de ejecución largo (consulte Supervisión de trabajos).

La medición de la capacidad total indica el número de procesadores que están disponibles en el host.

Memoria

La medición del uso indica la cantidad de memoria que XClarity Administrator está utilizando en la actualidad.

La medición de la capacidad total indica la cantidad total de memoria disponible en el host.

Datos del usuario

La medición del uso indica la cantidad de espacio de disco que XClarity Administrator está utilizando en la actualidad en el sistema de host.

La medida de capacidad total indica la cantidad total de espacio (usado o no usado) que se asigna para datos de usuario, como sistemas operativos y actualizaciones de firmware.

Para obtener más información sobre cómo gestionar el espacio de disco, consulte Gestión del espacio en el disco duro.

Atención: Si los recursos asignados no son suficientes para gestionar la cantidad actual de dispositivos gestionados de alto rendimiento, considere aumentar la asignación de recursos. Para obtener más información acerca de los requisitos de hardware recomendados basadas en el número de dispositivos gestionados en el entorno, consulte Sistemas host compatibles en la documentación en línea de XClarity Administrator.

Supervisión de tendencias existentes en el estado de aprovisionamiento

Lenovo XClarity Administrator recopila periódicamente el estado de aprovisionamiento, incluida la conformidad y los trabajos activos para las actualizaciones de firmware y los patrones de configuración para todos los dispositivos gestionados para que pueda supervisar las tendencias existentes en un período de tiempo.

Acerca de esta tarea

Debe tener autoridad de **lxc_admin** o **lxc-supervisor** para ver datos de tendencias.

Se recopilan los siguientes datos:

- **Actualizaciones de firmware**
  - **Dispositivos en cumplimiento**. El número de dispositivos en cumplimiento con su política de cumplimiento de firmware asignada.
  - **Dispositivos que no están en cumplimiento**. El número de dispositivos que no están en cumplimiento con su política de cumplimiento de firmware asignada.
  - **Dispositivos sin políticas**. Número de dispositivos que no tienen una política asignada de la política de cumplimiento de firmware
  - **Dispositivos no compatibles con actualizaciones**. Número de dispositivos que no admiten las actualizaciones de firmware
  - **Actualizaciones en curso**. Número de dispositivos para los que hay actualizaciones de firmware en curso
- **Patrones de configuración**
  - **Servidores con perfiles**. Número de dispositivos que tienen un perfil de servidor asignado
  - **Servidores sin perfiles**. Número de dispositivos que no tienen un perfil de servidor asignado
  - **Compatible con los servidores**. Número de dispositivos que cumplen con sus perfiles de servidor asignados
  - **No compatible con los servidores**. Número de dispositivos que no cumplen con sus perfiles de servidor asignados

– **Despliegues de patrones de servidor en curso**. Número de dispositivos para los que hay actualizaciones de patrón de configuración en curso

Procedimiento

Lleve a cabo los siguientes pasos para ver las tendencias existentes en el estado de aprovisionamiento.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Panel** para mostrar la página Panel.

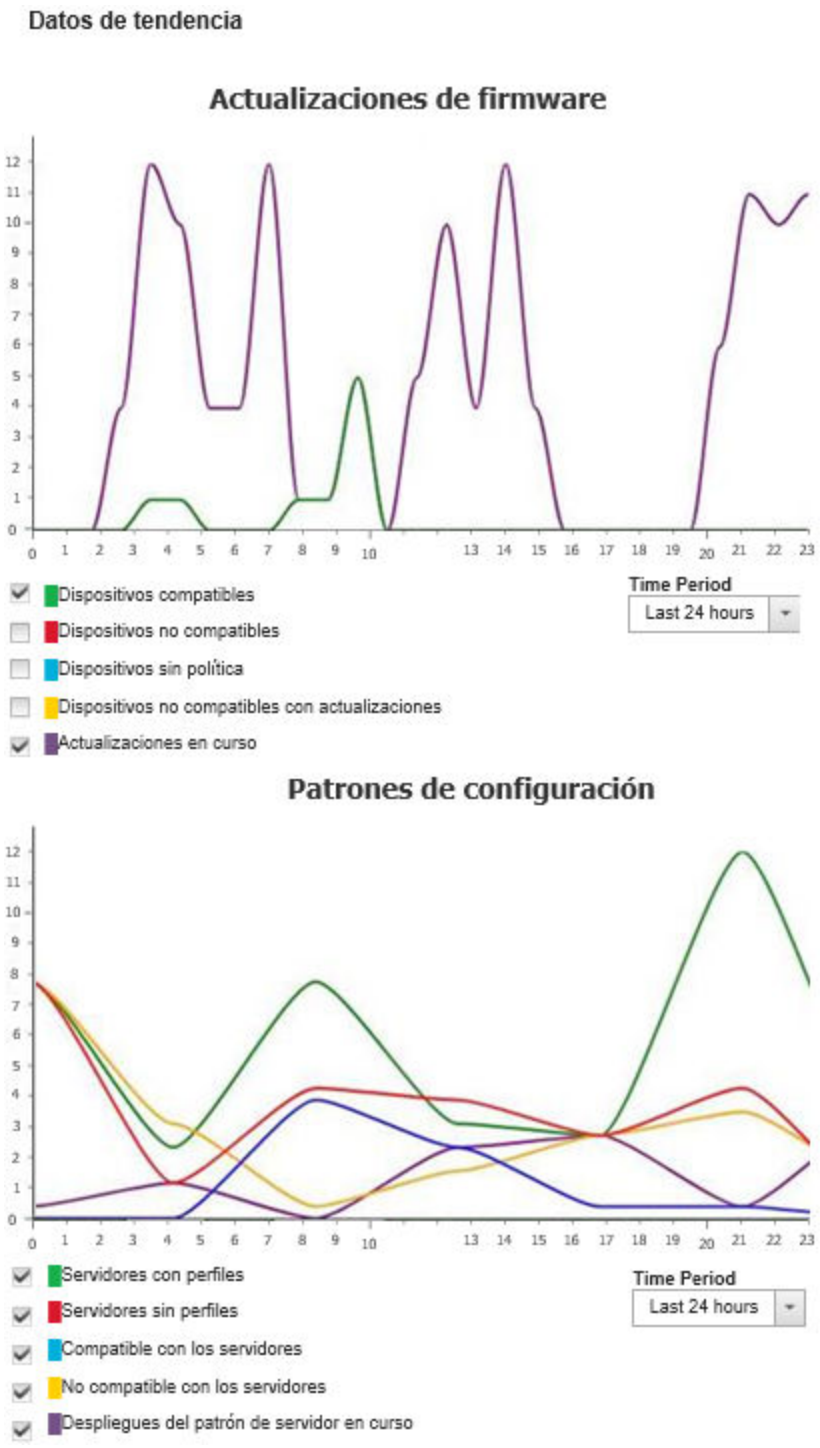
Paso 2. Haga clic en el enlace **Datos de tendencia** para mostrar el cuadro de diálogo Valores de umbral.

Paso 3. Borre o seleccione los datos que desea ver.

Paso 4. Seleccione el período de tiempo que desea ver.

- **24 horas**. Muestra los datos para las últimas 24 horas. Cada punto de datos es un promedio durante un período de 1 hora.
- **1 mes**. Muestra los datos para los últimos 30 días. Cada punto de datos es un promedio durante un período de 24 hora.

Los datos de tendencia se muestran como un gráfico en el período de tiempo seleccionado.



Supervisión de métricas históricas

Lenovo XClarity Administrator recopila periódicamente datos de métricas para dispositivos ThinkSystem y ThinkAgile gestionados, para que pueda analizar el estado actual de su entorno.

Antes de empezar

Solo se admiten las métricas históricas sistema para los servidores ThinkSystem (excepto SR635, SR645, SR655 y SR665).

Solo se admiten SSD en servidores ThinkAgile y ThinkSystem (excepto SR635 y SR655) que ejecutan hardware XCC lanzado después de abril de 2019.

No se admiten controladores SATA incorporados.

Las unidades NVMe deben admitir la especificación de interfaz de gestión NVMe (NVMe-MI).

Acerca de esta tarea

Se recopilan las siguientes métricas.

- **Supervisión de SSD** Esta tarjeta de informe incluye las siguientes estadísticas y gráficos.
  - La cantidad total de SSD en los dispositivos gestionados (en función del alcance).
  - La cantidad de SSD que se analizaron
  - La cantidad de SSD que no son elegibles para análisis
  - Un gráfico circular que muestra la cantidad de dispositivos con SSD que tienen vida restante en un rango específico.
    - Vida restante de <= 10 %. Cantidad de SSD con una vida restante de 10 % o menos
    - Vida restante de 11 % – 50 %. Cantidad de SSD con una vida restante de 11 % – 50 %
    - Vida restante de 51 % – 100 %. Cantidad de SSD con una vida restante de más de 50 %
- **Utilización del sistema** Esta tarjeta de informe incluye las siguientes estadísticas y gráficos.
  - El uso actual del procesador, como porcentaje
  - El uso actual de la memoria, como porcentaje
  - Un gráfico de líneas que muestra el uso del procesador y la memoria a lo largo del tiempo
- **Consumo de energía** Esta tarjeta de informe incluye las siguientes estadísticas y gráficos.
  - La entrada de alimentación total actual de todas las fuentes de alimentación, en vatios
  - Gráfico de línea que muestra la entrada de alimentación total a lo largo del tiempo
- **Temperatura del dispositivo** Esta tarjeta de informe incluye las siguientes estadísticas y gráficos.
  - La temperatura máxima actual del aire de entrada, en Celsius
  - Gráfico de línea que muestra la temperatura máxima a lo largo del tiempo

Puede pasar el mouse sobre cada línea en el gráfico circular, cada punto del gráfico de líneas o sobre el número que se encuentra junto a cada métrica para obtener más información sobre dicha métrica. Se pueden mostrar u ocultar las métricas haciendo clic en el ícono de color en la leyenda. También puede hacer clic en cualquier número vinculado u opción en el icono de **Valores** () que se encuentra en la esquina superior derecha de la tarjeta para ver una lista de todos los dispositivos que tienen métricas que se ajustan a los criterios seleccionados.

Procedimiento

Lleve a cabo los siguientes pasos para ver el diagrama de flujo de una actividad específica.

Paso 1. En la barra de menú de XClarity Administrator, haga clic en **Supervisión → Métricas históricas** para mostrar la página de Métricas históricas con tarjetas de informe para cada tipo de métrica.

Paso 2. Establezca el alcance de todos los dispositivos o de un grupo específico de estos.

Colocación de dispositivos en el modo de mantenimiento

Cuando un dispositivo está en modo de mantenimiento, Lenovo XClarity Administrator excluye todos los sucesos y alertas de ese dispositivo de todas las páginas en las que se muestran sucesos y alertas. Las alertas excluidas se registran de todos modos, pero se ocultan en la vista.

Acerca de esta tarea

Solo se excluyen los sucesos y las alertas que se generaron para un dispositivo mientras el dispositivo está en modo de mantenimiento. Se han generado los sucesos y las alertas antes de colocar el dispositivo en el modo de mantenimiento.

Si se coloca un dispositivo gestionado en mantenimiento y luego de vuelta en funcionamiento, es posible que el inventario de ese dispositivo no se actualice. Si observa anomalías, actualice manualmente el inventario desde la página dispositivo seleccionando el dispositivo y haga clic en **Todas las acciones → Inventario → Actualizar inventario**.

Procedimiento

Lleve a cabo uno de los siguientes pasos para ubicar dispositivos en el modo de mantenimiento.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Administración → Servicio y soporte**. Se abre la página Servicio y soporte.

Paso 2. Haga clic en **Acciones de punto final** en el panel de navegación izquierdo para mostrar la página Acciones de punto final.

Paso 3. Seleccione uno o más dispositivos para poner en modo de mantenimiento.

Paso 4. Haga clic en **Acciones → Mantenimiento** para mostrar el cuadro de diálogo Modo de mantenimiento.

Paso 5. Seleccione la fecha y hora para retirar el dispositivo del modo de mantenimiento y volver a colocarlo en servicio.

Seleccione **Indefinidamente** si no desea que el dispositivo se vuelva a colocar en servicio.

Paso 6. Haga clic en **Confirmar**. La columna Mantenimiento de la tabla cambia a Sí para dicho dispositivo.

Después de finalizar

Cuando haya terminado de realizar el mantenimiento en el dispositivo, puede volver a ponerlo en servicio seleccionando el dispositivo y haciendo clic en **Acciones → Mantenimiento** y luego haga clic en **Desactivar mantenimiento** en el cuadro de diálogo. Si no coloca el dispositivo manualmente de nuevo en el modo de servicio, se coloca en modo de servicio automáticamente después de que expire la fecha y hora finales especificadas.

Trabajo con alertas

Las *alertas* son condiciones de hardware o de gestión que es preciso investigar y necesitan la acción del usuario. Lenovo XClarity Administrator sondea los dispositivos gestionados en modo asíncrono y muestra las alertas que se reciben de dichos dispositivos.

Más información: XClarity Administrator: supervisión

Acerca de esta tarea

Normalmente, cuando se recibe una alerta, en el registro de sucesos se almacena el suceso correspondiente. Es posible que haya una alerta sin el suceso correspondiente en el registro de sucesos (incluso si el registro se autoajusta). Por ejemplo, los sucesos que se producen antes de gestionar un chasis no se muestran en el registro de sucesos. Sin embargo, las alertas del chasis se muestran en el registro de alertas, pues Lenovo XClarity Administrator sondea el CMM una vez que se ha gestionado el chasis.

Visualización de alertas activas

Puede ver una lista de todas las alertas de hardware y de administración activas.

Acerca de esta tarea

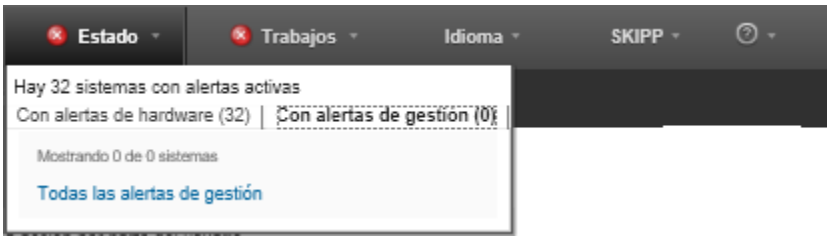
Nota: Las alertas para dispositivos Lenovo Storage solo se presentan en inglés, aunque la configuración regional de Lenovo XClarity Administrator tenga establecido otro idioma. Utilice un sistema de traducción externo para traducir los mensajes manualmente, si fuera necesario.

Procedimiento

Lleve a cabo uno de estos procedimientos para ver las alertas activas.

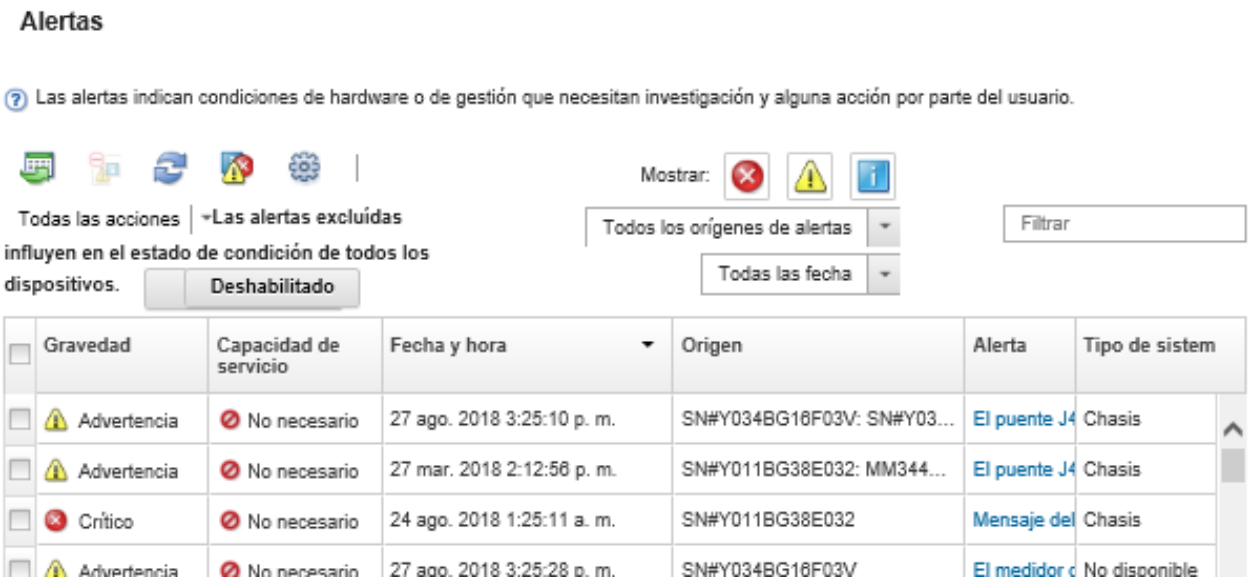
- Para ver únicamente las alertas de los dispositivos gestionados (conocidas como *alertas de hardware*), siga estos pasos:
  1. En la barra de título de XClarity Administrator, haga clic en el menú desplegable **Estado** para mostrar un resumen de las alertas de hardware y de administración.
  2. Haga clic en la pestaña **Con alertas de hardware** para ver un resumen de las alertas de cada dispositivo gestionado.

  3. Sitúe el cursor por encima de un dispositivo que se muestre dentro de dicha pestaña para ver una lista de las alertas de ese dispositivo.
  4. Haga clic en el enlace **Todas las alertas de hardware** para mostrar la página de alertas con una lista filtrada de todas las alertas de hardware.
- Para ver únicamente las alertas de XClarity Administrator (conocidas como *alertas de gestión*), siga estos pasos:
  1. En la barra de título de XClarity Administrator, haga clic en el menú desplegable **Estado** para mostrar un resumen de las alertas de hardware y de administración.
  2. Haga clic en la pestaña **Con alertas de gestión** para ver un resumen de todos los CMM y de todas las alertas de XClarity Administrator.



3. Sitúe el cursor por encima de un dispositivo que se muestre dentro de dicha pestaña para ver una lista de las alertas de ese dispositivo.
4. Haga clic en el enlace **Todas las alertas de gestión** para mostrar la página de alertas con una lista filtrada de todas las alertas del CMM y de XClarity Administrator.

- Para ver todas las alertas de XClarity Administrator, haga clic en **Supervisión → Alertas** en la barra de menús de XClarity Administrator. Se muestra la página de alertas con una lista de todas las alertas activas.

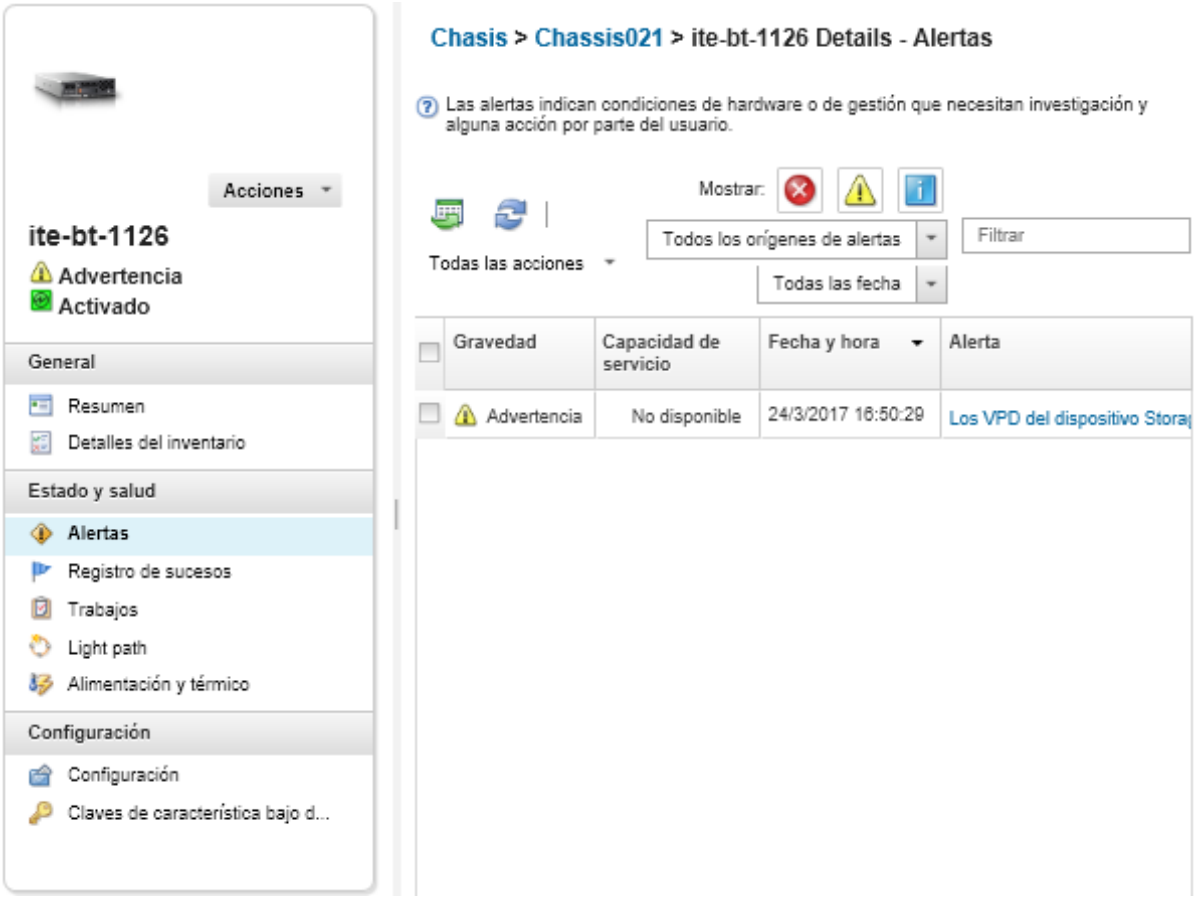


- Para ver las alertas de un dispositivo específico, siga estos pasos:
  1. En la barra de menús de XClarity Administrator, haga clic en **Hardware** y, a continuación haga clic en un tipo de dispositivo. Se muestra una página con una vista de tabla de todos los dispositivos gestionados de ese tipo. Por ejemplo, haga clic en **Hardware → Servidores** para mostrar la página Servidores.
  2. Haga clic en un dispositivo específico para mostrar la página Resumen del dispositivo.
  3. En Estado y salud, haga clic en **Alertas** para mostrar una lista de todas las alertas asociadas con ese dispositivo.

     Notas: La columna Capacidad de servicio puede mostrar “No disponible” si:

     – La alerta en el dispositivo se ha producido antes de que XClarity Administrator comenzara a gestionarlo

     – El registro de sucesos ha concluido y el suceso asociado a esa alerta ya no está en el registro de sucesos.



Resultados

Desde la página Alertas, puede llevar a cabo las siguientes acciones:

- Actualizar la lista de alertas haciendo clic en el icono **Actualizar** ( ).

  Consejo: Si se detectan nuevas alertas, el registro de alertas se actualiza automáticamente cada 30 segundos.
- Ver información acerca de una alerta específica (incluida una explicación y la acción del usuario) y acerca del dispositivo que es el origen de la alerta (como el identificador único universal) pulsando el enlace de la columna **Alerta**. Se muestra un cuadro de diálogo con información acerca de las propiedades y los detalles de la alerta.

  Nota: Si la explicación y las acciones de recuperación de una alerta no se muestran en la pestaña **Detalles**, vaya al Documentación en línea de Lenovo Flex System y, a continuación, busque el Id. de la alerta (por ejemplo, `FQXHMSE0004G`). El sitio web siempre proporcione la información más actualizada.
- De forma predeterminada, las alertas excluidas no influyen en el estado de dispositivos gestionados. Puede permitir que las alertas excluidas influyan en el estado de los dispositivos gestionados desde la página de alertas haciendo clic para alternar la habilitación de **Las alertas excluidas influyen en el estado de condición de todos los dispositivos**.
- Puede definir preferencias de umbral para generar alertas y sucesos cuando un valor, como la duración de una SSD en un servidor ThinkSystem o ThinkServer, supera un nivel crítico o de advertencia (consulte Configuración de preferencias de umbral para generar alertas y sucesos).
- Exportar el registro de alertas haciendo clic en el icono **Exportar como CSV** ( ).

Nota: Las marcas de tiempo del registro exportado utilizan la hora local especificada por el navegador web.

- Excluir alertas específicas de todas las páginas en las que se muestran alertas (consulte Exclusión de alertas).
- Restringir la lista de alertas que se muestran en la página actual:
  - Mostrar u ocultar las alertas de una determinada gravedad pulsando los siguientes iconos:
    - Icono **Alertas críticas** ()
    - Icono **Alertas de advertencia** ()
    - Icono **Alertas informativas** ()
  - Mostrar únicamente las alertas de determinados orígenes. Puede elegir una de las siguientes opciones de la lista desplegable:
    - Todos los orígenes de alerta
    - Sucesos de hardware
    - Sucesos de gestión
    - Sucesos del centro de servicio
    - Sucesos que pueda reparar el cliente
    - Sucesos que no se puedan reparar
  - Mostrar únicamente las aleras con una fecha y hora determinadas. Puede elegir una de las siguientes opciones de la lista desplegable:
    - Todas las fechas
    - Dos horas antes
    - 24 horas antes
    - La semana anterior
    - El mes anterior
  - Incluir únicamente las alertas que contengan un texto concreto introduciendo dicho texto en el campo **Filtro**.
  - Ordenar las alertas por columna pulsando un encabezado de columna.

Exclusión de alertas

Si hay alertas específicas que no son de su interés, puede excluirlas de todas las páginas en las que se muestran alertas. Las alertas excluidas siguen en el registro, pero se ocultan en todas las páginas en las que se muestran alertas, incluidos el estado del dispositivo y las vistas de los registros.

Acerca de esta tarea

Las alertas excluidas están ocultas para todos los usuarios, no solo para el usuario que ha establecido la configuración.

Puede poner dispositivos en el modo de mantenimiento, de forma que se excluyan todos los sucesos y las alertas de estos dispositivos (consulte Colocación de dispositivos en el modo de mantenimiento).

Restricción: Solo los usuarios con permisos de administrador pueden excluir o restaurar alertas.

Importante: Si excluye las alertas de estado, el estado del dispositivo no cambia en el resumen del dispositivo y las páginas detalladas.

Procedimiento

Lleve a cabo los pasos siguientes para excluir alertas del registro de alertas.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Supervisión → Alertas**. Se muestra la página Alertas.

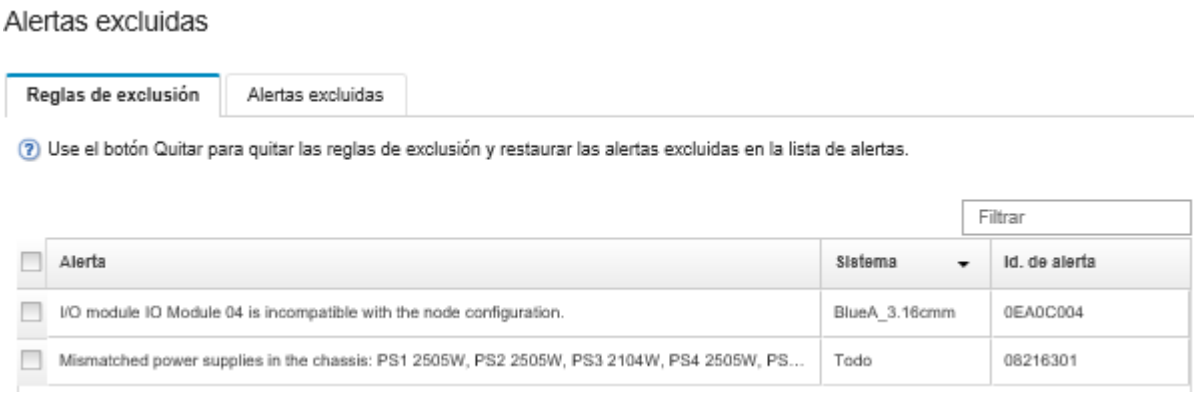
Paso 2. Seleccione las alertas que se van a excluir y haga clic en el icono **Excluir alertas** ( ). Se muestra el cuadro de diálogo Excluir alertas.

Paso 3. Seleccione una de las opciones siguientes:
- **Excluir alertas seleccionadas de todos los sistemas**. Excluye las alertas seleccionadas de todos los dispositivos gestionados.
- **Excluir solo alertas de los sistemas en el ámbito de la instancia seleccionada**. Excluye las alertas seleccionadas de los dispositivos gestionados a los que se aplican dichas alertas.

Paso 4. Haga clic en **Guardar**.

Después de finalizar

Cuando se excluyen alertas, Lenovo XClarity Administrator crea reglas de exclusión basadas en la información proporcionada. Puede ver una lista de las reglas de exclusión y las alertas excluidas en la página Alertas, al hacer clic en el icono **Mostrar alertas excluidas/confirmadas** ( ). En el cuadro de diálogo Alertas excluidas/reconocidas, haga clic en la pestaña **Reglas de exclusión** para ver una lista de las reglas de exclusión, o bien haga clic en la pestaña **Alertas excluidas** para ver la lista de las alertas excluidas.



De forma predeterminada, las alertas excluidas no influyen en el estado de dispositivos gestionados. Puede permitir que las alertas excluidas influyan en el estado de los dispositivos gestionados desde la página de alertas haciendo clic para alternar la habilitación de **Mostrar alertas excluidas/confirmadas**.

Puede restaurar alertas excluidas en el registro de alertas quitando la regla de exclusión correspondiente. Para quitar una regla de exclusión, haga clic en el icono **Mostrar alertas excluidas** ( ) para abrir el cuadro de diálogo Alertas excluidas, después, seleccione las reglas de exclusión o la alerta excluida que desee restaurar y, a continuación, haga clic en **Quitar**.

Resolución de una alerta

Lenovo XClarity Administrator proporciona información acerca de las acciones que deben realizarse para resolver una alerta.

Procedimiento

Lleve a cabo los pasos siguientes para resolver una alerta.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Supervisión → Alertas** para mostrar la página Alertas.

Paso 2. Ubique la alerta en el registro de alertas.

Paso 3. Haga clic en el vínculo de la columna **Alerta** para ver información acerca de la misma (incluida una explicación y las acciones de recuperación), así como las propiedades del dispositivo que es el origen de la alerta (como el identificador único universal).

Paso 4. Lleve a cabo las acciones de recuperación que se muestran en la pestaña **Detalles** para resolver la alerta. El ejemplo siguiente muestra las acciones de recuperación para un suceso.

Cambia el valor de la política de seguridad en el chasis gestionado al que se hace referencia para que coincida con la política de seguridad actual del servidor de administración.

Para cambiar la política de seguridad en el chasis, abra una sesión de la interfaz de la línea de comandos en el Chassis Management Module (CMM) y ejecute uno de los siguientes comandos:

- Para cambiar el nivel de la política de seguridad a `Secure`:
  ```
  security -p secure -T mm[p]
  ```
- Para cambiar el nivel de la política de seguridad a `Legacy`:
  ```
  security -p legacy -T mm[p]
  ```

Nota: Si la explicación y las acciones de recuperación de una alerta no se muestran en la pestaña **Detalles**, vaya al Documentación en línea de Lenovo Flex System y, a continuación, busque el Id. de la alerta (por ejemplo, `FQXHMSE0004G`). El sitio web siempre proporcione la información más actualizada.

Si el problema persiste aun después de realizar las acciones recomendadas, póngase en contacto con Lenovo Soporte.

Reconocer alertas

Cuando se reconoce una alerta activa, la alerta se muestra en las páginas en las que se muestran alertas, pero esto no afecta al estado de gravedad del dispositivo aplicable.

Procedimiento

Lleve a cabo los pasos siguientes para reconocer una alerta.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Supervisión → Alertas**. Se muestra la página Alertas.

Paso 2. Seleccione las alertas que va a reconocer.

Paso 3. Haga clic en el icono **Reconocer alertas** ( ).

Después de finalizar

- Puede ver una lista de las alertas reconocidas desde la página Alertas haciendo clic en el icono **Mostrar alertas excluidas/confirmadas** ( ) para mostrar el cuadro de diálogo Alertas excluidas/reconocidas y, a continuación, haciendo clic en la pestaña **Alertas reconocidas**.
- Puede eliminar el reconocimiento de una alerta activa haciendo clic en el icono **Mostrar alertas excluidas/confirmadas** ( ) para mostrar el cuadro de diálogo Alertas excluidas/reconocidas, haciendo clic en la pestaña **Alertas reconocidas**, seleccionando las alertas y haciendo clic en el icono **Eliminar reconocimiento** ( ).

Trabajo con sucesos

En Lenovo XClarity Administrator, puede tener acceso a un registro de sucesos y a un registro de auditoría.

Más información: XClarity Administrator: supervisión

Acerca de esta tarea

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

El *registro de auditoría* proporciona un historial de las acciones de los usuarios, tales como iniciar sesión en Lenovo XClarity Administrator, crear un usuario nuevo o cambiar la contraseña de un usuario. Puede usar el registro de auditoría para efectuar el seguimiento y la documentación de la autenticación y los controles de los sistemas de TI.

Supervisión de sucesos en el registro de sucesos

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

Acerca de esta tarea

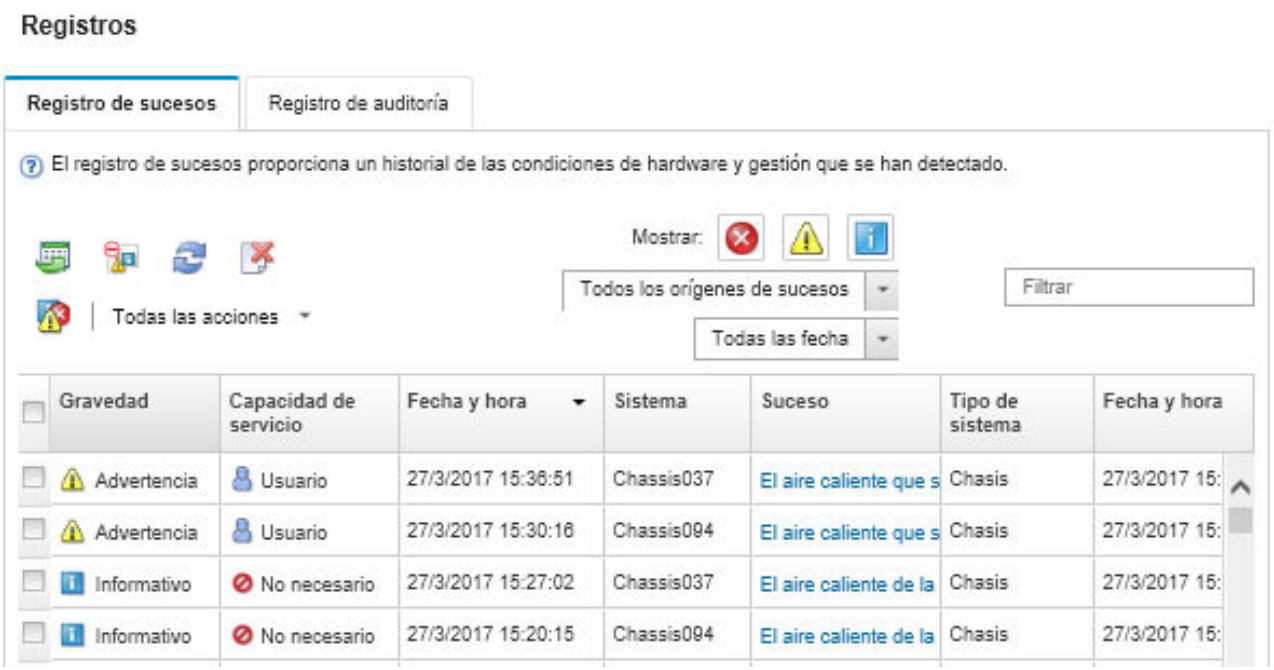
El registro de sucesos contiene sucesos informativos y no informativos. La cantidad de cada uno de estos sucesos varía hasta que se alcanza la cifra máxima de 50.000 sucesos en el registro de sucesos. En ese punto hay un máximo de 25.000 sucesos informativos y 25.000 sucesos no informativos. Por ejemplo, inicialmente hay 0 sucesos en el registro de sucesos. Supongamos que se reciben 20.000 sucesos informativos y 30.000 sucesos no informativos. Cuando se reciba el próximo suceso, se descartará el suceso informativo más antiguo, aunque exista un suceso no informativo más antiguo. Existen ocasiones en las que el registro se descuadra y hay 25.000 sucesos de cada tipo.

Lenovo XClarity Administrator envía un suceso cuando el registro de sucesos alcanza el 80 % de su tamaño mínimo y otro suceso cuando la suma de los registros de sucesos y de auditoría alcanza el 100 % del tamaño máximo.

Consejo: puede exportar el registro de sucesos para asegurarse de contar con un historial completo de todos los sucesos de hardware y de gestión. Para exportar el registro de sucesos, haga clic en el icono **Exportar como CSV** ( ).

Procedimiento

Para ver el registro de sucesos, haga clic en **Supervisión → Registros de sucesos** en la barra de menús de Lenovo XClarity Administrator y, a continuación, haga clic en la pestaña **Registro de sucesos**. Se muestra la página Registro de sucesos.



La columna **Capacidad de servicio** indica si el dispositivo requiere servicio. Esta columna puede contener uno de los siguientes valores:

- **No necesario**. El suceso es informativo y no requiere servicio.
- **Usuario**. Adopte las medidas de recuperación necesarias para resolver el problema.

  Para ver información sobre un determinado suceso, haga clic en el vínculo de la columna **Suceso**. Se muestra un cuadro de diálogo con información acerca de las propiedades del dispositivo que ha enviado el suceso, detalles acerca del suceso y acciones de recuperación.
- **Soporte**. Si la función Llamar a casa está habilitada en Lenovo XClarity Administrator, normalmente el suceso se envía al LenovoCentro de soporte, salvo que ya exista un informe de servicio abierto con el mismo Id. de suceso para el dispositivo.

  Si la opción Llamar a casa no está habilitada, le recomendamos que abra manualmente un informe de servicio para resolver el problema (consulte Apertura de un informe de servicio en la documentación en línea de Lenovo XClarity Administrator).

Resultados

Desde la página Registro de sucesos, puede llevar a cabo las siguientes acciones:

- Vea el origen del suceso pulsando el vínculo de la columna **Origen**.
- Actualizar la lista de sucesos haciendo clic en el icono **Actualizar** ( ).

  Consejo: El registro de sucesos se actualiza automáticamente cada 30 segundos si se detectan nuevos sucesos.
- Borre todos los sucesos del registro de sucesos seleccionando **Todas las acciones → Borrar registro de sucesos**.
- Ver los detalles de un suceso concreto pulsando el vínculo de la columna **Suceso** y pulsando la pestaña **Detalles**.
- Exportar el registro de sucesos haciendo clic en el icono **Exportar como CSV** ( ).

Nota: Las marcas de tiempo del registro exportado utilizan la hora local especificada por el navegador web.

- Excluir sucesos concretos de todas las páginas donde se muestran sucesos (consulte Exclusión de sucesos).
- Restringir la lista de sucesos de hardware y gestión que se muestran en la página actual:
  - Mostrar u ocultar los sucesos de una determinada gravedad pulsando los siguientes iconos de la lista desplegable:
    - Icono **Sucesos críticos** ()
    - Icono **Sucesos de advertencia** ()
    - Icono **Sucesos informativos** ()
  - Mostrar únicamente los sucesos de determinados orígenes. Puede elegir una de las siguientes opciones de la lista desplegable:
    - Todos los orígenes de alerta
    - Sucesos de hardware
    - Sucesos de gestión
    - Sucesos que se puedan reparar
    - Sucesos que pueda reparar el cliente
    - Sucesos que no se puedan reparar
  - Mostrar únicamente los sucesos con una fecha y hora determinadas. Puede elegir una de las siguientes opciones:
    - Todas las fechas
    - 2 horas antes
    - 24 horas antes
    - La semana anterior
    - El mes anterior
    - Custom

    Si selecciona **Personalizado**, puede filtrar los sucesos de hardware y de gestión que se han producido entre una fecha de inicio personalizada y la fecha actual.
  - Incluir únicamente los sucesos que contengan un texto determinado introduciendo dicho texto en el campo **Filtro**.
  - Ordenar los sucesos por columna pulsando un encabezado de columna.

Supervisión de sucesos en el registro de auditoría

El *registro de auditoría* proporciona un historial de las acciones de los usuarios, tales como iniciar sesión en Lenovo XClarity Administrator, crear un usuario nuevo o cambiar la contraseña de un usuario. Puede usar el registro de auditoría para efectuar el seguimiento y la documentación de la autenticación y los controles de los sistemas de TI.

Acerca de esta tarea

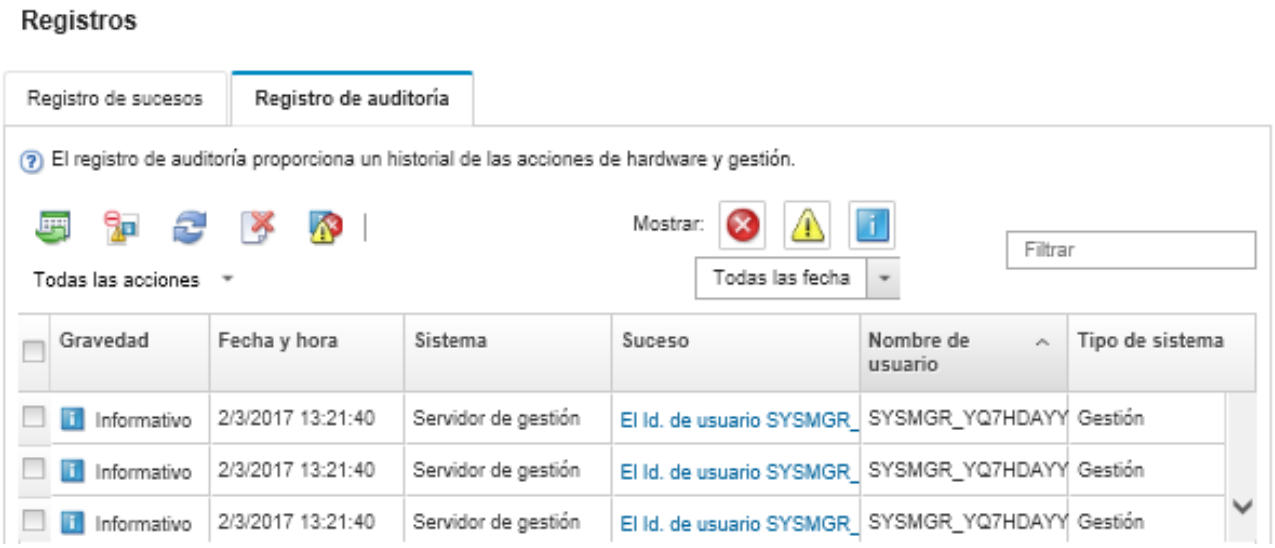
El registro de auditoría puede contener 50.000 sucesos como máximo. Cuando se alcanza el tamaño máximo, el suceso más antiguo del registro se elimina para poder añadir el nuevo.

XClarity Administrator envía un suceso cuando el registro de auditoría alcanza el 80 % de su tamaño máximo y otro suceso cuando la suma de los registros de sucesos y de auditoría alcanza el 100 % del tamaño máximo.

Consejo: puede exportar el registro de auditoría para asegurarse de contar con un historial completo de todos los sucesos de auditoría. Para exportar el registro de auditoría, haga clic en el icono **Exportar como CSV** ( ).

Procedimiento

Para ver el registro de auditoría, haga clic en **Supervisión → Registros de sucesos** en la barra de menús de XClarity Administrator y, a continuación, haga clic en la pestaña **Registro de auditoría**. Se muestra la página Registro de auditoría.



Para ver información sobre un determinado suceso de auditoría, haga clic en el vínculo de la columna **Suceso**. Se muestra un cuadro de diálogo con información acerca de las propiedades del dispositivo que ha enviado el suceso, detalles acerca del suceso y acciones de recuperación.

Resultados

Desde esta página puede llevar a cabo las siguientes acciones:

- Vea el origen del suceso de auditoría pulsando el vínculo de la columna **Origen**.
- Actualizar la lista de sucesos de auditoría haciendo clic en el icono **Actualizar** ( ).

  Consejo: El registro de sucesos se actualiza automáticamente cada 30 segundos si se detectan nuevos sucesos.
- Ver los detalles de un suceso de auditoría concreto pulsando el vínculo de la columna **Suceso** y pulsando la pestaña **Detalles** a continuación.
- Exportar el registro de auditoría haciendo clic en el icono **Exportar como CSV** ( ).

  Nota: Las marcas de tiempo del registro exportado utilizan la hora local especificada por el navegador web.
- Excluir sucesos de auditoría concretos de todas las páginas donde se muestran sucesos (consulte Exclusión de sucesos).
- Restringir la lista de sucesos de auditoría que se muestran en la página actual:
  - Mostrar u ocultar los sucesos de una determinada gravedad pulsando los siguientes iconos:
    - Icono **Sucesos críticos** ( )

  - Icono **Sucesos de advertencia** ()
  - Icono **Sucesos informativos** ()
- Mostrar únicamente los sucesos con una fecha y hora determinadas. Puede elegir una de las siguientes opciones de la lista desplegable:
  - Todas las fechas
  - 2 horas antes
  - 24 horas antes
  - La semana anterior
  - El mes anterior
  - Custom

  Si selecciona **Personalizado**, puede filtrar los sucesos de hardware y de gestión que se han producido entre una fecha de inicio personalizada y la fecha actual.
- Incluir únicamente los sucesos que contengan un texto determinado introduciendo dicho texto en el campo **Filtro**.
- Ordenar los sucesos por columna pulsando un encabezado de columna.

Resolución de un suceso

Lenovo XClarity Administrator proporciona información acerca de las acciones que deben realizarse para resolver un suceso.

Procedimiento

Lleve a cabo los pasos siguientes para resolver un suceso.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Supervisión → Registros de sucesos** para mostrar la página Registros.

Paso 2. Haga clic en la pestaña **Registro de sucesos**.

Paso 3. Busque el suceso en el registro de sucesos.

Paso 4. Haga clic en el vínculo de la columna **Suceso** para ver la información acerca del mismo (incluida una explicación y las acciones de recuperación) y acerca del dispositivo que es la fuente del suceso.

Paso 5. Haga clic en la pestaña **Detalles**.

Paso 6. Lleve a cabo las acciones de recuperación que se muestran en la pestaña **Detalles** para resolver el suceso.

Nota: Si no aparecen la explicación y la acción de recuperación de un suceso, vaya al Documentación en línea de Lenovo Flex System y busque el título del suceso. El sitio web siempre proporcione la información más actualizada.

Si el problema persiste aun después de realizar las acciones recomendadas, póngase en contacto con Lenovo Soporte.

Exclusión de sucesos

Si hay sucesos específicos que no son de su interés, puede excluirlos de todas las páginas en las que se muestran sucesos. Los sucesos excluidos siguen en el registro, pero están ocultos en todas las páginas en las que se muestran sucesos.

Acerca de esta tarea

Los sucesos excluidos están ocultos para todos los usuarios, no solo para el usuario que ha establecido la configuración.

Puede poner dispositivos en el modo de mantenimiento, de forma que se excluyan todos los sucesos y las alertas de estos dispositivos (consulte Colocación de dispositivos en el modo de mantenimiento).

Restricción: solo los usuarios con permisos de administrador pueden excluir o restaurar sucesos.

Procedimiento

Lleve a cabo los pasos siguientes para excluir sucesos de los registros de sucesos.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, pulse **Supervisión → Registros de sucesos** y, a continuación, pulse la pestaña **Registro de sucesos**. Aparecen los registros de sucesos.

Paso 2. Seleccione los sucesos que desea excluir y haga clic en el icono **Excluir sucesos** ( ). Se muestra el cuadro de diálogo Excluir sucesos.

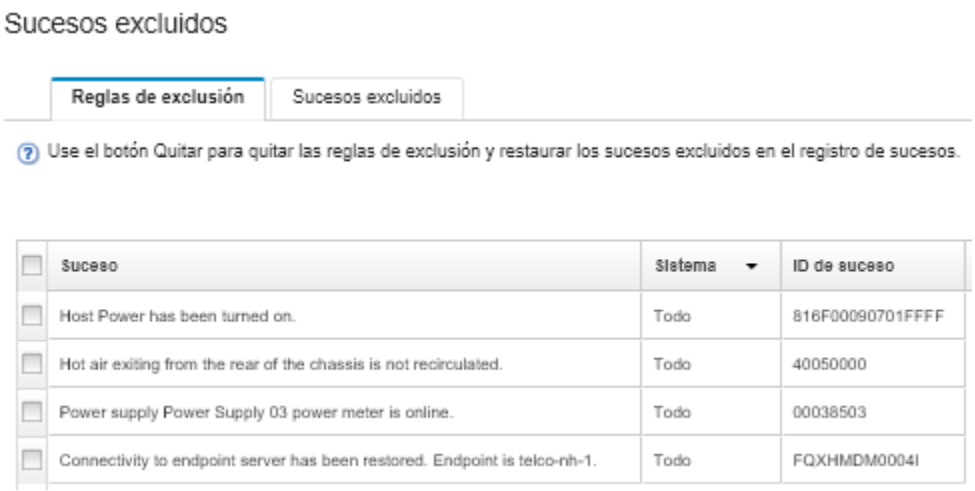
Paso 3. Seleccione una de las opciones siguientes:
- **Excluir sucesos seleccionados de todos los sistemas**. Excluye los sucesos seleccionados de todos los dispositivos gestionados.
- **Excluir solo sucesos de los sistemas en el ámbito de la instancia seleccionada**. Excluye los sucesos seleccionados de los dispositivos gestionados a los que se aplican los sucesos seleccionados.

Paso 4. Haga clic en **Guardar**.

Después de finalizar

Cuando se excluyen sucesos, Lenovo XClarity Administrator crea reglas de exclusión basadas en la información indicada.

- Visualice una lista de las reglas de exclusión y los sucesos excluidos en la página Registros, al hacer clic en el icono **Mostrar sucesos excluidos** ( ). En el cuadro de diálogo Sucesos excluidos, haga clic en la pestaña **Reglas de exclusión** para ver las reglas de exclusión, o bien haga clic en la pestaña **Sucesos excluidos** para ver los sucesos excluidos.



- Restaure los sucesos excluidos en el registro de sucesos al quitar la regla de exclusión correspondiente. Para quitar una regla de exclusión, haga clic en el icono **Mostrar sucesos excluidos** ( ) para visualizar el cuadro de diálogo Sucesos excluidos, después, seleccione las reglas de exclusión que desee restaurar y, a continuación, haga clic en **Quitar exclusiones**.

- Para evitar que los sucesos de mantenimiento que se encuentran en la lista de sucesos excluidos abran automáticamente los informes de problemas, haga clic en **Administración → Servicio y soporte** desde la barra de menú de Lenovo XClarity Administrator, después, haga clic en la pestaña **Despachadores de servicio** y, a continuación, seleccione **No** en la pregunta **¿Desea que los sucesos excluidos abran el informe de problemas?**

Reenvío de sucesos

Puede configurar Lenovo XClarity Administrator de modo que reenvíe los sucesos a los dispositivos móviles y las aplicaciones conectadas del entorno, a fin de agregar y supervisar el estado del hardware y los problemas de tiempo de ejecución del entorno de hardware.

Más información:  XClarity Administrator: supervisión

Enviar sucesos a syslog, en el gestor remoto de SNMP, correo electrónico y otros servicios de sucesos

Puede configurar Lenovo XClarity Administrator de modo que reenvíe los sucesos a las aplicaciones conectadas del entorno, a fin de agregar y supervisar el estado del hardware y los problemas de tiempo de ejecución del entorno de hardware. Puede definir el alcance de los sucesos que se reenviarán en función del dispositivo, la clase o gravedad del suceso y el componente.

Acerca de esta tarea

Lenovo XClarity Administrator puede reenviar sucesos a uno o varios dispositivos. Para los sucesos de auditoría, puede optar por reenviar todos ellos o ninguno. No se pueden reenviar sucesos de auditoría concretos. Para los sucesos de hardware y gestión, puede reenviar aquellos que revistan uno o varios niveles de gravedad determinados (críticos, de advertencia o informativos) y para uno o varios componentes (tales como unidades de disco, procesadores y adaptadores).

Lenovo XClarity Administrator usa despachadores de sucesos para reenviar los sucesos. Un *despachador de sucesos* incluye información acerca del protocolo que se debe utilizar, así como acerca del destinatario, de los dispositivos que es preciso supervisar y de los sucesos que se van a reenviar. Una vez creado y habilitado un despachador de sucesos, Lenovo XClarity Administrator comienza a supervisar los sucesos entrantes de acuerdo con los criterios de filtrado. Cuando se detecta una coincidencia, se usa el protocolo asociado para reenviar el suceso.

Se admiten los siguientes protocolos:

- **Análisis de registro de Azure**. Lenovo XClarity Administrator reenvía los eventos monitoreados por la red a una interfaz deAnálisis de registro Microsoft Azure.
- **Correo electrónico**. Lenovo XClarity Administrator reenvía los sucesos supervisados a una o varias direcciones de correo electrónico mediante SMTP. El correo electrónico contiene información acerca del suceso, así como el nombre de host del dispositivo de origen y vínculos a la interfaz web de Lenovo XClarity Administrator y a la aplicación Lenovo XClarity Mobile.
- **FTP**. Reenvía los eventos monitoreados por la red a una un servidor FTP.
- **REST**. Lenovo XClarity Administrator envía los sucesos supervisados a través de la red a un servicio web REST.
- **SNMP**. Lenovo XClarity Administrator reenvía los sucesos supervisados a través de la red a un gestor de SNMP remoto. Se admiten las trampas SNMPv1 y SNMPv3.

  Para obtener información acerca del archivo base de información de gestión (MIB) que describe las interrupciones SNMP que se generan mediante Lenovo XClarity Administrator, consulte el archivo lenovoMgrAlert.mibArchivo lenovoMgrAlert.mib en la documentación en línea de Lenovo XClarity Administrator.

- **Syslog**. Lenovo XClarity Administrator reenvía los sucesos supervisados a través de la red a un servidor de registro central donde se pueden usar herramientas nativas para supervisar el syslog.

Puede crear y habilitar hasta 20 despachadores de sucesos para enviar sucesos a destinatarios específicos.

Si XClarity Administrator se reinicia después de configurar los despachadores de sucesos, debe esperar que el servidor de gestión vuelva a generar los datos internos antes de que se puedan reenviar correctamente los sucesos.

Para la XClarity Administrator versión 1.2.0 y posteriores, **Conmutadores** se incluye en la pestaña **Sucesos** de los cuadros de diálogo Nuevo despachador de sucesos y Cambiar despachadores de sucesos. Si se actualizó a 1.2.0 o posterior a partir de una versión anterior, recuerde actualizar los despachadores de sucesos para incluir o excluir sucesos de RackSwitch, según corresponda. Esto es necesario, incluso si seleccionó la casilla de verificación **Todos los sistemas** para seleccionar todos los dispositivos.

Nota: Los sucesos no se entregan si, por ejemplo, se pierde la conectividad entre Lenovo XClarity Administrator y el despachador de sucesos o si el puerto se bloquea.

Configuración del reenvío de sucesos a Análisis de registro de Azure

Puede configurar Lenovo XClarity Administrator para que reenvíe sucesos específicos a Análisis de registro de Azure.

Acerca de esta tarea

Puede crear y habilitar hasta 20 despachadores de sucesos para enviar sucesos a destinatarios específicos.

Si XClarity Administrator se reinicia después de configurar los despachadores de sucesos, debe esperar que el servidor de gestión vuelva a generar los datos internos antes de que se puedan reenviar correctamente los sucesos.

Nota: Para la XClarity Administrator versión 1.2.0 y posteriores, **Conmutadores** se incluye en la pestaña **Sucesos** de los cuadros de diálogo Nuevo despachador de sucesos y Cambiar despachadores de sucesos. Si se actualizó a 1.2.0 o posterior a partir de una versión anterior, recuerde actualizar los despachadores de sucesos para incluir o excluir sucesos de RackSwitch, según corresponda. Esto es necesario, incluso si seleccionó la casilla de verificación **Todos los sistemas** para seleccionar todos los dispositivos.

Procedimiento

Realice los siguientes pasos para crear un despachador de sucesos para Análisis de registro de Azure.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Supervisión → Reenvío de sucesos**. Se muestra la página Reenvío de sucesos.

Paso 2. Haga clic en la pestaña **Despachador de sucesos**.

Paso 3. Haga clic en el icono **Crear** ( ). Se abre la pestaña **General** del cuadro de diálogo Nuevo despachador de sucesos.

Paso 4. Seleccione **Análisis de registro de Azure** como tipo de despachador de sucesos y rellene la información específica del protocolo:

- Escriba el nombre y una descripción opcional del despachador de sucesos.
- Introduzca la clave principal de la interfaz Análisis de registro de Azure.
- Especifique el período de desconexión (en segundos) para la solicitud. El valor predeterminado es 30 segundos.
- **Opcional**: si se requiere autenticación, seleccione uno de los siguientes tipos de autenticación:

- **Básico**. Se autentica en el servidor especificado usando el Id. de usuario especificado y la contraseña.
- **Ninguno**. No se utiliza ninguna autenticación.

Paso 5. Haga clic en **Formato de salida** para elegir el formato de salida de los datos de sucesos que se reenviarán. La información varía según el tipo de despachador de sucesos.

El siguiente formato de salida de ejemplo es el formato predeterminado para los destinatarios de Análisis de registro de Azure. Todas las palabras entre corchetes dobles son las variables que se sustituyen con los valores reales cuando se despacha un suceso. Las variables disponibles para los destinatarios de Análisis de registro de Azure se enumeran el cuadro de diálogo Formato de salida.

```
{\"Msg\":\"[[EventMessage]]\",\"EventID\":\"[[EventID]]\",\"Serialnum\":
\"[[EventSerialNumber]]\",\"SenderUUID\":\"[[EventSenderUUID]]\",\"Flags\":
\"[[EventFlags]]\",\"Userid\":\"[[EventUserName]]\",\"LocalLogID\":
\"[[EventLocalLogID]]\",\"DeviceName\":\"[[DeviceFullPathName]]\",\"SystemName\":
\"[[SystemName]]\",\"Action\":\"[[EventAction]]\",\"FailFRUs\":
\"[[EventFailFRUs]]\",\"Severity\":\"[[EventSeverity]]\",\"SourceID\":
\"[[EventSourceUUID]]\",\"SourceLogSequence\":[[EventSourceLogSequenceNumber]],
\"FailSNs\":\"[[EventFailSerialNumbers]]\",\"FailFRUUUIDs\":
\"[[EventFailFRUUUIDs]]\",\"EventClass\":\"[[EventClass]]\",\"ComponentID\":
\"[[EventComponentUUID]]\",\"Mtm\":\"[[EventMachineTypeModel]]\",\"MsgID\":
\"[[EventMessageID]]\",\"SequenceNumber\":\"[[EventSequenceID]]\",\"TimeStamp\":
\"[[EventTimeStamp]]\",\"Args\":[[EventMessageArguments]],\"Service\":
\"[[EventService]]\",\"CommonEventID\":\"[[CommonEventID]]\",\"EventDate\":
\"[[EventDate]]\",\"EventSource\":\"[[EventSource]]\",\"DeviceSerialNumber\":
\"[[DeviceSerialNumber]]\",\"DeviceIPAddress\":\"[[DeviceIPAddress]]\",
\"LXCA\":\"[[LXCA_IP]]\"}
```

Puede hacer clic en **Restablecer valores predeterminados** para cambiar el formato de salida a los campos predeterminados.

Paso 6. Haga clic en el botón de alternación **Permitir sucesos excluidos** para permitir o prevenir el reenvío de sucesos excluidos.

Paso 7. Seleccione **Habilitar este despachador** para activar el reenvío de sucesos para este despachador de sucesos.

Paso 8. Pulse **Siguiente** para mostrar la pestaña **Dispositivos**.

Paso 9. Seleccione los dispositivos y grupos que desee supervisar para este despachador de sucesos.

Consejo Para reenviar sucesos de todos los dispositivos gestionados (actuales y futuros), seleccione la casilla de verificación **Igualar todos los sistemas**.Si no selecciona la casilla **Igualar todos los sistemas**, asegúrese de que los dispositivos seleccionados no tengan un DUMMY-UUID en la columna UUID. Se asigna un Dummy-UUID a los dispositivos que aún no se recuperan después de un reinicio o no han sido detectados completamente por el servidor de gestión. Si selecciona un dispositivo con un Dummy-UUID, el reenvío de sucesos no funcionará para este dispositivo hasta que el dispositivo sea completamente detectado o recuperado y el Dummy-UUID cambie a su UUID real.

Paso 10. Haga clic en **Siguiente** para mostrar la pestaña **Sucesos**.

Paso 11. Seleccione los filtros que se utilizarán para este despachador de sucesos.

- **Coincidir por categorías de sucesos**.
  1. Para reenviar todos los sucesos de auditoría, sin importar el nivel de estado, seleccione **Incluir todos los sucesos de auditoría**.
  2. Para reenviar todos los sucesos de garantía, seleccione la opción **Incluir los sucesos de garantía**.

3. Para volver a enviar todos los sucesos de cambio de estado y salud, seleccione **Incluir los sucesos de cambio de estado**.
4. Para volver a enviar todos los sucesos de actualización de estado y salud, seleccione **Incluir los sucesos de actualización de estado**.
5. Seleccione las clases de sucesos y niveles de capacidad de servicio que desee reenviar.
6. Introduzca el Id. de uno o varios sucesos que desea excluir de reenvío. Separe los identificadores utilizando una coma (por ejemplo, `FQXHMEM0214I,FQXHMEM0214I`).

- **Coincidir por el código de suceso**. Introduzca el Id. de uno o varios sucesos que desee reenviar. Separe los identificadores entre sí mediante comas.
- **Excluir por categorías de sucesos**.
  1. Para excluir todos los sucesos de auditoría, sin importar el nivel de estado, seleccione **Excluir todos los sucesos de auditoría**.
  2. Para excluir todos los sucesos de garantía, seleccione la opción **Excluir los sucesos de garantía**.
  3. Para excluir todos los sucesos de cambio de estado y salud, seleccione **Excluir los sucesos de cambio de estado**.
  4. Para excluir todos los sucesos de actualización de estado y salud, seleccione **Excluir los sucesos de actualización de estado**.
  5. Seleccione las clases de sucesos y niveles de capacidad de servicio que desee excluir.
  6. Introduzca el Id. de uno o varios sucesos que desee reenviar. Separe los identificadores utilizando una coma.
- **Excluir por el código de suceso**. Introduzca el Id. de uno o varios sucesos que desee excluir. Separe los identificadores entre sí mediante comas.

Paso 12. Elija si se deben incluir determinados tipos de sucesos.

- **Incluir todos los sucesos de auditoría**. Envía notificaciones sobre sucesos de auditoría, según las clases y gravedades de los sucesos seleccionados.
- **Incluir sucesos de garantía**. Enviar notificaciones sobre garantías.
- **Incluye sucesos de cambio de estado**. Envía notificaciones sobre cambios de estado.
- **Incluye sucesos de actualización de estado**. Se enviaron notificaciones sobre nuevas alertas.
- **Incluir sucesos del boletín**. Envía notificaciones sobre boletines nuevos.

Paso 13. Seleccione los tipos de sucesos y niveles de gravedad por los que desea que se le notifique.

Paso 14. Seleccione si se deben filtrar sucesos por capacidad de servicio.

Paso 15. Haga clic en **Siguiente** para mostrar la pestaña **Programador**.

Paso 16. **Opcional:** defina las horas y los días en los que desea que se reenvíen sucesos específicos a este despachador de sucesos. Solo se reenvían los sucesos que se producen durante el periodo de tiempo especificado.

Si no crea una planificación para el despachador de sucesos, los sucesos se reenviarán las 24 horas del día, 7 días a la semana.

1. Use el icono **Desplazar a la izquierda** (◀) y el icono **Desplazar a la derecha** (▶) y los botones **Día**, **Semana** y **Mes** para determinar el día y la hora a la que desea que comience la planificación.
2. Haga clic en dos veces la hora para abrir el cuadro de diálogo Nuevo periodo de tiempo.
3. Complete la información requerida, incluida la fecha, horas de inicio y término y si desea que se repita la programación.

4. Haga clic en **Crear** para guardar la planificación y cerrar el cuadro de diálogo. La nueva planificación se añade al calendario.

Consejo:
- Puede cambiar la hora arrastrando la entrada de programación hacia otra hora en el calendario.
- Puede cambiar la duración al seleccionar la parte superior o inferior de la entrada de programación y arrastrarla hacia la nueva hora en el calendario.
- Puede cambiar la hora de término al seleccionar la parte inferior de la entrada de programación y arrastrarla hacia la nueva hora en el calendario.
- Puede cambiar la programación al pulsar dos veces la entrada de programación en el calendario y pulsar **Editar entrada**.
- Se puede visualizar un resumen de todas las entradas de programación al seleccionar **Mostrar resumen del planificador**. El resumen incluye los espacios de tiempo de cada entrada y las entradas que se repiten.
- Puede eliminar una entrada de programación del calendario o resumen de programador seleccionando la entrada y haciendo clic en **Eliminar entrada**.

Paso 17. Haga clic en **Crear**.

El despachador de sucesos aparecerá en la tabla Reenvío de sucesos.

Paso 18. Seleccione el nuevo despachador de sucesos, haga clic en **Generar suceso de prueba** y luego compruebe que el reenvío de sucesos se realice correctamente al servidor de Análisis de registro de Azure correspondiente.

Después de finalizar

Desde la página Reenvío de sucesos, también puede realizar las acciones siguientes en un despachador de sucesos:

- Actualizar la lista de despachadores de sucesos haciendo clic en el icono **Actualizar** ( ).
- Ver los detalles de un despachador de sucesos pulsando el vínculo de la columna **Nombre**.
- Cambiar las propiedades de los despachadores de sucesos y filtrar los criterios pulsando el nombre del despachador de sucesos en la columna **Nombre**.
- Eliminar el despachador de sucesos haciendo clic en el icono **Eliminar** ( ).
- Suspender el reenvío de sucesos (consulte Suspensión del reenvío de sucesos).

Configuración del reenvío de sucesos a un servicio de correo electrónico usando SMTP

Puede configurar Lenovo XClarity Administrator para reenviar sucesos específicos a un servicio de correo electrónico mediante SMTP.

Antes de empezar

Para reenviar un correo electrónico a un servicio por correo electrónico en Internet (como Gmail, Hotmail, o Yahoo), el servidor SMTP debe ser compatible con el correo de la web del reenvío.

Antes de configurar un despachador de sucesos a un servicio web de Gmail, revise la información en Configurar reenvío de sucesos a un servicio SMTP de GmailConfigurar el reenvío de sucesos en syslog, en el gestor remoto de SNMP, o en correo electrónico en la documentación en línea de Lenovo XClarity Administrator.

Acerca de esta tarea

Puede crear y habilitar hasta 20 despachadores de sucesos para enviar sucesos a destinatarios específicos.

Si XClarity Administrator se reinicia después de configurar los despachadores de sucesos, debe esperar que el servidor de gestión vuelva a generar los datos internos antes de que se puedan reenviar correctamente los sucesos.

Nota: Para la XClarity Administrator versión 1.2.0 y posteriores, **Conmutadores** se incluye en la pestaña **Sucesos** de los cuadros de diálogo Nuevo despachador de sucesos y Cambiar despachadores de sucesos. Si se actualizó a 1.2.0 o posterior a partir de una versión anterior, recuerde actualizar los despachadores de sucesos para incluir o excluir sucesos de RackSwitch, según corresponda. Esto es necesario, incluso si seleccionó la casilla de verificación **Todos los sistemas** para seleccionar todos los dispositivos.

Procedimiento

Realice los siguientes pasos para crear un despachador de sucesos para correo electrónico usando SMTP.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Supervisión → Reenvío de sucesos**. Se muestra la página Reenvío de sucesos.

Paso 2. Haga clic en la pestaña **Despachador de sucesos**.

Paso 3. Haga clic en el icono **Crear** ( ). Se abre la pestaña **General** del cuadro de diálogo Nuevo despachador de sucesos.

Paso 4. Seleccione **Correo electrónico** como tipo de despachador de sucesos y rellene la información específica del protocolo:

- Escriba el nombre, el host de destino y una descripción opcional del despachador de sucesos.
- Especifique el puerto que se usará para reenviar sucesos. El valor predeterminado es `25`.
- Especifique el período de desconexión (en segundos) para la solicitud. El valor predeterminado es 30 segundos.
- Especifique la dirección de correo electrónico de cada destinatario. Separe las direcciones de correo electrónico entre sí mediante comas.

  Para enviar el correo electrónico para el contacto de soporte que se asigna para el dispositivo, seleccione **Usar correos de contacto de soporte** (consulte Definición de los contactos de soporte para un dispositivo en la documentación en línea de XClarity Administrator).
- **Opcional:** ingrese la dirección de correo electrónico del remitente del correo electrónico (por ejemplo, `john@company.com`).

Si no especifica una dirección de correo electrónico, la dirección del remitente es `LXCA.<source_identifier>@<smtp_host>` de manera predeterminada.

Si especifica únicamente el dominio del remitente, el formato de la dirección del remitente es *<LXCA_host_name>*@*<sender_domain>* (por ejemplo, XClarity1@company.com).

Notas:

- Si configura el servidor SMTP de modo que sea necesario indicar un nombre de host para reenviar correos electrónicos y no configura un nombre de host para XClarity Administrator, es posible que el servidor SMTP rechace los sucesos reenviados. Si XClarity Administrator no dispone de un nombre de host, el suceso se reenvía junto con la dirección IP. Si no es posible obtener la dirección IP por cualquier motivo, se envía "localhost" en su lugar, lo que puede provocar que el servidor SMTP rechace el suceso.
- Si especifica el dominio del remitente, el origen no se identifica en la dirección del remitente. Por el contrario, la información sobre el origen del suceso se incluye en el cuerpo del correo electrónico, incluido el nombre del sistema, la dirección IP, el tipo o modelo y el número de serie.
- Si el servidor SMTP solo acepta los correos electrónicos enviados por un usuario registrado, se rechaza la dirección del remitente predeterminado (`LXCA.<source_identifier>@<smtp_host>`). En este caso, debe especificar al menos un nombre de dominio en el campo **Dirección Desde**.

- **Opcional:** para establecer una conexión segura al servidor SMTP, seleccione los tipos de conexión siguientes:
  - **SSL**. Utilice el protocolo SSL mientras se comunica.
  - **STARTTLS**. Utiliza TLS para formar una comunicación segura en un canal no seguro.

  Si se selecciona uno de estos tipos de conexión, LXCA intenta descargar e importar el certificado de servidor SMTP a su almacén de confianza. Se le solicita aceptar la adición de este certificado al almacén de confianza.
- **Opcional:** si se requiere autenticación, seleccione uno de los siguientes tipos de autenticación:
  - **Regular**. Se autentica en el servidor SMTP especificado usando el Id. de usuario especificado y la contraseña.
  - **NTLM**. Utiliza el protocolo de NT LAN Manager (NTLM) para la autenticación con el servidor SMTP especificado utilizando el Id. de usuario, contraseña y el nombre de dominio especificado.
  - **OAUTH2**. Utiliza el protocolo Simple Authentication and Security Layer (SASL) para autenticar en el servidor SMTP especificado utilizando el nombre de usuario y token de seguridad especificado. Normalmente, el nombre de usuario es su dirección de correo electrónico.

    Atención: El token de seguridad caduca después de un corto período de tiempo. Es de su responsabilidad actualizar el token de seguridad.
  - **Ninguno**. No se utiliza ninguna autenticación.

Paso 5. Haga clic en **Formato de salida** para elegir el formato de salida de los datos de sucesos que se van a reenviar en el cuerpo del correo electrónico y el formato del asunto del correo electrónico. La información varía según el tipo de despachador de sucesos.

El siguiente formato de salida de ejemplo es el formato predeterminado para los destinatarios de correo electrónico. Todas las palabras entre corchetes dobles son las variables que se sustituyen con los valores reales cuando se despacha un suceso. Las variables disponibles para los destinatarios de correo electrónico se enumeran el cuadro de diálogo Formato de salida.

Asunto de correo electrónico

```
[[DeviceName]]-[[EventMessage]]
```

Cuerpo de correo electrónico

```
Alert: [[EventDate]] [[EventMessage]]\n
\n
Hardware Information:\n
Managed Endpoint    : [[DeviceHardwareType]] at [[DeviceIPAddress]]\n
Device name          : [[DeviceName]]\n
Product name         : [[DeviceProductName]]\n
Host name            : [[DeviceHostName]]\n
Machine Type         : [[DeviceMachineType]]\n
Machine Model        : [[DeviceMachineModel]]\n
Serial Number        : [[DeviceSerialNumber]]\n
DeviceHealthStatus   : [[DeviceHealthStatus]]\n
IPv4 addresses       : [[DeviceIPV4Addresses]]\n
IPv6 addresses       : [[DeviceIPV6Addresses]]\n
Chassis              : [[DeviceChassisName]]\n
DeviceBays           : [[DeviceBays]]\n
\n
LXCA is: [[ManagementServerIP]]\n
\n
Event Information:\n
  Event ID         : [[EventID]]\n
  Common Event ID : [[CommonEventID]]\n
  EventSeverity    : [[EventSeverity]]\n
  Event Class      : [[EventClass]]\n
  Sequence ID      : [[EventSequenceID]]\n
  Event Source ID : [[EventSourceUUID]]\n
  Component ID     : [[EventComponentUUID]]\n
  Serial Num       : [[EventSerialNumber]]\n
  MTM              : [[EventMachineTypeModel]]\n
  EventService     : [[EventService]]\n
  Console link     : [[ConsoleLink]]\n
  iOS link         : [[iOSLink]]\n
  Android link     : [[AndroidLink]]\n
  System Name      : [[DeviceFullPathName]]\n
```

Puede hacer clic en **Restablecer valores predeterminados** para cambiar el formato de salida a los campos predeterminados.

Paso 6. Haga clic en el botón de alternación **Permitir sucesos excluidos** para permitir o prevenir el reenvío de sucesos excluidos.

Paso 7. Seleccione **Habilitar este despachador** para activar el reenvío de sucesos para este despachador de sucesos.

Paso 8. Pulse **Siguiente** para mostrar la pestaña **Dispositivos**.

Paso 9. Seleccione los dispositivos y grupos que desee supervisar para este despachador de sucesos.

Consejo Para reenviar sucesos de todos los dispositivos gestionados (actuales y futuros), seleccione la casilla de verificación **Igualar todos los sistemas**.Si no selecciona la casilla **Igualar todos los sistemas**, asegúrese de que los dispositivos seleccionados no tengan un DUMMY-UUID en la columna UUID. Se asigna un Dummy-UUID a los dispositivos que aún no se recuperan después de un reinicio o no han sido detectados completamente por el servidor de gestión. Si selecciona un dispositivo con un Dummy-UUID, el reenvío de sucesos no funcionará para este dispositivo hasta que el dispositivo sea completamente detectado o recuperado y el Dummy-UUID cambie a su UUID real.

Paso 10. Haga clic en **Siguiente** para mostrar la pestaña **Sucesos**.

Paso 11. Seleccione los filtros que se utilizarán para este despachador de sucesos.

- **Coincidir por categorías de sucesos**.

1. Para reenviar todos los sucesos de auditoría, sin importar el nivel de estado, seleccione **Incluir todos los sucesos de auditoría**.
2. Para reenviar todos los sucesos de garantía, seleccione la opción **Incluir los sucesos de garantía**.
3. Para volver a enviar todos los sucesos de cambio de estado y salud, seleccione **Incluir los sucesos de cambio de estado**.
4. Para volver a enviar todos los sucesos de actualización de estado y salud, seleccione **Incluir los sucesos de actualización de estado**.
5. Seleccione las clases de sucesos y niveles de capacidad de servicio que desee reenviar.
6. Introduzca el Id. de uno o varios sucesos que desea excluir de reenvío. Separe los identificadores utilizando una coma (por ejemplo, `FQXHMEM0214I,FQXHMEM0214I`).

- **Coincidir por el código de suceso**. Introduzca el Id. de uno o varios sucesos que desee reenviar. Separe los identificadores entre sí mediante comas.
- **Excluir por categorías de sucesos**.
  1. Para excluir todos los sucesos de auditoría, sin importar el nivel de estado, seleccione **Excluir todos los sucesos de auditoría**.
  2. Para excluir todos los sucesos de garantía, seleccione la opción **Excluir los sucesos de garantía**.
  3. Para excluir todos los sucesos de cambio de estado y salud, seleccione **Excluir los sucesos de cambio de estado**.
  4. Para excluir todos los sucesos de actualización de estado y salud, seleccione **Excluir los sucesos de actualización de estado**.
  5. Seleccione las clases de sucesos y niveles de capacidad de servicio que desee excluir.
  6. Introduzca el Id. de uno o varios sucesos que desee reenviar. Separe los identificadores utilizando una coma.
- **Excluir por el código de suceso**. Introduzca el Id. de uno o varios sucesos que desee excluir. Separe los identificadores entre sí mediante comas.

Paso 12. Elija si se deben incluir determinados tipos de sucesos.

- **Incluir todos los sucesos de auditoría**. Envía notificaciones sobre sucesos de auditoría, según las clases y gravedades de los sucesos seleccionados.
- **Incluir sucesos de garantía**. Enviar notificaciones sobre garantías.
- **Incluye sucesos de cambio de estado**. Envía notificaciones sobre cambios de estado.
- **Incluye sucesos de actualización de estado**. Se enviaron notificaciones sobre nuevas alertas.
- **Incluir sucesos del boletín**. Envía notificaciones sobre boletines nuevos.

Paso 13. Seleccione los tipos de sucesos y niveles de gravedad por los que desea que se le notifique.

Paso 14. Seleccione si se deben filtrar sucesos por capacidad de servicio.

Paso 15. Haga clic en **Siguiente** para mostrar la pestaña **Programador**.

Paso 16. **Opcional:** defina las horas y los días en los que desea que se reenvíen sucesos específicos a este despachador de sucesos. Solo se reenvían los sucesos que se producen durante el periodo de tiempo especificado.

Si no crea una planificación para el despachador de sucesos, los sucesos se reenviarán las 24 horas del día, 7 días a la semana.

1. Use el icono **Desplazar a la izquierda** (◀) y el icono **Desplazar a la derecha** (▶) y los botones **Día**, **Semana** y **Mes** para determinar el día y la hora a la que desea que comience la planificación.

2. Haga clic en dos veces la hora para abrir el cuadro de diálogo Nuevo periodo de tiempo.
3. Complete la información requerida, incluida la fecha, horas de inicio y término y si desea que se repita la programación.
4. Haga clic en **Crear** para guardar la planificación y cerrar el cuadro de diálogo. La nueva planificación se añade al calendario.

Consejo:
- Puede cambiar la hora arrastrando la entrada de programación hacia otra hora en el calendario.
- Puede cambiar la duración al seleccionar la parte superior o inferior de la entrada de programación y arrastrarla hacia la nueva hora en el calendario.
- Puede cambiar la hora de término al seleccionar la parte inferior de la entrada de programación y arrastrarla hacia la nueva hora en el calendario.
- Puede cambiar la programación al pulsar dos veces la entrada de programación en el calendario y pulsar **Editar entrada**.
- Se puede visualizar un resumen de todas las entradas de programación al seleccionar **Mostrar resumen del planificador**. El resumen incluye los espacios de tiempo de cada entrada y las entradas que se repiten.
- Puede eliminar una entrada de programación del calendario o resumen de programador seleccionando la entrada y haciendo clic en **Eliminar entrada**.

Paso 17. Haga clic en **Crear**.

El despachador de sucesos aparecerá en la tabla Reenvío de sucesos.

Paso 18. Seleccione el nuevo despachador de sucesos, haga clic en **Generar suceso de prueba** y luego compruebe que el reenvío de sucesos se realice correctamente al servicio de correo electrónico correspondiente.

Después de finalizar

Desde la página Reenvío de sucesos, también puede realizar las acciones siguientes en un despachador de sucesos:

- Actualizar la lista de despachadores de sucesos haciendo clic en el icono **Actualizar** ( ).
- Ver los detalles de un despachador de sucesos pulsando el vínculo de la columna **Nombre**.
- Cambiar las propiedades de los despachadores de sucesos y filtrar los criterios pulsando el nombre del despachador de sucesos en la columna **Nombre**.
- Eliminar el despachador de sucesos haciendo clic en el icono **Eliminar** ( ).

- Suspender el reenvío de sucesos (consulte Suspensión del reenvío de sucesos).

Configuración del reenvío de sucesos a un servicio SMTP de Gmail

Puede configurar Lenovo XClarity Administrator para reenviar sucesos supervisados a un servicio por correo electrónico en Internet, como Gmail.

Utilice los ejemplos de configuración para ayudarlo a configurar su despachador de sucesos para utilizar el servicio SMTP de Gmail.

Nota: Gmail recomienda el uso del método de autenticación OAUTH2 para una comunicación más segura. Si elige utilizar la autenticación regular, recibirá un correo electrónico que indica que una aplicación intentó utilizar su cuenta sin utilizar los últimos estándares de seguridad. El correo electrónico incluye instrucciones para configurar su cuenta de correo electrónico para aceptar estos tipos de aplicaciones.

Para obtener información detallada acerca de cómo configurar un servidor SMTP de Gmail, consulte https://support.google.com/a/answer/176600?hl=en.

Autenticación regular utilizando el SSL en el puerto 465

Este ejemplo se comunica con el servidor SMTP de Gmail usando el protocolo de SSL en el puerto 465 y se autentica utilizando una cuenta y una contraseña válidas de usuario de Gmail.

Parámetro	Valor
Host	smtp.gmail.com
Puerto	465
SSL	Seleccionar
STARTTLS	Claro
Autenticación	Regular
Usuario	Dirección de correo electrónico Gmail válida
Contraseña	Contraseña de autenticación de Gmail
Dirección Desde	(opcional)

Autenticación regular utilizando el TLS en el puerto 587

Este ejemplo se comunica con el servidor SMTP de Gmail usando el protocolo de TLS en el puerto 587 y se autentica utilizando una cuenta y una contraseña válidas de usuario de Gmail.

Parámetro	Valor
Host	smtp.gmail.com
Puerto	587
SSL	Claro
STARTTLS	Seleccionar
Autenticación	Regular
Usuario	Dirección de correo electrónico Gmail válida
Contraseña	Contraseña de autenticación de Gmail
Dirección Desde	(opcional)

Autenticación OAUTH2 utilizando el TLS en el puerto 587

Este ejemplo se comunica con el servidor SMTP de Gmail usando el protocolo de TLS en el puerto 587 y se autentica utilizando una cuenta y un token de seguridad válidos de Gmail.

Utilice el siguiente procedimiento de ejemplo para obtener el token de seguridad.

1. Cree un proyecto en la consola de desarrolladores de Google y recupere el Id. de cliente y el secreto del cliente. Para obtener más información al respecto, visite el sitio web de Página web de inicio de sesión de sitios de Google.
   a. En un navegador web, abra Página Web de API de Google.
   b. Haga clic en **Seleccionar un proyecto → Crear un proyecto** en el menú en esa página web. Se muestra el cuadro de diálogo Proyecto nuevo.
   c. Escriba un nombre, seleccione **Sí** para aceptar el acuerdo de licencia y haga clic en **Crear**.
   d. En la pestaña **Visión general**, utilice el campo de búsqueda para buscar “gmail.”
   e. Haga clic en **GMAIL API** en los resultados de búsqueda.
   f. Haga clic en **Habilitar**.
   g. Haga clic en la pestaña **Credenciales**.
   h. Haga clic en la **pantalla de consentimiento de OAuth**.
   i. Escriba un nombre en el campo de **Nombre de producto que se muestra a los usuarios** y haga clic en **Guardar**.
   j. Haga clic en **Crear credenciales → Id. de cliente de OAuth**.
   k. Seleccione **Otro** e introduzca un nombre.
   l. Haga clic en **Crear**. Se muestra el cuadro de diálogo Cliente de OAuth con su Id. de cliente y secreto del cliente.
   m. Registre el Id. de cliente y el secreto del cliente para utilizarlo en el futuro.
   n. Haga clic en **Aceptar** para cerrar el cuadro de diálogo.
2. Utilice el script Python de oauth2.py para generar y autorizar un token de seguridad ingresando el Id. de cliente y el secreto del cliente que se generaron cuando creó el proyecto.

   Nota: Se requiere Python 2.7 para completar este paso. Puede descargar e instalar Python 2.7 desde Sitio web de Python.
   a. En un navegador web, abra Página web de gmail-oauth2-tools.
   b. Haga clic en **Sin procesar** y luego guarde el contenido como nombre de archivo `oauth2.py` en el sistema local.
   c. Ejecute el mandato siguiente para un terminal (Linux) o una línea de mandatos (Windows):
   ```
   py oauth2.py --user=<your_email> --client_id=<client_id>
      --client_secret=<client_secret> --generate_oauth2_token
   ```
   Por ejemplo
   ```
   py oauth2.py --user=jon@gmail.com
      --client_id=884243132302-458elfqjiebpuvdmvdackp6elip8kl63.apps.googleusercontent.com
      --client_secret=3tnyXgEiBIbT2mOOzqnlTszk --generate_oauth2_token
   ```
   Este mandato devuelve una URL que debe usar para autorizar el token y para recuperar un código de verificación del sitio web de Google, por ejemplo:
   ```
   To authorize token, visit this url and follow the directions:

   https://accounts.google.com/o/oauth2/auth?client_id=884243132302
   -458elfqjiebpuvdmvdackp6elip8kl63.apps.googleusercontent.com&amp;redirect_uri=
   urn%3Aietf%3Awg%3Aoauth%3A2.0%3Aoob&amp;response_type=code&amp;scope=https%3A%2F%2Fmail.
   ```

```
google.com%2F

Enter verification code:
```

d. En un navegador web, abra la URL del paso anterior.

e. Haga clic en **Permitir** para aceptar este servicio. Se entrega un código de verificación.

f. Introduzca el código de la verificación en el mandato de `oauth2.py`.

El mandato devuelve el token de seguridad y restaura el token, por ejemplo:

```
Refresh Token: 1/K8lPGx6UQQajj7tQGYKq8mVG8lVvGIVzHqzxFIMeYEQMEudVrK5jSpoR3OzcRFq6
Access Token: ya29.CjHXAsyoH9GuCZutgIOxm1SGSqKrUkjIoH14SGMnljZ6rwp3gZmK7SrGDPCQx_KN-34f
Access Token Expiration Seconds: 3600
```

Importante: El token de seguridad caduca después de un período de tiempo. Puede utilizar el script Python de oauth2.py y el token de actualización para generar un nuevo token de seguridad. Es de su responsabilidad generar el nuevo token de seguridad y actualizar el despachador de sucesos en Lenovo XClarity Administrator con el nuevo token.

3. En la interfaz web de Lenovo XClarity Administrator, configure el despachador de sucesos para el correo electrónico utilizando los atributos siguientes:

Parámetro	Valor
Host	smtp.gmail.com
Puerto	587
SSL	Claro
STARTTLS	Seleccionar
Autenticación	OAUTH2
Usuario	Dirección de correo electrónico Gmail válida
Token	Token de seguridad
Dirección Desde	(opcional)

Configuración del reenvío de sucesos a un servidor FTP

Puede configurar Lenovo XClarity Administrator para que reenvíe sucesos específicos a un servidor FTP.

Acerca de esta tarea

Puede crear y habilitar hasta 20 despachadores de sucesos para enviar sucesos a destinatarios específicos.

Si XClarity Administrator se reinicia después de configurar los despachadores de sucesos, debe esperar que el servidor de gestión vuelva a generar los datos internos antes de que se puedan reenviar correctamente los sucesos.

Nota: Para la XClarity Administrator versión 1.2.0 y posteriores, **Conmutadores** se incluye en la pestaña **Sucesos** de los cuadros de diálogo Nuevo despachador de sucesos y Cambiar despachadores de sucesos. Si se actualizó a 1.2.0 o posterior a partir de una versión anterior, recuerde actualizar los despachadores de sucesos para incluir o excluir sucesos de RackSwitch, según corresponda. Esto es necesario, incluso si seleccionó la casilla de verificación **Todos los sistemas** para seleccionar todos los dispositivos.

Procedimiento

Realice los siguientes pasos para crear un despachador de sucesos para un servidor FTP.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Supervisión → Reenvío de sucesos**. Se muestra la página Reenvío de sucesos.

Paso 2. Haga clic en la pestaña **Despachador de sucesos**.

Paso 3. Haga clic en el icono **Crear** ( ). Se abre la pestaña **General** del cuadro de diálogo Nuevo despachador de sucesos.

Paso 4. Seleccione **FTP** como tipo de despachador de sucesos y rellene la información específica del protocolo:

- Escriba el nombre, el host de destino y una descripción opcional de los despachadores de sucesos.
- Especifique el puerto que se usará para reenviar sucesos. El valor predeterminado es 21.
- Especifique el período de desconexión (en segundos) para la solicitud. El valor predeterminado es 30 segundos.
- **Opcional:** Especificar la secuencia de caracteres que se extraerá del contenido.
- Ingrese el formato de nombre de archivo para usar para el archivo que contiene el suceso reenviado. El formato predeterminado es `event_[[EventSequenceID]].txt`.

  Nota: Cada archivo contiene información para un solo suceso.
- Introduzca la ruta en el servidor FTP remoto en el que se cargará del archivo.
- Elija la codificación de caracteres, **UTF-8** o **Big5**. De forma predeterminada, esto es UTF-8.
- Seleccione el tipo de autenticación. Puede presentar uno de los valores siguientes.
  - **Anónimo**. (de forma predeterminada) No se utiliza ninguna autenticación.
  - **Básico**. Se autentica en el servidor FTP usando el Id. de usuario especificado y la contraseña.

Paso 5. Haga clic en **Formato de salida** para elegir el formato de salida de los datos de sucesos que se reenviarán. La información varía según el tipo de despachadores de sucesos.

El siguiente formato de salida de ejemplo es el formato predeterminado para los destinatarios de FTP. Todas las palabras entre corchetes dobles son las variables que se sustituyen con los valores reales cuando se despacha un suceso. Las variables disponibles para los destinatarios de FTP se enumeran el cuadro de diálogo Formato de salida.

```
Alert: [[EventDate]] [[EventMessage]]\n
\n
Hardware Information:\n
Managed Endpoint    : [[DeviceHardwareType]] at [[DeviceIPAddress]]\n
Device name          : [[DeviceName]]\n
Product name         : [[DeviceProductName]]\n
Host name            : [[DeviceHostName]]\n
Machine Type         : [[DeviceMachineType]]\n
Machine Model        : [[DeviceMachineModel]]\n
Serial Number        : [[DeviceSerialNumber]]\n
DeviceHealthStatus   : [[DeviceHealthStatus]]\n
IPv4 addresses       : [[DeviceIPV4Addresses]]\n
IPv6 addresses       : [[DeviceIPV6Addresses]]\n
Chassis              : [[DeviceChassisName]]\n
DeviceBays           : [[DeviceBays]]\n
\n
LXCA is: [[ManagementServerIP]]\n
\n
Event Information:\n
  Event ID         : [[EventID]]\n
  Common Event ID : [[CommonEventID]]\n
```

```
EventSeverity   : [[EventSeverity]]\n
Event Class     : [[EventClass]]\n
Sequence ID     : [[EventSequenceID]]\n
Event Source ID : [[EventSourceUUID]]\n
Component ID    : [[EventComponentUUID]]\n
Serial Num      : [[EventSerialNumber]]\n
MTM             : [[EventMachineTypeModel]]\n
EventService    : [[EventService]]\n
Console link    : [[ConsoleLink]]\n
iOS link        : [[iOSLink]]\n
Android link    : [[AndroidLink]]\n
System Name     : [[DeviceFullPathName]]\n"
```

Puede hacer clic en **Restablecer valores predeterminados** para cambiar el formato de salida a los campos predeterminados.

Paso 6. Haga clic en el botón de alternación **Permitir sucesos excluidos** para permitir o prevenir el reenvío de sucesos excluidos.

Paso 7. Seleccione **Habilitar este despachador** para activar el reenvío de sucesos para este despachador de sucesos.

Paso 8. Pulse **Siguiente** para mostrar la pestaña **Dispositivos**.

Paso 9. Seleccione los dispositivos y grupos que desee supervisar para este despachador de sucesos.

Consejo Para reenviar sucesos de todos los dispositivos gestionados (actuales y futuros), seleccione la casilla de verificación **Igualar todos los sistemas**.Si no selecciona la casilla **Igualar todos los sistemas**, asegúrese de que los dispositivos seleccionados no tengan un DUMMY-UUID en la columna UUID. Se asigna un Dummy-UUID a los dispositivos que aún no se recuperan después de un reinicio o no han sido detectados completamente por el servidor de gestión. Si selecciona un dispositivo con un Dummy-UUID, el reenvío de sucesos no funcionará para este dispositivo hasta que el dispositivo sea completamente detectado o recuperado y el Dummy-UUID cambie a su UUID real.

Paso 10. Haga clic en **Siguiente** para mostrar la pestaña **Sucesos**.

Paso 11. Seleccione los filtros que se utilizarán para este despachador de sucesos.

- **Coincidir por categorías de sucesos**.
  1. Para reenviar todos los sucesos de auditoría, sin importar el nivel de estado, seleccione **Incluir todos los sucesos de auditoría**.
  2. Para reenviar todos los sucesos de garantía, seleccione la opción **Incluir los sucesos de garantía**.
  3. Para volver a enviar todos los sucesos de cambio de estado y salud, seleccione **Incluir los sucesos de cambio de estado**.
  4. Para volver a enviar todos los sucesos de actualización de estado y salud, seleccione **Incluir los sucesos de actualización de estado**.
  5. Seleccione las clases de sucesos y niveles de capacidad de servicio que desee reenviar.
  6. Introduzca el Id. de uno o varios sucesos que desea excluir de reenvío. Separe los identificadores utilizando una coma (por ejemplo, `FQXHMEM0214I,FQXHMEM0214I`).
- **Coincidir por el código de suceso**. Introduzca el Id. de uno o varios sucesos que desee reenviar. Separe los identificadores entre sí mediante comas.
- **Excluir por categorías de sucesos**.
  1. Para excluir todos los sucesos de auditoría, sin importar el nivel de estado, seleccione **Excluir todos los sucesos de auditoría**.

2. Para excluir todos los sucesos de garantía, seleccione la opción **Excluir los sucesos de garantía**.
3. Para excluir todos los sucesos de cambio de estado y salud, seleccione **Excluir los sucesos de cambio de estado**.
4. Para excluir todos los sucesos de actualización de estado y salud, seleccione **Excluir los sucesos de actualización de estado**.
5. Seleccione las clases de sucesos y niveles de capacidad de servicio que desee excluir.
6. Introduzca el Id. de uno o varios sucesos que desee reenviar. Separe los identificadores utilizando una coma.

- **Excluir por el código de suceso**. Introduzca el Id. de uno o varios sucesos que desee excluir. Separe los identificadores entre sí mediante comas.

Paso 12. Elija si se deben incluir determinados tipos de sucesos.

- **Incluir todos los sucesos de auditoría**. Envía notificaciones sobre sucesos de auditoría, según las clases y gravedades de los sucesos seleccionados.
- **Incluir sucesos de garantía**. Enviar notificaciones sobre garantías.
- **Incluye sucesos de cambio de estado**. Envía notificaciones sobre cambios de estado.
- **Incluye sucesos de actualización de estado**. Se enviaron notificaciones sobre nuevas alertas.
- **Incluir sucesos del boletín**. Envía notificaciones sobre boletines nuevos.

Paso 13. Seleccione los tipos de sucesos y niveles de gravedad por los que desea que se le notifique.

Paso 14. Seleccione si se deben filtrar sucesos por capacidad de servicio.

Paso 15. Haga clic en **Siguiente** para mostrar la pestaña **Programador**.

Paso 16. **Opcional:** defina las horas y los días en los que desea que se reenvíen sucesos específicos a este despachador de sucesos. Solo se reenvían los sucesos que se producen durante el periodo de tiempo especificado.

Si no crea una planificación para el despachador de sucesos, los sucesos se reenviarán las 24 horas del día, 7 días a la semana.

1. Use el icono **Desplazar a la izquierda** (◀) y el icono **Desplazar a la derecha** (▶) y los botones **Día**, **Semana** y **Mes** para determinar el día y la hora a la que desea que comience la planificación.
2. Haga clic en dos veces la hora para abrir el cuadro de diálogo Nuevo periodo de tiempo.
3. Complete la información requerida, incluida la fecha, horas de inicio y término y si desea que se repita la programación.
4. Haga clic en **Crear** para guardar la planificación y cerrar el cuadro de diálogo. La nueva planificación se añade al calendario.

Consejo:
- Puede cambiar la hora arrastrando la entrada de programación hacia otra hora en el calendario.
- Puede cambiar la duración al seleccionar la parte superior o inferior de la entrada de programación y arrastrarla hacia la nueva hora en el calendario.
- Puede cambiar la hora de término al seleccionar la parte inferior de la entrada de programación y arrastrarla hacia la nueva hora en el calendario.
- Puede cambiar la programación al pulsar dos veces la entrada de programación en el calendario y pulsar **Editar entrada**.
- Se puede visualizar un resumen de todas las entradas de programación al seleccionar **Mostrar resumen del planificador**. El resumen incluye los espacios de tiempo de cada entrada y las entradas que se repiten.

- Puede eliminar una entrada de programación del calendario o resumen de programador seleccionando la entrada y haciendo clic en **Eliminar entrada**.

Paso 17. Haga clic en **Crear**.

El despachador de sucesos aparecerá en la tabla Reenvío de sucesos.

Paso 18. Seleccione el nuevo despachador de sucesos, haga clic en **Generar suceso de prueba** y luego compruebe que el reenvío de sucesos se realice correctamente al servidor de FTP correspondiente.

Después de finalizar

Desde la página Reenvío de sucesos, también puede realizar las acciones siguientes en un despachador de sucesos:

- Actualizar la lista de despachadores de sucesos haciendo clic en el icono **Actualizar** ( ).
- Ver los detalles de un despachador de sucesos pulsando el vínculo de la columna **Nombre**.
- Cambiar las propiedades de los despachadores de sucesos y filtrar los criterios pulsando el nombre del despachador de sucesos en la columna **Nombre**.
- Eliminar el despachador de sucesos haciendo clic en el icono **Eliminar** ( ).
- Suspender el reenvío de sucesos (consulte Suspensión del reenvío de sucesos).

Configuración del reenvío de sucesos a un servicio web REST

Puede configurar Lenovo XClarity Administrator para que reenvíe sucesos específicos a un servidor web REST.

Acerca de esta tarea

Puede crear y habilitar hasta 20 despachadores de sucesos para enviar sucesos a destinatarios específicos.

Si XClarity Administrator se reinicia después de configurar los despachadores de sucesos, debe esperar que el servidor de gestión vuelva a generar los datos internos antes de que se puedan reenviar correctamente los sucesos.

Nota: Para la XClarity Administrator versión 1.2.0 y posteriores, **Conmutadores** se incluye en la pestaña **Sucesos** de los cuadros de diálogo Nuevo despachador de sucesos y Cambiar despachadores de sucesos. Si se actualizó a 1.2.0 o posterior a partir de una versión anterior, recuerde actualizar los despachadores de

sucesos para incluir o excluir sucesos de RackSwitch, según corresponda. Esto es necesario, incluso si seleccionó la casilla de verificación **Todos los sistemas** para seleccionar todos los dispositivos.

Procedimiento

Realice los siguientes pasos para crear un despachador de sucesos para un servidor web REST.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Supervisión → Reenvío de sucesos**. Se muestra la página Reenvío de sucesos.

Paso 2. Haga clic en la pestaña **Despachador de sucesos**.

Paso 3. Haga clic en el icono **Crear** ( ). Se abre la pestaña **General** del cuadro de diálogo Nuevo despachador de sucesos.

Paso 4. Seleccione **REST** como tipo de despachador de sucesos y rellene la información específica del protocolo:

- Ingrese la ruta de acceso de recursos en el que el reenviador publicará los sucesos (por ejemplo, /rest/test).
- Seleccione el protocolo que se utilizará para reenviar sucesos. Puede presentar uno de los valores siguientes.
  - **HTTP**
  - **HTTPS**
- Seleccione el método REST. Puede presentar uno de los valores siguientes.
  - **PUT**
  - **POST**
- Especifique el período de desconexión (en segundos) para la solicitud. El valor predeterminado es 30 segundos.
- **Opcional:** si se requiere autenticación, seleccione uno de los siguientes tipos de autenticación:
  - **Básico**. Se autentica en el servidor especificado usando el Id. de usuario especificado y la contraseña.
  - **Ninguno**. No se utiliza ninguna autenticación.

Paso 5. Haga clic en **Formato de salida** para elegir el formato de salida de los datos de sucesos que se reenviarán. La información varía según el tipo de despachador de sucesos.

El siguiente formato de salida de ejemplo es el formato predeterminado para los destinatarios de servicio web REST. Todas las palabras entre corchetes dobles son las variables que se sustituyen con los valores reales cuando se despacha un suceso. Las variables disponibles para los destinatarios del servicio web REST se enumeran el cuadro de diálogo Formato de salida.

```
{\"msg\":\"[[EventMessage]]\",\"eventID\":\"[[EventID]]\",\"serialnum\":
\"[[EventSerialNumber]]\",\"senderUUID\":\"[[EventSenderUUID]]\",\"flags\":
\"[[EventFlags]]\",\"userid\":\"[[EventUserName]]\",\"localLogID\":
\"[[EventLocalLogID]]\",\"systemName\":\"[[DeviceFullPathName]]\",\"action\":
[[EventActionNumber]],\"failFRUNumbers\":\"[[EventFailFRUs]]\",\"severity\":
[[EventSeverityNumber]],\"sourceID\":\"[[EventSourceUUID]]\",
\"sourceLogSequence\":[[EventSourceLogSequenceNumber]],\"failFRUSNs\":
\"[[EventFailSerialNumbers]]\",\"failFRUUUIDs\":\"[[EventFailFRUUUIDs]]\",
\"eventClass\":[[EventClassNumber]],\"componentID\":\"[[EventComponentUUID]]\",
\"mtm\":\"[[EventMachineTypeModel]]\",\"msgID\":\"[[EventMessageID]]\",
"sequenceNumber\":\"[[EventSequenceID]]\",\"timeStamp\":\"[[EventTimeStamp]]\",
\"args\":[[EventMessageArguments]],\"service\":[[EventServiceNumber]],
\"commonEventID\":\"[[CommonEventID]]\",\"eventDate\":\"[[EventDate]]\"}"
```

Puede hacer clic en **Restablecer valores predeterminados** para cambiar el formato de salida a los campos predeterminados.

Paso 6. Haga clic en el botón de alternación **Permitir sucesos excluidos** para permitir o prevenir el reenvío de sucesos excluidos.

Paso 7. Seleccione **Habilitar este despachador** para activar el reenvío de sucesos para este despachador de sucesos.

Paso 8. Pulse **Siguiente** para mostrar la pestaña **Dispositivos**.

Paso 9. Seleccione los dispositivos y grupos que desee supervisar para este despachador de sucesos.

Consejo Para reenviar sucesos de todos los dispositivos gestionados (actuales y futuros), seleccione la casilla de verificación **Igualar todos los sistemas**.Si no selecciona la casilla **Igualar todos los sistemas**, asegúrese de que los dispositivos seleccionados no tengan un DUMMY-UUID en la columna UUID. Se asigna un Dummy-UUID a los dispositivos que aún no se recuperan después de un reinicio o no han sido detectados completamente por el servidor de gestión. Si selecciona un dispositivo con un Dummy-UUID, el reenvío de sucesos no funcionará para este dispositivo hasta que el dispositivo sea completamente detectado o recuperado y el Dummy-UUID cambie a su UUID real.

Paso 10. Haga clic en **Siguiente** para mostrar la pestaña **Sucesos**.

Paso 11. Seleccione los filtros que se utilizarán para este despachador de sucesos.

- **Coincidir por categorías de sucesos**.
  1. Para reenviar todos los sucesos de auditoría, sin importar el nivel de estado, seleccione **Incluir todos los sucesos de auditoría**.
  2. Para reenviar todos los sucesos de garantía, seleccione la opción **Incluir los sucesos de garantía**.
  3. Para volver a enviar todos los sucesos de cambio de estado y salud, seleccione **Incluir los sucesos de cambio de estado**.
  4. Para volver a enviar todos los sucesos de actualización de estado y salud, seleccione **Incluir los sucesos de actualización de estado**.
  5. Seleccione las clases de sucesos y niveles de capacidad de servicio que desee reenviar.
  6. Introduzca el Id. de uno o varios sucesos que desea excluir de reenvío. Separe los identificadores utilizando una coma (por ejemplo, `FQXHMEM0214I,FQXHMEM0214I`).
- **Coincidir por el código de suceso**. Introduzca el Id. de uno o varios sucesos que desee reenviar. Separe los identificadores entre sí mediante comas.
- **Excluir por categorías de sucesos**.
  1. Para excluir todos los sucesos de auditoría, sin importar el nivel de estado, seleccione **Excluir todos los sucesos de auditoría**.
  2. Para excluir todos los sucesos de garantía, seleccione la opción **Excluir los sucesos de garantía**.
  3. Para excluir todos los sucesos de cambio de estado y salud, seleccione **Excluir los sucesos de cambio de estado**.
  4. Para excluir todos los sucesos de actualización de estado y salud, seleccione **Excluir los sucesos de actualización de estado**.
  5. Seleccione las clases de sucesos y niveles de capacidad de servicio que desee excluir.
  6. Introduzca el Id. de uno o varios sucesos que desee reenviar. Separe los identificadores utilizando una coma.
- **Excluir por el código de suceso**. Introduzca el Id. de uno o varios sucesos que desee excluir. Separe los identificadores entre sí mediante comas.

Paso 12. Elija si se deben incluir determinados tipos de sucesos.

- **Incluir todos los sucesos de auditoría**. Envía notificaciones sobre sucesos de auditoría, según las clases y gravedades de los sucesos seleccionados.
- **Incluir sucesos de garantía**. Enviar notificaciones sobre garantías.
- **Incluye sucesos de cambio de estado**. Envía notificaciones sobre cambios de estado.
- **Incluye sucesos de actualización de estado**. Se enviaron notificaciones sobre nuevas alertas.
- **Incluir sucesos del boletín**. Envía notificaciones sobre boletines nuevos.

Paso 13. Seleccione los tipos de sucesos y niveles de gravedad por los que desea que se le notifique.

Paso 14. Seleccione si se deben filtrar sucesos por capacidad de servicio.

Paso 15. Haga clic en **Siguiente** para mostrar la pestaña **Programador**.

Paso 16. **Opcional:** defina las horas y los días en los que desea que se reenvíen sucesos específicos a este despachador de sucesos. Solo se reenvían los sucesos que se producen durante el periodo de tiempo especificado.

Si no crea una planificación para el despachador de sucesos, los sucesos se reenviarán las 24 horas del día, 7 días a la semana.

1. Use el icono **Desplazar a la izquierda** (◀) y el icono **Desplazar a la derecha** (▶) y los botones **Día**, **Semana** y **Mes** para determinar el día y la hora a la que desea que comience la planificación.
2. Haga clic en dos veces la hora para abrir el cuadro de diálogo Nuevo periodo de tiempo.
3. Complete la información requerida, incluida la fecha, horas de inicio y término y si desea que se repita la programación.
4. Haga clic en **Crear** para guardar la planificación y cerrar el cuadro de diálogo. La nueva planificación se añade al calendario.

Consejo:
- Puede cambiar la hora arrastrando la entrada de programación hacia otra hora en el calendario.
- Puede cambiar la duración al seleccionar la parte superior o inferior de la entrada de programación y arrastrarla hacia la nueva hora en el calendario.
- Puede cambiar la hora de término al seleccionar la parte inferior de la entrada de programación y arrastrarla hacia la nueva hora en el calendario.
- Puede cambiar la programación al pulsar dos veces la entrada de programación en el calendario y pulsar **Editar entrada**.
- Se puede visualizar un resumen de todas las entradas de programación al seleccionar **Mostrar resumen del planificador**. El resumen incluye los espacios de tiempo de cada entrada y las entradas que se repiten.
- Puede eliminar una entrada de programación del calendario o resumen de programador seleccionando la entrada y haciendo clic en **Eliminar entrada**.

Paso 17. Haga clic en **Crear**.

El despachador de sucesos aparecerá en la tabla Reenvío de sucesos.

Paso 18. Seleccione el nuevo despachador de sucesos, haga clic en **Generar suceso de prueba** y luego compruebe que el reenvío de sucesos se realice correctamente al servicio web REST correspondiente.

Después de finalizar

Desde la página Reenvío de sucesos, también puede realizar las acciones siguientes en un despachador de sucesos:

- Actualizar la lista de despachadores de sucesos haciendo clic en el icono **Actualizar** ( ).
- Ver los detalles de un despachador de sucesos pulsando el vínculo de la columna **Nombre**.
- Cambiar las propiedades de los despachadores de sucesos y filtrar los criterios pulsando el nombre del despachador de sucesos en la columna **Nombre**.
- Eliminar el despachador de sucesos haciendo clic en el icono **Eliminar** ( ).
- Suspender el reenvío de sucesos (consulte Suspensión del reenvío de sucesos).

Configurar el reenvío de sucesos en un gestor SNMPv1 o SNMPv3 remoto

Puede configurar Lenovo XClarity Administrator para reenviar sucesos específicos a un gestor de SNMPv1 o SNMPv3 remoto.

Acerca de esta tarea

Puede crear y habilitar hasta 20 despachadores de sucesos para enviar sucesos a destinatarios específicos.

Si XClarity Administrator se reinicia después de configurar los despachadores de sucesos, debe esperar que el servidor de gestión vuelva a generar los datos internos antes de que se puedan reenviar correctamente los sucesos.

Nota: Para la XClarity Administrator versión 1.2.0 y posteriores, **Conmutadores** se incluye en la pestaña **Sucesos** de los cuadros de diálogo Nuevo despachador de sucesos y Cambiar despachadores de sucesos. Si se actualizó a 1.2.0 o posterior a partir de una versión anterior, recuerde actualizar los despachadores de sucesos para incluir o excluir sucesos de RackSwitch, según corresponda. Esto es necesario, incluso si seleccionó la casilla de verificación **Todos los sistemas** para seleccionar todos los dispositivos.

Para obtener información sobre la MIB de XClarity Administrator, consulte Archivo lenovoMgrAlert.mib.

Procedimiento

Lleve a cabo los pasos siguientes para crear un despachador de sucesos para un gestor SNMPv1 o SNMPv3 remoto.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Supervisión → Reenvío de sucesos**. Se muestra la página Reenvío de sucesos.

Paso 2. Haga clic en la pestaña **Despachador de sucesos**.

Paso 3. Haga clic en el icono **Crear** ( ). Se abre la pestaña **General** del cuadro de diálogo Nuevo despachador de sucesos.

Paso 4. Seleccione **SNMPv1** o **SNMPv3** como tipo de despachador de sucesos y rellene la información específica del protocolo:

- Escriba el nombre y el host de destino del despachador de sucesos.
- Especifique el puerto que se usará para reenviar sucesos. El valor predeterminado es `162`.
- **Opcional:** ingrese información adicional, incluida la descripción, el nombre de contacto y la ubicación.
- Seleccione la versión de SNMP. Puede presentar uno de los valores siguientes.
  - **SNMPv1**. Si se selecciona esta versión, especifique la contraseña de la comunidad que se envía con cada solicitud de SNMP al dispositivo.
  - **SNMPv3**. Esta es la versión predeterminada y se recomienda para una seguridad mejorada. Si se selecciona SNMPv3, especifique opcionalmente el Id. de usuario, el tipo y la contraseña de autenticación y el tipo y la contraseña de privacidad.

    Si el receptor de capturas de SNMPv3 requiere el Id. de motor para la instancia de XClarity Administrator, puede encontrar el Id. de motor realizando los pasos siguientes:

    1. Asegúrese de que los parámetros de conexión (nombre de usuario, authProtocol, authPassword, privProtocol, privPassword) coincidan con los que se fijaron en XClarity Administrator.
    2. Con el software preferido (como snmpwalk), realice una petición SNMP GET en el servidor de XClarity Administrator utilizando uno de los OID siguientes:
       - EngineID: 1.3.6.1.6.3.10.2.1.1.0
       - EngineBoots : 1.3.6.1.6.3.10.2.1.2.0

       Utilice la siguiente sintaxis para el comando `snmpget`. Tenga en cuenta que el tipo de autenticación -a de reenvío puede ser SHA o en blanco (sin autenticación).
       ```
       snmpget -v 3 -u <FORWARDER_USER_ID> -l authPriv -a <FORWARDER_AUTH_TYPE> -A <FORWARDER
       ```

       Por ejemplo, si la dirección IP de XClarity Administrator es 192.0.1.0, el tipo de autenticación es SHA y el tipo de privacidad es AES, el siguiente comando muestra el ID del motor.
       ```
       snmpget -v 3 -u someUserID -l authPriv -a SHA -A someUserIDPassword_1 -x AES -X somePrivacyPassword_
       ```

       Se arroja el siguiente mensaje de ejemplo. En este ejemplo, el ID de motor es 0x80001370017F00000134C27E12.
       ```
       iso.3.6.1.6.3.10.2.1.1.0 = Hex-STRING: 80 00 13 70 01 7F 00 00 01 34 C2 7E 12
       ```
- Especifique el período de desconexión (en segundos) para la solicitud. El valor predeterminado es 30 segundos.
- **Opcional**: si es necesaria la autenticación de la captura, introduzca la contraseña del Id. del usuario y la contraseña de autenticación. Debe introducirse el mismo Id. de usuario y contraseña en el gestor de SNMP remoto al que se reenvían las capturas.
- Seleccione el protocolo de autenticación que utilizará el gestor de SNMP remoto para verificar el emisor de capturas. Puede presentar uno de los valores siguientes
  - **SHA**. Usa el protocolo SHA para autenticar al servidor SNMP específico usando el Id. de usuario, la contraseña y el nombre de dominio especificados.

  - **Ninguno**. No se utiliza ninguna autenticación
- Si es necesaria la captura de cifrado, introduzca el tipo de privacidad (protocolo de cifrado) y la contraseña. Puede presentar uno de los valores siguientes. Debe introducirse el mismo protocolo y contraseña en el gestor de SNMP remoto al que se reenvían las capturas.
  - **AES**
  - **DES**
  - **Ninguno**

Paso 5. Haga clic en el botón de alternación **Permitir sucesos excluidos** para permitir o prevenir el reenvío de sucesos excluidos.

Paso 6. Seleccione **Habilitar este despachador** para activar el reenvío de sucesos para este despachador de sucesos.

Paso 7. Pulse **Siguiente** para mostrar la pestaña **Dispositivos**.

Paso 8. Seleccione los dispositivos y grupos que desee supervisar para este despachador de sucesos.

Consejo Para reenviar sucesos de todos los dispositivos gestionados (actuales y futuros), seleccione la casilla de verificación **Igualar todos los sistemas**.Si no selecciona la casilla **Igualar todos los sistemas**, asegúrese de que los dispositivos seleccionados no tengan un DUMMY-UUID en la columna UUID. Se asigna un Dummy-UUID a los dispositivos que aún no se recuperan después de un reinicio o no han sido detectados completamente por el servidor de gestión. Si selecciona un dispositivo con un Dummy-UUID, el reenvío de sucesos no funcionará para este dispositivo hasta que el dispositivo sea completamente detectado o recuperado y el Dummy-UUID cambie a su UUID real.

Paso 9. Haga clic en **Siguiente** para mostrar la pestaña **Sucesos**.

Paso 10. Seleccione los filtros que se utilizarán para este despachador de sucesos.

- **Coincidir por categorías de sucesos**.
  1. Para reenviar todos los sucesos de auditoría, sin importar el nivel de estado, seleccione **Incluir todos los sucesos de auditoría**.
  2. Para reenviar todos los sucesos de garantía, seleccione la opción **Incluir los sucesos de garantía**.
  3. Para volver a enviar todos los sucesos de cambio de estado y salud, seleccione **Incluir los sucesos de cambio de estado**.
  4. Para volver a enviar todos los sucesos de actualización de estado y salud, seleccione **Incluir los sucesos de actualización de estado**.
  5. Seleccione las clases de sucesos y niveles de capacidad de servicio que desee reenviar.
  6. Introduzca el Id. de uno o varios sucesos que desea excluir de reenvío. Separe los identificadores utilizando una coma (por ejemplo, `FQXHMEM0214I,FQXHMEM0214I`).
- **Coincidir por el código de suceso**. Introduzca el Id. de uno o varios sucesos que desee reenviar. Separe los identificadores entre sí mediante comas.
- **Excluir por categorías de sucesos**.
  1. Para excluir todos los sucesos de auditoría, sin importar el nivel de estado, seleccione **Excluir todos los sucesos de auditoría**.
  2. Para excluir todos los sucesos de garantía, seleccione la opción **Excluir los sucesos de garantía**.
  3. Para excluir todos los sucesos de cambio de estado y salud, seleccione **Excluir los sucesos de cambio de estado**.
  4. Para excluir todos los sucesos de actualización de estado y salud, seleccione **Excluir los sucesos de actualización de estado**.

5. Seleccione las clases de sucesos y niveles de capacidad de servicio que desee excluir.
6. Introduzca el Id. de uno o varios sucesos que desee reenviar. Separe los identificadores utilizando una coma.

- **Excluir por el código de suceso**. Introduzca el Id. de uno o varios sucesos que desee excluir. Separe los identificadores entre sí mediante comas.

Paso 11. Elija si se deben incluir determinados tipos de sucesos.

- **Incluir todos los sucesos de auditoría**. Envía notificaciones sobre sucesos de auditoría, según las clases y gravedades de los sucesos seleccionados.
- **Incluir sucesos de garantía**. Enviar notificaciones sobre garantías.
- **Incluye sucesos de cambio de estado**. Envía notificaciones sobre cambios de estado.
- **Incluye sucesos de actualización de estado**. Se enviaron notificaciones sobre nuevas alertas.
- **Incluir sucesos del boletín**. Envía notificaciones sobre boletines nuevos.

Paso 12. Seleccione los tipos de sucesos y niveles de gravedad por los que desea que se le notifique.

Paso 13. Seleccione si se deben filtrar sucesos por capacidad de servicio.

Paso 14. Haga clic en **Siguiente** para mostrar la pestaña **Programador**.

Paso 15. **Opcional:** defina las horas y los días en los que desea que se reenvíen sucesos específicos a este despachador de sucesos. Solo se reenvían los sucesos que se producen durante el periodo de tiempo especificado.

Si no crea una planificación para el despachador de sucesos, los sucesos se reenviarán las 24 horas del día, 7 días a la semana.

1. Use el icono **Desplazar a la izquierda** (◀) y el icono **Desplazar a la derecha** (▶) y los botones **Día**, **Semana** y **Mes** para determinar el día y la hora a la que desea que comience la planificación.
2. Haga clic en dos veces la hora para abrir el cuadro de diálogo Nuevo periodo de tiempo.
3. Complete la información requerida, incluida la fecha, horas de inicio y término y si desea que se repita la programación.
4. Haga clic en **Crear** para guardar la planificación y cerrar el cuadro de diálogo. La nueva planificación se añade al calendario.

Consejo:
- Puede cambiar la hora arrastrando la entrada de programación hacia otra hora en el calendario.
- Puede cambiar la duración al seleccionar la parte superior o inferior de la entrada de programación y arrastrarla hacia la nueva hora en el calendario.
- Puede cambiar la hora de término al seleccionar la parte inferior de la entrada de programación y arrastrarla hacia la nueva hora en el calendario.
- Puede cambiar la programación al pulsar dos veces la entrada de programación en el calendario y pulsar **Editar entrada**.
- Se puede visualizar un resumen de todas las entradas de programación al seleccionar **Mostrar resumen del planificador**. El resumen incluye los espacios de tiempo de cada entrada y las entradas que se repiten.
- Puede eliminar una entrada de programación del calendario o resumen de programador seleccionando la entrada y haciendo clic en **Eliminar entrada**.

Paso 16. Haga clic en **Crear**.

El despachador de sucesos aparecerá en la tabla Reenvío de sucesos.

Paso 17. Seleccione el nuevo despachador de sucesos, haga clic en **Generar suceso de prueba** y luego compruebe que el reenvío de sucesos se realice correctamente al gestor de SNMP correspondiente.

Después de finalizar

Desde la página Reenvío de sucesos, también puede realizar las acciones siguientes en un despachador de sucesos:

- Actualizar la lista de despachadores de sucesos haciendo clic en el icono **Actualizar** ( ).
- Ver los detalles de un despachador de sucesos pulsando el vínculo de la columna **Nombre**.
- Cambiar las propiedades de los despachadores de sucesos y filtrar los criterios pulsando el nombre del despachador de sucesos en la columna **Nombre**.
- Eliminar el despachador de sucesos haciendo clic en el icono **Eliminar** ( ).
- Suspender el reenvío de sucesos (consulte Suspensión del reenvío de sucesos).
- Para descargar el archivo MIB que contiene información acerca de las capturas de SNMP, haga clic en el icono **Crear** ( ) y luego haga clic en **Descargar archivo MIB** en la pestaña General del cuadro de diálogo nuevo reenvío de sucesos

Archivo lenovoMgrAlert.mib
Este archivo base de información de gestión (MIB) describe las capturas de SNMP que genera Lenovo XClarity Administrator, incluidas las alertas que han sido generadas por XClarity Administrator y los dispositivos gestionados. Puede compilar este archivo MIB en cualquier gestor de capturas de SNMP, de manera que las capturas de SNMP enviadas desde XClarity Administrator puedan reproducirse de forma adecuada.

Puede descargar el archivo MIB desde la interfaz web al hacer clic en **Supervisión → Reenvío de sucesos** desde la barra de menú, luego el icono **Crear** ( ), seleccionando **SNMP** para el tipo de despachador de sucesos y luego **Descargar archivo MIB** en la parte inferior del cuadro de diálogo.

Los objetos siguientes se incluyen en todas las capturas de SNMP salientes. También es posible incluir objetos adicionales en algunas capturas de SNMP. Todos los objetos están descritos en el archivo MIB. Tenga en cuenta que la información de recuperación no está incluida en la captura.

Nota: Esta lista puede variar de una versión de XClarity Administrator a otra.
- **mgrTrapAppId**. Esto es “Lenovo Event Manager”.

- **mgrTrapCommonEvtID**. ID de suceso común
- **mgrTrapDateTime**. Fecha y hora local en la que se ha producido el suceso
- **mgrTrapEventClass**. Origen del suceso. Esto puede ser auditoría, refrigeración, alimentación, discos, memoria, procesadores, sistema, prueba, adaptador, expansión, IOModule o blade.
- **mgrTrapEvtID**. El identificador único del suceso
- **mgrTrapFailFRUs**. Una lista separada por comas de los UUID de FRU con problemas, si corresponde
- **mgrTrapFailSNs**. Una lista separada por comas de los números de serie de las FRU con problemas, si corresponde.
- **mgrTrapFullyQualifiedDomainName**. Nombre de dominio completamente calificado: nombre de host y nombre de dominio
- **mgrTrapID**. Id. de la interrupción
- **mgrTrapMsgText**. Texto del mensaje (solo en inglés)
- **mgrTrapMsgID**. Identificador de mensaje
- **mgrTrapMtm**. Modelo de tipo de modelo del dispositivo que ha producido el suceso
- **mgrTrapService**. Indicador de capacidad de servicio. Esto puede ser 000 (desconocido), 100 (ninguno), 200 (centro de servicio) o 300 (cliente)
- **mgrTrapSeverity**. Indicador de gravedad. Esto puede ser Informativo, Advertencia, Menor, Importante o Crítico
- **mgrTrapSN**. Número de serie del dispositivo que ha producido el suceso
- **mgrTrapSrcIP**. Dirección IP del dispositivo desde el que se recibió el suceso que se presentó
- **mgrTrapSrcLoc**. Ubicación del dispositivo que ha producido el suceso, solo en inglés (por ejemplo, Ranura n.º xx)
- **mgrTrapSrcName**. Nombre de host o pantalla del dispositivo que ha producido el suceso
- **mgrTrapSysContact**. Id. de contacto configurado por el usuario
- **mgrTrapSysLocation**. Información de ubicación del dispositivo configurada por el usuario
- **mgrTrapSystemName**. Nombre del dispositivo, nombre del componente y ubicación de ranura
- **mgrTrapTxtId**. Nombre de host o dirección IP del servidor de Lenovo Event Manager que ha levantado la trampa
- **mgrTrapUserid**. Id. de usuario que está asociado con el suceso (si el suceso es interno y la clase de suceso es Auditoría)
- **mgrTrapUuid**. UUID del dispositivo que ha producido el suceso

Configuración del reenvío de sucesos a un syslog

Puede configurar Lenovo XClarity Administrator para que reenvíe sucesos específicos a un syslog.

Acerca de esta tarea

Puede crear y habilitar hasta 20 despachadores de sucesos para enviar sucesos a destinatarios específicos.

Si XClarity Administrator se reinicia después de configurar los despachadores de sucesos, debe esperar que el servidor de gestión vuelva a generar los datos internos antes de que se puedan reenviar correctamente los sucesos.

Nota: Para la XClarity Administrator versión 1.2.0 y posteriores, **Conmutadores** se incluye en la pestaña **Sucesos** de los cuadros de diálogo Nuevo despachador de sucesos y Cambiar despachadores de sucesos. Si se actualizó a 1.2.0 o posterior a partir de una versión anterior, recuerde actualizar los despachadores de sucesos para incluir o excluir sucesos de RackSwitch, según corresponda. Esto es necesario, incluso si seleccionó la casilla de verificación **Todos los sistemas** para seleccionar todos los dispositivos.

Procedimiento

Realice los siguientes pasos para crear un despachador de sucesos para un syslog.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Supervisión → Reenvío de sucesos**. Se muestra la página Reenvío de sucesos.

Paso 2. Haga clic en la pestaña **Despachador de sucesos**.

Paso 3. Haga clic en el icono **Crear** ( ). Se abre la pestaña **General** del cuadro de diálogo Nuevo despachador de sucesos.

Paso 4. Seleccione **Syslog** como tipo de despachador de sucesos y rellene la información específica del protocolo:

- Escriba el nombre, el host de destino y una descripción opcional del despachador de sucesos.
- Especifique el puerto que se usará para reenviar sucesos. El valor predeterminado es `514`.
- Seleccione el protocolo que se utilizará para reenviar sucesos. Puede presentar uno de los valores siguientes.
  - **UDP**
  - **TCP**
- Especifique el período de desconexión (en segundos) para la solicitud. El valor predeterminado es 30 segundos.
- Opcionalmente, seleccione el formato de la marca de tiempo en syslog. Puede presentar uno de los valores siguientes.
  - **Hora local**. El formato predeterminado, por ejemplo `Fri Mar 31 05:57:18 EDT 2017`.
  - **Hora GMT**. Estándar internacional (ISO8601) de fechas y horas, por ejemplo `2017-03-31T05:58:20-04:00`.

Paso 5. Haga clic en **Formato de salida** para elegir el formato de salida de los datos de sucesos que se reenviarán. La información varía según el tipo de despachador de sucesos.

El siguiente formato de salida de ejemplo es el formato predeterminado para los destinatarios de sylog. Todas las palabras entre corchetes dobles son las variables que se sustituyen con los valores reales cuando se despacha un suceso. Las variables disponibles para los destinatarios de sylog se enumeran el cuadro de diálogo Formato de salida.

```
<8[[SysLogSeverity]]> [[EventTimeStamp]] [appl=LXCA service=[[EventService]] severity=[[EventSeverity]]
class=[[EventClass]] appladdr=[[LXCA_IP]] user=[[EventUserName]] src=[[SysLogSource]] uuid=[[UUID]]
me=[[DeviceSerialNumber]] resourceIP=[[DeviceIPAddress]] systemName=[[DeviceFullPathName]]
seq=[[EventSequenceID]] EventID=[[EventID]] CommonEventID=[[CommonEventID]]
```

Puede hacer clic en **Restablecer valores predeterminados** para cambiar el formato de salida a los campos predeterminados.

Paso 6. Haga clic en el botón de alternación **Permitir sucesos excluidos** para permitir o prevenir el reenvío de sucesos excluidos.

Paso 7. Seleccione **Habilitar este despachador** para activar el reenvío de sucesos para este despachador de sucesos.

Paso 8. Pulse **Siguiente** para mostrar la pestaña **Dispositivos**.

Paso 9. Seleccione los dispositivos y grupos que desee supervisar para este despachador de sucesos.

Consejo Para reenviar sucesos de todos los dispositivos gestionados (actuales y futuros), seleccione la casilla de verificación **Igualar todos los sistemas**.Si no selecciona la casilla **Igualar todos los sistemas**, asegúrese de que los dispositivos seleccionados no tengan un DUMMY-UUID en la columna UUID. Se asigna un Dummy-UUID a los dispositivos que aún no se recuperan después de un reinicio o no han sido detectados completamente por el servidor de gestión. Si selecciona un dispositivo con un Dummy-UUID, el reenvío de sucesos no funcionará para este dispositivo hasta que el dispositivo sea completamente detectado o recuperado y el Dummy-UUID cambie a su UUID real.

Paso 10. Haga clic en **Siguiente** para mostrar la pestaña **Sucesos**.

Paso 11. Seleccione los filtros que se utilizarán para este despachador de sucesos.

- **Coincidir por categorías de sucesos**.
  1. Para reenviar todos los sucesos de auditoría, sin importar el nivel de estado, seleccione **Incluir todos los sucesos de auditoría**.
  2. Para reenviar todos los sucesos de garantía, seleccione la opción **Incluir los sucesos de garantía**.
  3. Para volver a enviar todos los sucesos de cambio de estado y salud, seleccione **Incluir los sucesos de cambio de estado**.
  4. Para volver a enviar todos los sucesos de actualización de estado y salud, seleccione **Incluir los sucesos de actualización de estado**.
  5. Seleccione las clases de sucesos y niveles de capacidad de servicio que desee reenviar.
  6. Introduzca el Id. de uno o varios sucesos que desea excluir de reenvío. Separe los identificadores utilizando una coma (por ejemplo, `FQXHMEM0214I,FQXHMEM0214I`).
- **Coincidir por el código de suceso**. Introduzca el Id. de uno o varios sucesos que desee reenviar. Separe los identificadores entre sí mediante comas.
- **Excluir por categorías de sucesos**.
  1. Para excluir todos los sucesos de auditoría, sin importar el nivel de estado, seleccione **Excluir todos los sucesos de auditoría**.
  2. Para excluir todos los sucesos de garantía, seleccione la opción **Excluir los sucesos de garantía**.
  3. Para excluir todos los sucesos de cambio de estado y salud, seleccione **Excluir los sucesos de cambio de estado**.
  4. Para excluir todos los sucesos de actualización de estado y salud, seleccione **Excluir los sucesos de actualización de estado**.
  5. Seleccione las clases de sucesos y niveles de capacidad de servicio que desee excluir.
  6. Introduzca el Id. de uno o varios sucesos que desee reenviar. Separe los identificadores utilizando una coma.
- **Excluir por el código de suceso**. Introduzca el Id. de uno o varios sucesos que desee excluir. Separe los identificadores entre sí mediante comas.

Paso 12. Elija si se deben incluir determinados tipos de sucesos.

- **Incluir todos los sucesos de auditoría**. Envía notificaciones sobre sucesos de auditoría, según las clases y gravedades de los sucesos seleccionados.
- **Incluir sucesos de garantía**. Enviar notificaciones sobre garantías.
- **Incluye sucesos de cambio de estado**. Envía notificaciones sobre cambios de estado.
- **Incluye sucesos de actualización de estado**. Se enviaron notificaciones sobre nuevas alertas.
- **Incluir sucesos del boletín**. Envía notificaciones sobre boletines nuevos.

Paso 13. Seleccione los tipos de sucesos y niveles de gravedad por los que desea que se le notifique.

Paso 14. Seleccione si se deben filtrar sucesos por capacidad de servicio.

Paso 15. Haga clic en **Siguiente** para mostrar la pestaña **Programador**.

Paso 16. **Opcional:** defina las horas y los días en los que desea que se reenvíen sucesos específicos a este despachador de sucesos. Solo se reenvían los sucesos que se producen durante el periodo de tiempo especificado.

Si no crea una planificación para el despachador de sucesos, los sucesos se reenviarán las 24 horas del día, 7 días a la semana.

1. Use el icono **Desplazar a la izquierda** (◀) y el icono **Desplazar a la derecha** (▶) y los botones **Día**, **Semana** y **Mes** para determinar el día y la hora a la que desea que comience la planificación.
2. Haga clic en dos veces la hora para abrir el cuadro de diálogo Nuevo periodo de tiempo.
3. Complete la información requerida, incluida la fecha, horas de inicio y término y si desea que se repita la programación.
4. Haga clic en **Crear** para guardar la planificación y cerrar el cuadro de diálogo. La nueva planificación se añade al calendario.

Consejo:
- Puede cambiar la hora arrastrando la entrada de programación hacia otra hora en el calendario.
- Puede cambiar la duración al seleccionar la parte superior o inferior de la entrada de programación y arrastrarla hacia la nueva hora en el calendario.
- Puede cambiar la hora de término al seleccionar la parte inferior de la entrada de programación y arrastrarla hacia la nueva hora en el calendario.
- Puede cambiar la programación al pulsar dos veces la entrada de programación en el calendario y pulsar **Editar entrada**.
- Se puede visualizar un resumen de todas las entradas de programación al seleccionar **Mostrar resumen del planificador**. El resumen incluye los espacios de tiempo de cada entrada y las entradas que se repiten.
- Puede eliminar una entrada de programación del calendario o resumen de programador seleccionando la entrada y haciendo clic en **Eliminar entrada**.

Paso 17. Haga clic en **Crear**.

El despachador de sucesos aparecerá en la tabla Reenvío de sucesos.

Paso 18. Seleccione el nuevo despachador de sucesos, haga clic en **Generar suceso de prueba** y luego compruebe que el reenvío de sucesos se realice correctamente al syslog correspondiente.

Después de finalizar

Desde la página Reenvío de sucesos, también puede realizar las acciones siguientes en un despachador de sucesos:

- Actualizar la lista de despachadores de sucesos haciendo clic en el icono **Actualizar** ( ).
- Ver los detalles de un despachador de sucesos pulsando el vínculo de la columna **Nombre**.

- Cambiar las propiedades de los despachadores de sucesos y filtrar los criterios pulsando el nombre del despachador de sucesos en la columna **Nombre**.
- Eliminar el despachador de sucesos haciendo clic en el icono **Eliminar** ().
- Suspender el reenvío de sucesos (consulte Suspensión del reenvío de sucesos).

Suspensión del reenvío de sucesos

Puede suspender el reenvío de sucesos deshabilitando al despachador de sucesos. Al suspender el reenvío de sucesos, se detiene la supervisión de los sucesos entrantes. Los sucesos que se reciban mientras la supervisión esté suspendida no se reenviarán.

Acerca de esta tarea

El estado deshabilitado no es persistente. Si se reinicia el nodo de gestión, se habilitarán todos los despachadores de sucesos.

Procedimiento

Lleve a cabo los pasos siguientes para deshabilitar el reenvío de sucesos.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Supervisión → Reenvío de sucesos**. Se muestra la página Reenvío de sucesos.

Paso 2. Seleccione **Deshabilitar** en la columna **Estado** de cada despachador de sucesos que desee suspender.

Reenviar sucesos a dispositivos móviles

Puede configurar Lenovo XClarity Administrator para reenviar notificaciones de sucesos automáticas a dispositivos móviles

Antes de empezar

Se deben cumplir los siguientes requisitos para reenviar sucesos a dispositivos móviles:

- Asegúrese de que haya un servidor DNS configurado para permitir que Lenovo XClarity Administrator se conecte a los servidores automáticos de Apple o Google. Esto se puede configurar al hacer clic en **Administración → Acceso a red → Editar acceso de red** y luego hacer clic en la pestaña de **Configuración de Internet** (consulte Configuración del acceso de red).
- Asegúrese de que todos los puertos requeridos para la gestión de sucesos estén abiertos en la red y en los firewalls. Para obtener más información acerca de los requisitos de los puertos, consulte Disponibilidad de puertos en la documentación en línea de Lenovo XClarity Administrator.

Acerca de esta tarea

Cuando se instala la aplicación Lenovo XClarity Mobile en un dispositivo móvil, puede habilitar cada instancia conectada de Lenovo XClarity Administrator a notificaciones de sucesos automáticas a ese dispositivo móvil. Cuando las notificaciones automáticas están habilitadas para una instancia específica, una suscripción se crea en Lenovo XClarity Administrator para ese dispositivo móvil.

Puede definir los sucesos que son notificados automáticamente en el dispositivo móvil asignando filtros de sucesos globales predefinidos o personalizados para cada instancia de Lenovo XClarity Administrator. Los filtros de sucesos globales predefinidos se habilitan de forma predeterminada. Lenovo XClarity Administrator comienza a supervisar los sucesos entrantes de acuerdo con los criterios de filtro. Cuando se detecta una coincidencia, el suceso se envía al dispositivo móvil.

Para obtener más información acerca de Lenovo XClarity Mobile y los dispositivos móviles compatibles, consulte Uso de la aplicación Lenovo XClarity Mobile.

Procedimiento

Para configurar notificaciones automáticas a ese dispositivo móvil, realice los pasos siguientes desde la aplicación Lenovo XClarity Mobile en su dispositivo móvil.

Paso 1. Habilitar las notificaciones automáticas:

- Puede habilitar notificaciones automáticas cuando crea una conexión a una instancia de Lenovo XClarity Administrator. Las notificaciones automáticas se habilitan de manera predeterminada.
- Puede habilitar notificaciones automáticas en conexiones existentes habilitando uno o más filtros de sucesos

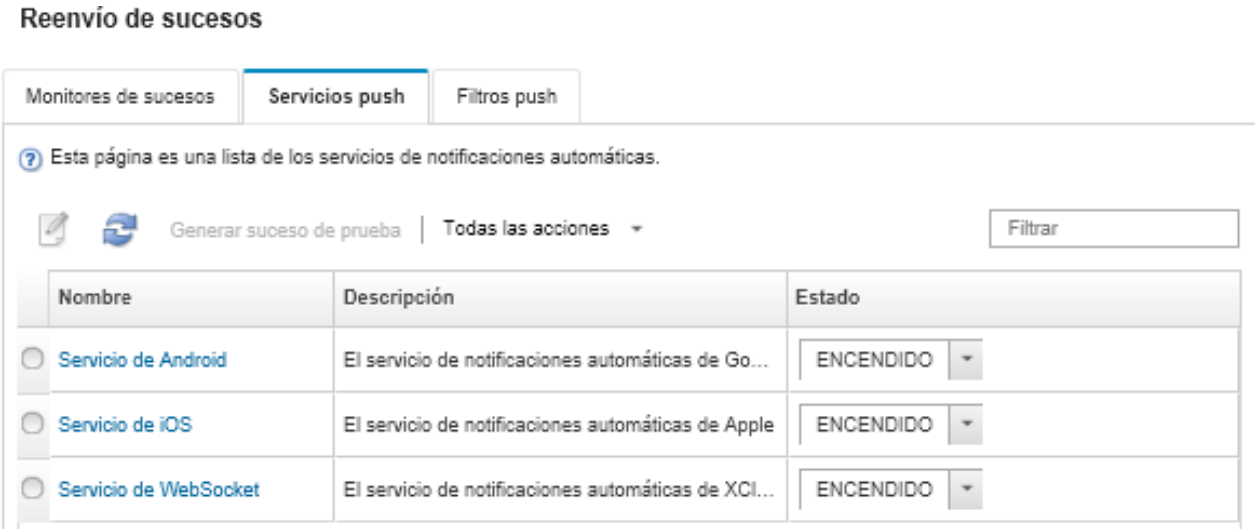
Paso 2. Asigne filtros globales de sucesos para especificar qué eventos deben ser remitidos al dispositivo móvil:

Nota: Puede agregar o eliminar filtros globales de la suscripción únicamente desde la aplicación Lenovo XClarity Mobile. Puede crear filtros globales únicamente desde la interfaz web de Lenovo XClarity Administrator. Para obtener más información sobre cómo crear filtros globales de sucesos personalizados, consulte Crear filtros de sucesos para dispositivos móviles y WebSockets.

1. Toque **Configuración → Notificaciones automáticas**. Se muestra una lista de conexiones de Lenovo XClarity Administrator.
2. Toque la instancia de Lenovo XClarity Administrator para visualizar una lista de filtros de envío.
3. Habilite los filtros de sucesos para los sucesos que desea que se envíen automáticamente al dispositivo móvil para la instancia de Lenovo XClarity Administrator.
4. Toque **Tocar para generar notificación automática de prueba** para verificar que las notificaciones de sucesos se envíen correctamente.

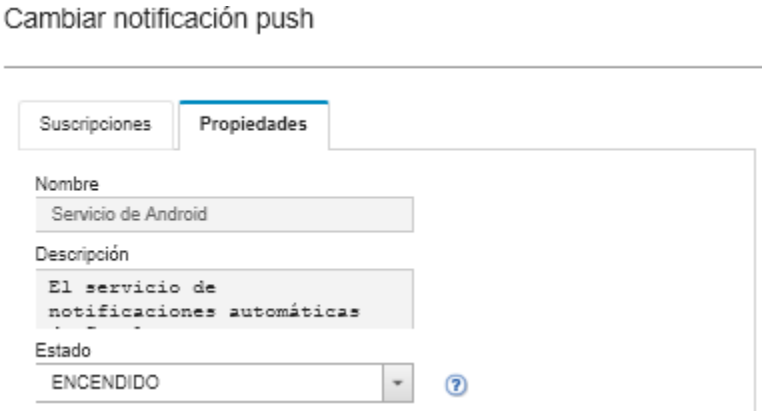
Resultados

Puede gestionar suscripciones desde la página Reenvío de sucesos en la interfaz web de Lenovo XClarity Administrator. Haga clic en **Supervisión → Reenvío de sucesos** para visualizar la página Reenvío de sucesos.



- Puede cambiar las propiedades del servicio de notificación del dispositivo de la pestaña **Servicio de envío automático** en la página Reenvío de sucesos haciendo clic en el enlace para el servicio de la

notificación automática (Google o Apple) en la columna **Nombre** para visualizar el cuadro de diálogo de Cambiar notificación automática y, a continuación, haga clic en la pestaña **Propiedades**.



- Puede habilitar y deshabilitar las suscripciones:
  - Habilite o deshabilite todas las suscripciones para un servicio específico de notificación del dispositivo en la pestaña **Servicio de envío automático** en la página Reenvío de sucesos seleccionando el estado de **ACTIVADO** o **DESACTIVADO** en la tabla para el servicio de notificación del dispositivo.
  - Habilite o deshabilite todas las suscripciones para un dispositivo específico desde la aplicación Lenovo XClarity Mobile al tocar **Configuración → Notificación automática** y luego habilite o deshabilite Habilitar notificación automática.
  - Habilite o deshabilite una suscripción específica desde la aplicación Lenovo XClarity Mobile al tocar **Configuración → Notificación automática**, luego toque conexión Lenovo XClarity Administrator y habilite al menos un filtro de sucesos o deshabilite todos los filtros de sucesos.
- Puede generar un suceso de prueba para todas las suscripciones para un servicio móvil específico en la pestaña **Servicio de envío automático** en la página Reenvío de sucesos seleccionando el servicio móvil y al hacer clic en **Generar suceso de prueba**.
- Puede ver una lista de suscripciones actuales. Desde la pestaña **Servicio de envío automático** en la página Reenvío de sucesos, haga clic en el enlace para el servicio de la notificación automática del dispositivo correspondiente (Android o iOS) en la columna **Nombre** para visualizar el cuadro de diálogo de Cambiar notificación automática y, a continuación, haga clic en la pestaña **Suscripciones**. El Id. de dispositivo identifica cada suscripción.

  Sugerencias:

  - El Id. de dispositivo corresponde a los primeros y últimos 6 dígitos de identificación del registro de envío automático. Puede encontrar el Id. de registro de envío automático en la aplicación Lenovo XClarity Mobile al a tocar **Configuración → Acerca de → Id. de registro de envío automático**.
  - Si inició sesión como usuario con uno de los roles siguientes, se muestran todas las suscripciones; de lo contrario, solo se muestran las suscripciones para el usuario que inició la sesión.
    - **lxc-admin**
    - **lxc-supervisor**
    - **lxc-security-admin**
    - **lxc-sysmgr**
- Puede ver la lista de filtros de sucesos asignados a la suscripción en la pestaña **Suscripciones** en el cuadro de diálogo Cambiar notificación automática al ampliar la **Lista del filtros** en la columna **Filtros de sucesos** para la suscripción.

- Puede crear filtros de sucesos para una suscripción específica en la pestaña **Suscripciones** en el cuadro de diálogo de Cambiar notificación automática seleccionando la suscripción y hacer clic en el icono **Crear** ( ).

  Nota: Estos filtros de sucesos se aplican solo a una suscripción específica y no se pueden utilizar por otras suscripciones.

  También puede editar o eliminar un filtro de sucesos seleccionando el filtro de suceso y hacer clic en el icono **Editar** ( ) o en el icono **Eliminar** ( ), respectivamente.
- Puede determinar el estado de la notificación automática intentada más recientemente para una suscripción específica en la pestaña **Suscripciones** en el cuadro de diálogo Cambiar notificación automática. La columna **Indicación de hora** indica la fecha y hora de la última notificación automática. **Estado** indica si la notificación automática se entregó correctamente al servicio de envío automático. No hay estado disponible con relación a si la notificación automática se entregó correctamente al dispositivo del servicio. Si la entrega al servicio automático falló, la columna Estado proporciona información adicional acerca del error.
- Puede crear un suceso de prueba para una suscripción específica en la pestaña **Suscripciones** en el cuadro de diálogo de Cambiar notificación automática seleccionando la suscripción y hacer clic en **Generar suceso de prueba**
- Puede eliminar una suscripción en la pestaña **Suscripciones** en el cuadro de diálogo Cambiar notificación automática seleccionando la suscripción y hacer clic en el icono **Eliminar** ( ).

Reenvío de sucesos a los servicios de WebSocket

Puede configurar Lenovo XClarity Administrator para reenviar notificaciones de sucesos automáticas a servicios de WebSocket.

Acerca de esta tarea

Las suscripciones de WebSocket no se almacenan de forma persistente en Lenovo XClarity Administrator. Cuando se reanuda Lenovo XClarity Administrator, los suscriptores de WebSocket deben suscribirse nuevamente.

Procedimiento

Para enviar notificaciones automáticas de sucesos a un servicio de WebSocket, complete los pasos siguientes.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Supervisión → Reenvío de sucesos**. Se muestra la página Reenvío de sucesos.

Paso 2. Haga clic en la pestaña de **Servicios de notificaciones automáticas** .

Paso 3. Haga clic en el enlace relativo al **Servicio de WebSocket** en la columna **Nombre**. Se muestra el cuadro de diálogo Notificación automática.

Paso 4. Haga clic en la pestaña **Suscripciones**.

Paso 5. Haga clic en el icono **Crear** ( ).

Paso 6. Introduzca la dirección IP del host de destino.

Paso 7. Haga clic en **Crear**.

Paso 8. Seleccione la nueva suscripción, haga clic en **Generar suceso de prueba** y luego compruebe que el reenvío de sucesos se realice correctamente al servicio de WebSocket.

Resultados

En la pestaña **Suscripciones** en el cuadro de diálogo Cambiar notificación automática, puede realizar las acciones siguientes en una suscripción seleccionada de WebSocket:

- Actualizar la lista de servicios de WebSocket haciendo clic en el icono **Actualizar** ( ).
- Eliminar suscripciones al seleccionar las suscripciones y hacer clic en el icono **Eliminar** ( ).
- Determine el estado de la notificación automática más reciente para una suscripción específica al ver el contenido de la columna **Estado**. Si el intento falla, esta columna contiene un mensaje que describe el error.

En la pestaña **Propiedades** en el cuadro de diálogo Cambiar notificación automática, puede realizar las acciones siguientes:

- Cambie las propiedades del servicio de WebSocket, incluida el tiempo inactivo de conexión, el tamaño de búfer máximo, el número máximo de suscriptores y el período de desconexión del registro.
- Puede restablecer el servicio de WebSocket a los valores predeterminados pulsando **Restaurar valores predeterminados**.
- Suspenda las notificaciones automáticas de sucesos para todas las suscripciones para el servicio de WebSocket estableciendo el **Estado** como desactivado.

En la pestaña **Servicio de envío automático** en la página Reenvío de sucesos, puede generar un suceso de prueba para todas las suscripciones de WebSocket al seleccionar el servicio de WebSocket y hacer clic en **Generar suceso de prueba**.

Crear filtros de sucesos para dispositivos móviles y WebSockets

Puede crear filtros globales de sucesos que se pueden utilizar en una o más suscripciones para dispositivos móviles y WebSockets. También puede crear filtros de sucesos que son exclusivos de una suscripción.

Antes de empezar

Para crear filtros de sucesos debe tener autoridad de supervisor.

Puede crear hasta 20 filtros globales de sucesos.

Acerca de esta tarea

Los siguientes filtros globales de sucesos son predeterminados:

- **Coincidir todos los críticos**. Este filtro coincide con todos los sucesos críticos que son generados por cualquier dispositivo gestionado o por XClarity Administrator.
- **Coincidir todas las advertencias**. Este filtro coincide con todos los sucesos de advertencia que son generados por cualquier dispositivo gestionado o por XClarity Administrator.

Procedimiento

Para crear un filtro global de sucesos, lleve a cabo los pasos siguientes.

- Cree un filtro global de sucesos que cualquier suscripción puede utilizar.
  1. En la barra de menús de XClarity Administrator, haga clic en **Supervisión → Reenvío de sucesos**. Se muestra la página Reenvío de sucesos.
  2. Haga clic en la pestaña de **Filtros de notificaciones automáticas** .
  3. Haga clic en el icono **Crear** ( ). Se abre la pestaña **General** del cuadro de diálogo Nuevo filtro de notificación automática.
  4. Especifique el nombre y la descripción de la opción para este filtro del suceso.
  5. Haga clic en **Siguiente** para mostrar la pestaña **Sistemas**.
  6. Seleccione los dispositivos que desea supervisar.

     Consejo Para reenviar sucesos de todos los dispositivos gestionados (actuales y futuros), seleccione la casilla de verificación **Igualar todos los sistemas**.Si no selecciona la casilla **Igualar todos los sistemas**, asegúrese de que los dispositivos seleccionados no tengan un DUMMY-UUID en la columna UUID. Se asigna un Dummy-UUID a los dispositivos que aún no se recuperan después de un reinicio o no han sido detectados completamente por el servidor de gestión. Si selecciona un dispositivo con un Dummy-UUID, el reenvío de sucesos no funcionará para este dispositivo hasta que el dispositivo sea completamente detectado o recuperado y el Dummy-UUID cambie a su UUID real.
  7. Haga clic en **Siguiente** para mostrar la pestaña **Sucesos**.
  8. Seleccione los componentes y niveles de gravedad de los sucesos que desee reenviar.

     Consejo:
     - Para reenviar todos los sucesos de hardware, seleccione la opción **Coincidir todos los sucesos**.
     - Para reenviar sucesos de auditoría, seleccione la opción **Incluir todos los sucesos de auditoría**.
     - Para reenviar sucesos de garantía, seleccione la opción **Incluir los sucesos de garantía**.
  9. Haga clic en **Crear**.
- Cree un filtro de suceso para una suscripción específica:
  1. En la barra de menús de XClarity Administrator, haga clic en **Supervisión → Reenvío de sucesos**. Se muestra la página Nuevo reenvío de sucesos.
  2. Haga clic en la pestaña de **Filtros de notificaciones automáticas** .
  3. Seleccione el enlace para el tipo de dispositivo móvil (Android o iOS) en la columna Nombre de la tabla. Se muestra el cuadro de diálogo Notificación automática.
  4. Haga clic en la pestaña **Suscripciones** para visualizar una lista de suscripciones activas.
  5. Seleccione la suscripción y haga clic en el icono **Crear** ( ). Se abre la pestaña **General** del cuadro de diálogo Nuevo filtro de sucesos.
  6. Especifique el nombre y la descripción de la opción para este filtro del suceso.
  7. Haga clic en **Siguiente** para mostrar la pestaña **Sistemas**.
  8. Seleccione los dispositivos que desea supervisar.

Consejo Para reenviar sucesos de todos los dispositivos gestionados (actuales y futuros), seleccione la casilla de verificación **Igualar todos los sistemas**.Si no selecciona la casilla **Igualar todos los sistemas**, asegúrese de que los dispositivos seleccionados no tengan un DUMMY-UUID en la columna UUID. Se asigna un Dummy-UUID a los dispositivos que aún no se recuperan después de un reinicio o no han sido detectados completamente por el servidor de gestión. Si selecciona un dispositivo con un Dummy-UUID, el reenvío de sucesos no funcionará para este dispositivo hasta que el dispositivo sea completamente detectado o recuperado y el Dummy-UUID cambie a su UUID real.

9. Haga clic en **Siguiente** para mostrar la pestaña **Sucesos**.
10. Seleccione los componentes y niveles de gravedad de los sucesos que desee reenviar.

    Consejo:
    - Para reenviar todos los sucesos de hardware, seleccione la opción **Coincidir todos los sucesos**.
    - Para reenviar sucesos de auditoría, seleccione la opción **Incluir todos los sucesos de auditoría**.
    - Para reenviar sucesos de garantía, seleccione la opción **Incluir los sucesos de garantía**.
11. Haga clic en **Crear**.

Después de finalizar

Desde la pestaña Filtros de notificaciones automáticas en la página Reenvío de sucesos, también puede realizar las acciones siguientes en un filtro de sucesos seleccionado:

- Actualizar la lista de filtros de sucesos haciendo clic en el icono **Actualizar** ( ).
- Ver los detalles de un filtro de sucesos pulsando el vínculo de la columna **Nombre**.
- Cambiar las propiedades del filtro de sucesos y filtrar los criterios pulsando el icono **Editar** ( ).

Eliminar el filtro de sucesos haciendo clic en el icono **Eliminar** ( ).

Uso de trabajos

Los *trabajos* son tareas que tardan más en ejecutarse y se llevan a cabo en uno o varios dispositivos. Puede programar que determinados trabajos se ejecuten solo una vez (inmediatamente o en un momento posterior), de forma recurrente, o cuando se produce un suceso específico.

Los trabajos se ejecutan en segundo plano. Puede ver el estado de cada trabajo en el registro de trabajos.

Supervisión de trabajos

Puede ver un registro de todos los trabajos iniciados mediante Lenovo XClarity Administrator. La lista incluirá todos los trabajos en ejecución, completados o con errores.

Acerca de esta tarea

Los *trabajos* son tareas que tardan más en ejecutarse y se llevan a cabo en uno o varios dispositivos. Por ejemplo, si despliega un sistema operativo en varios servidores, el despliegue en cada servidor figura en la lista como un trabajo independiente.

Los trabajos se ejecutan en segundo plano. Puede ver el estado de cada trabajo en el registro de trabajos.

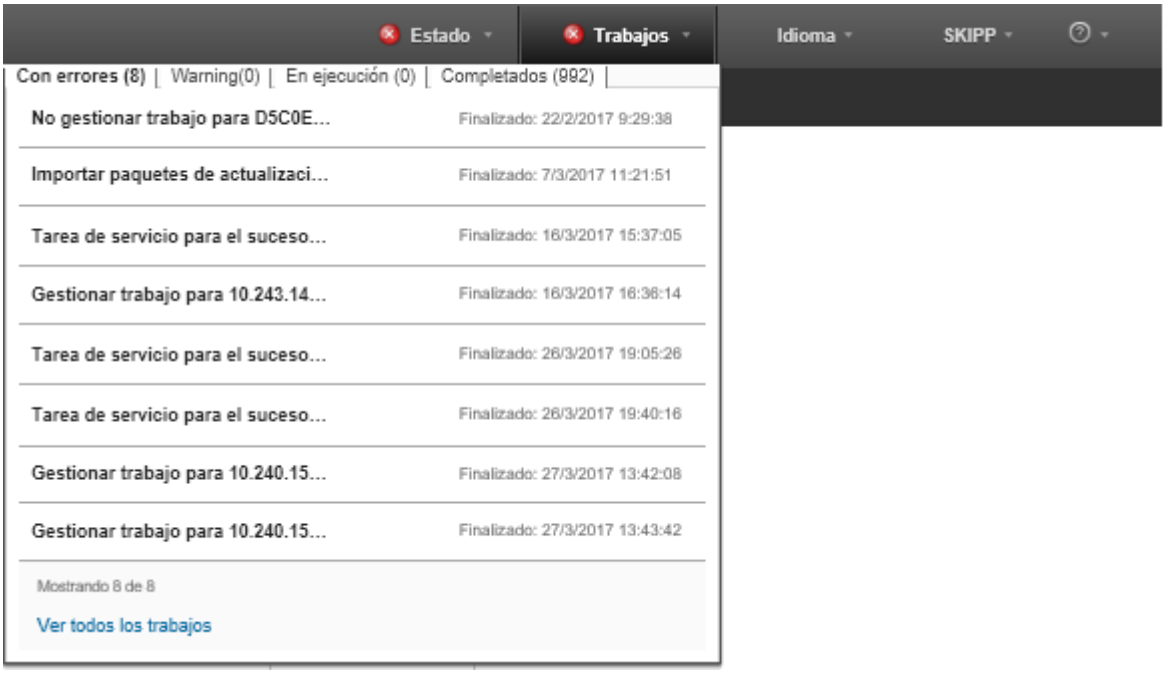
El registro de trabajos contiene información acerca de cada trabajo. El registro puede contener como máximo 1000 sucesos o 1 GB. Cuando se alcanza el tamaño máximo, se eliminan los trabajos más antiguos que se completaron correctamente. De no haber trabajos completados correctamente en el registro, se eliminan los trabajos más antiguos que se completaron con advertencias. De no haber trabajos completados

correctamente o con advertencias en el registro, se eliminan los trabajos más antiguos que se completaron con errores.

Procedimiento

Lleve a cabo uno de los pasos siguientes para mostrar el registro de trabajos.

- En la barra de título de XClarity Administrator, haga clic en **Trabajos** para mostrar un resumen de los trabajos en ejecución, completados y con errores.

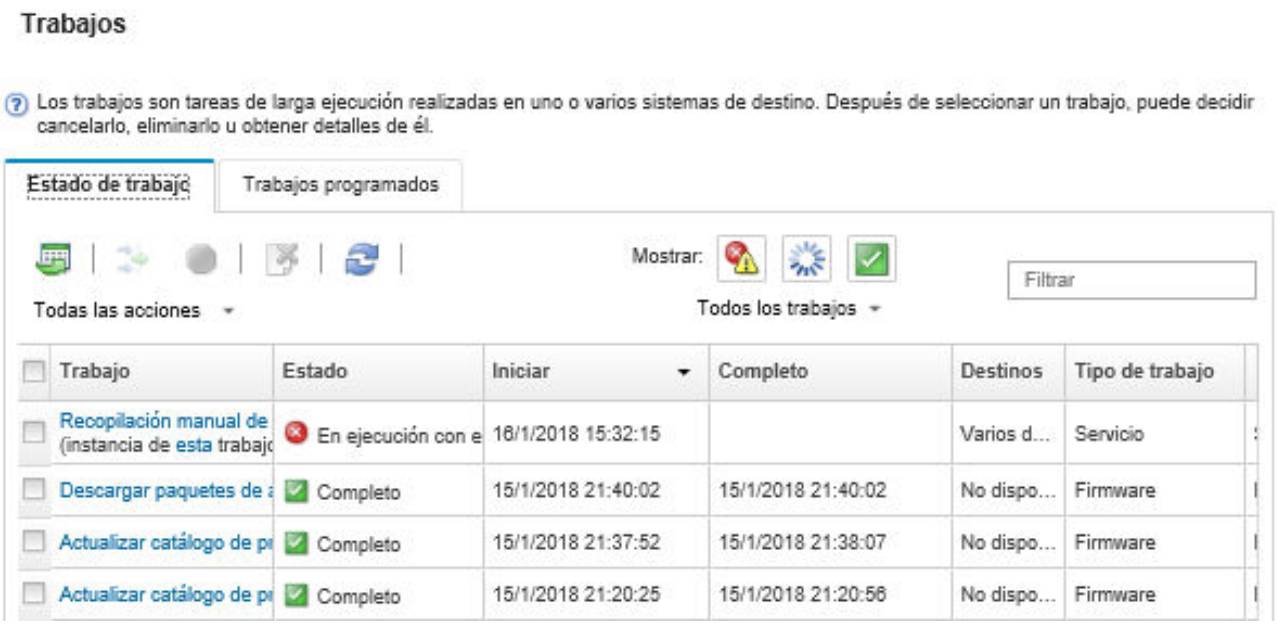


  En este menú desplegable, puede hacer clic en las pestañas siguientes:
  - **Errores**. Muestra una lista de todos los trabajos que presentan errores asociados.
  - **Advertencias**. Muestra una lista de todos los trabajos que presentan advertencias asociadas.
  - **En ejecución**. Muestra una lista de todos los trabajos que están en curso en la actualidad.
  - **Completados**. Muestra una lista de todos los trabajos completados.

  Sitúe el cursor sobre una entrada de trabajo en el menú desplegable para obtener más información acerca del trabajo, incluidos el estado, el progreso y el usuario que creó el trabajo.
- En la barra de título de XClarity Administrator, haga clic en la barra de título **Trabajos** y, a continuación, haga clic en el enlace **Ver todos los trabajos** para mostrar la página Estados de trabajos.
- En la barra de menú de XClarity Administrator, haga clic en **Supervisar → trabajos** y haga clic en la pestaña **Estado de trabajo** para mostrar la página Estado de trabajo.

Después de finalizar

Se muestra la página Trabajos con una lista de todos los trabajos de XClarity Administrator.



Desde esta página puede llevar a cabo las siguientes acciones:

- Cree programas de trabajo haciendo clic en la pestaña **Trabajos programados** (consulte Programación de trabajos).
- Obtenga más información acerca un trabajo específico al hacer clic en la columna descripción de la tarea en la columna **Trabajos**. Se muestra un cuadro de diálogo con una lista de subtareas (subtrabajos) y sus objetivos, un resumen de las subtareas, lo que incluye todas las acciones necesarias y detalles de registro que incluyen la severidad y la marca de hora de cada mensaje. Puede elegir ocultar o mostrar los registros de las tareas secundarias.
- Para los trabajos programados, visualice información acerca del programa de trabajo al hacer clic en “este” enlace, bajo la descripción de trabajo en la columna **Trabajos**.
- Cambie el número de trabajos que se visualizan por página. El valor predeterminado es 10 trabajos. Puede visualizar 25, 50 o todos los trabajos.
- Reducir la lista de trabajos que se muestran:
  - Para mostrar solo los trabajos de determinados orígenes, haga clic en **Tipos de trabajo** y elija una de las opciones siguientes.
    - **Todos los tipos de trabajos**
    - **Servicio**
    - **Gestión**
    - **Configuración**
    - **Firmware**
    - **Estado**
    - **Alimentación**
    - **Acceso remoto**
    - **Id. del sistema**
    - **Imágenes del SO**
    - **Despliegue del SO**
    - **Exportar perfil del SO**
    - **Personalizado**
    - **Lista de sistemas**
    - **Desconocido**
  - Muestra una lista compuesta de trabajos programados asociados a un tipo específico de programa al hacer clic en **Tipos de programación** y al seleccionar una de las opciones siguientes.

  - **Todos los tipos de programación**
  - **Una vez**
  - **Recurrente**
  - **Activado**
- Para ocultar o mostrar los trabajos con errores o advertencias, pulse el icono **Ocultar trabajos con errores o advertencias** ().
- Para ocultar o mostrar los trabajos que están en ejecución en la actualidad, pulse el icono **Ocultar trabajos en ejecución** ().
- Para ocultar o mostrar los trabajos completados, haga clic en el icono **Ocultar trabajos completados** ().
- Para incluir únicamente los trabajos que contengan un texto determinado, especifique dicho texto en el campo **Filtro**.
- Si se aplica un filtro a la página, puede quitarlo al hacer clic en el icono **Mostrar todos los trabajos** ().
- Para ordenar los trabajos por columna, haga clic en un encabezado de columna.

- Exportar la lista de trabajos como archivo CSV haciendo clic en el icono **Exportar como CSV** ().

  Nota: Las marcas de tiempo del registro exportado utilizan la hora local especificada por el navegador web.
- Cancelar los trabajos en ejecución o subtareas; para ello, seleccione uno o varios trabajos o subtareas en curso y haga clic en el icono **Detener** ().

  Nota: La cancelación del trabajo puede tardar varios minutos en completarse.
- Eliminar los trabajos completados del registro de trabajos o subtareas; para ello, seleccione uno o varios trabajos o subtareas completados y pulse el icono **Eliminar** ().
- Exportar información acerca de los trabajos específicos al seleccionar los trabajos y pulse el icono **Exportar como CSV** ().
- Actualizar el registro de trabajos; para ello, haga clic en el icono **Actualizar** ().

Programación de trabajos

Ahora puede crear programas en Lenovo XClarity Administrator para ejecutar ciertas tareas en momentos específicos.

Acerca de esta tarea

Puede programar los siguientes tipos de trabajos:
- Tareas simples, como apagado y reinicio
- Recopilar datos de servicio de dispositivos específicos
- Actualización de los catálogos de actualizaciones de firmware y controladores de dispositivos de SO desde el sitio web de Lenovo
- Actualizar el catálogo de actualizaciones de XClarity Administrator desde el sitio Web de Lenovo
- Descargar firmware desde el sitio Web de Lenovo
- Actualización de firmware y controladores de dispositivos del SO en los dispositivos gestionados
- Creación de copias de seguridad de datos y valores de XClarity Administrator
- Creación de copia de seguridad y restauración de datos de configuración de conmutador

Puede programar trabajos de modo que se ejecuten:
- Solo una vez (de inmediato o en una instancia posterior)
- Recurrentemente
- Cuando se produce un suceso específico

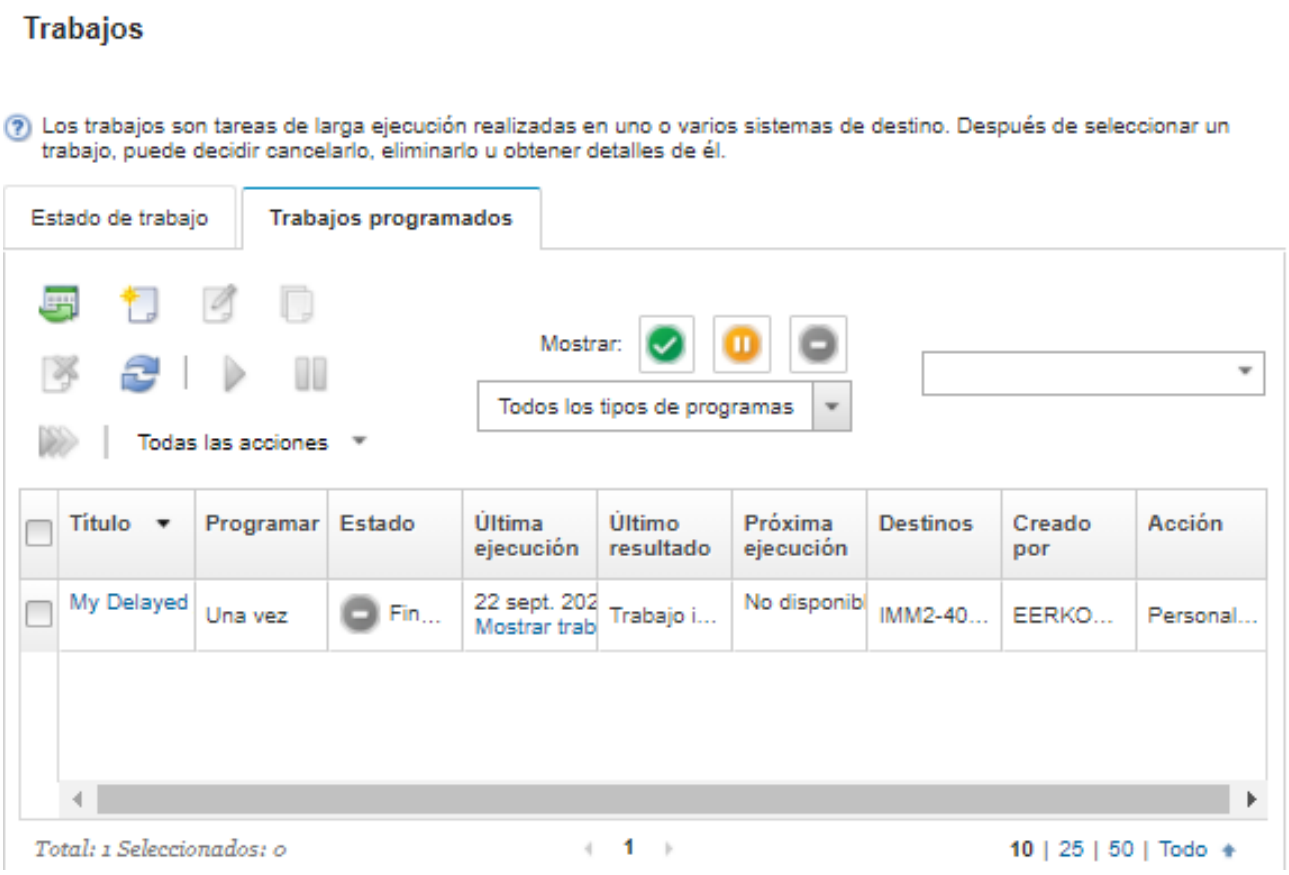
Procedimiento

Para crear y programar una tarea, complete los siguientes pasos.

- Para tareas complejas, como la actualización de firmware y recopilación de datos del servicio, cree el trabajo desde la página o diálogo de tarea actual.
  1. Haga clic en **Programa** para crear un programa para ejecutar esta tarea. Se muestra el cuadro de diálogo Programar trabajo nuevos.
  2. Introduzca un nombre para el trabajo.
  3. Especifique cuando se debe ejecutar el trabajo. Las opciones disponibles dependen del tipo de tarea. Algunos trabajos no se pueden configurar de modo que sean recurrentes o que se activen por un suceso
     - **Una vez**. Estos trabajos se ejecutan solo una vez. Especifique la fecha y hora en la que desea ejecutar este trabajo.
     - **Recurrente**. Estos trabajos se ejecutan más de una vez. Especifique cuándo y con qué frecuencia desea ejecutar este trabajo.
     - **Activado por suceso**. Estos trabajos se ejecutan cuando ocurre un suceso específico.
       a. Especifique la fecha y hora en la que desea ejecutar este trabajo y haga clic en **Siguiente**.
       b. Seleccione el suceso que activará el trabajo.
  4. Haga clic en **Crear trabajo**.
- Para tareas simples, como encender y reiniciar el sistema, cree el programa de trabajo desde la página Trabajos.
  1. En la barra de menú de XClarity Administrator, haga clic en **Supervisión → Trabajos** y, a continuación, haga clic en la pestaña **Trabajo programado** para mostrar la página Trabajos programados.
  2. Haga clic en el icono **Crear** ( ) para mostrar el cuadro de diálogo Programar trabajos nuevos.
  3. Introduzca un nombre para el trabajo.
  4. Especifique cuando se debe ejecutar el trabajo.
     - **Una vez**. Estos trabajos se ejecutan solo una vez.
       a. Especifique la fecha y hora en la que desea ejecutar este trabajo y haga clic en **Siguiente**.
       b. Seleccione los dispositivos gestionados en los que el trabajo se ha de ejecutar.
     - **Recurrente**. Estos trabajos se ejecutan más de una vez.
       a. Especifique cuándo y con qué frecuencia desea ejecutar este trabajo.
       b. Seleccione los dispositivos gestionados en los que el trabajo se ha de ejecutar**.**
     - **Activado por suceso**. Estos trabajos se ejecutan cuando ocurre un suceso específico.
       a. Especifique la fecha y hora en la que desea ejecutar este trabajo y haga clic en **Siguiente**.
       b. Seleccione los dispositivos gestionados en los que el trabajo se ha de ejecutar y haga clic en **Siguiente**.
       c. Seleccione el suceso que activará el trabajo.
  5. Haga clic en **Crear**.

Después de finalizar

La pestaña Trabajos programados se abre con una lista de todos los programas de trabajo en XClarity Administrator.



Desde esta página puede llevar a cabo las siguientes acciones:

- Visualice la información acerca de todos los trabajos completados y activos de un trabajo específico al hacer clic en el vínculo de la columna **Trabajo**.
  - Muestre la lista de programas de trabajo asociados a un tipo específico de programa al hacer clic en **Tipos de programación** y al seleccionar una de las opciones siguientes:
    - **Todos los tipos de programación**
    - **Una vez**
    - **Recurrente**
    - **Activado**
  - Muestre u oculte solo programaciones de trabajos que están en un estado específico al hacer clic en uno de los siguientes iconos:
    - Para todos los trabajos programados activos, haga clic en el icono **Activos** ( ).
    - Para todos los trabajos programados no activos, haga clic en el icono **Pausado** ( ).
    - Para todos los trabajos programados que ya se ejecutaron y que no están programados para volver a ejecutarse, haga clic en el icono **Terminado** ( ).
  - Para incluir únicamente los trabajos programados que contengan un texto determinado, especifique dicho texto en el campo **Filtro**.
  - Para ordenar los trabajos programados por columna, haga clic en un encabezado de columna.

- Para visualizar el último trabajo ejecutado, observe la columna **Última ejecución**. Para ver el estado del último trabajo ejecutado, haga clic en el enlace “Estado de trabajo” en la columna.
- Para ver cuando se programa el trabajo para ejecutarse posteriormente, observe la columna **Siguiente ejecución**. Para ver una lista de todas los fechas y horas futuras, haga clic en el vínculo “Más” en la columna.
- Para ejecutar inmediatamente el trabajo asociado con el programa, haga clic en el icono **Ejecutar** ().
- Para deshabilitar o habilitar una tarea programada, haga clic en el icono **Pausar** () o el icono **Activar** () respectivamente.
- Para copiar y modificar un programa de trabajo, haga clic en el icono **Copiar** ().
- Para editar un programa de trabajo, haga clic en el icono **Editar** ().
- Para eliminar una o más planificaciones de trabajo seleccionadas, haga clic en el icono **Eliminar** ().
- Exportar información acerca de las programaciones de trabajo específicas al seleccionar las programaciones de trabajo y pulse el icono **Exportar como CSV** ().
- Para actualizar la lista de programación de trabajo, haga clic en **Todas las acciones → Actualizar**.

Adición de una resolución y comentarios a un trabajo

Puede añadir una resolución y comentarios a una tarea completada, independientemente del estado de éxito o error. Puede hacer esto para un trabajo principal y para las subtareas del trabajo.

Procedimiento

Lleve a cabo uno de los siguientes pasos para añadir una resolución y comentarios a un trabajo.

Paso 1. En la barra de menú de Lenovo XClarity Administrator, haga clic en **Supervisar → trabajos** y haga clic en la pestaña **Estado de trabajo** para mostrar la página Estado de trabajo.

Paso 2. Haga clic en el enlace para el trabajo en la columna **Trabajo** para mostrar los detalles del trabajo.

Paso 3. Pulse el icono de **Notas** () para mostrar el cuadro de diálogo Notas.

En este cuadro de diálogo, puede ver un historial de todas las notas y las soluciones que se han añadido a la tarea. Puede borrar el historial haciendo clic en **Borrar todos los registros**.

Paso 4. Elija una de las siguientes resoluciones.
- **Sin cambios**
- **Investigando**
- **Resuelto**
- **Cancelado**

Paso 5. Agregue un comentario en el campo **Nota**.

Paso 6. Haga clic en **Aplicar**.

En la página Estado de trabajo, la resolución se muestra en la columna **Estado** para ese trabajo.

Visualización de relaciones entre trabajos y sucesos

Un *diagrama de flujo* es una vista gráfica que muestra la relación entre las actividades (incluidos los trabajos y sucesos) que un usuario inicia manualmente o que Lenovo XClarity Administrator inicia automáticamente. El diagrama de flujo ayuda a identificar problemas ilustrando la secuencia de acciones que se inició y las sucesos que se generaron, cuando generaron eventos y lo que causaron que se generaran.

Antes de empezar

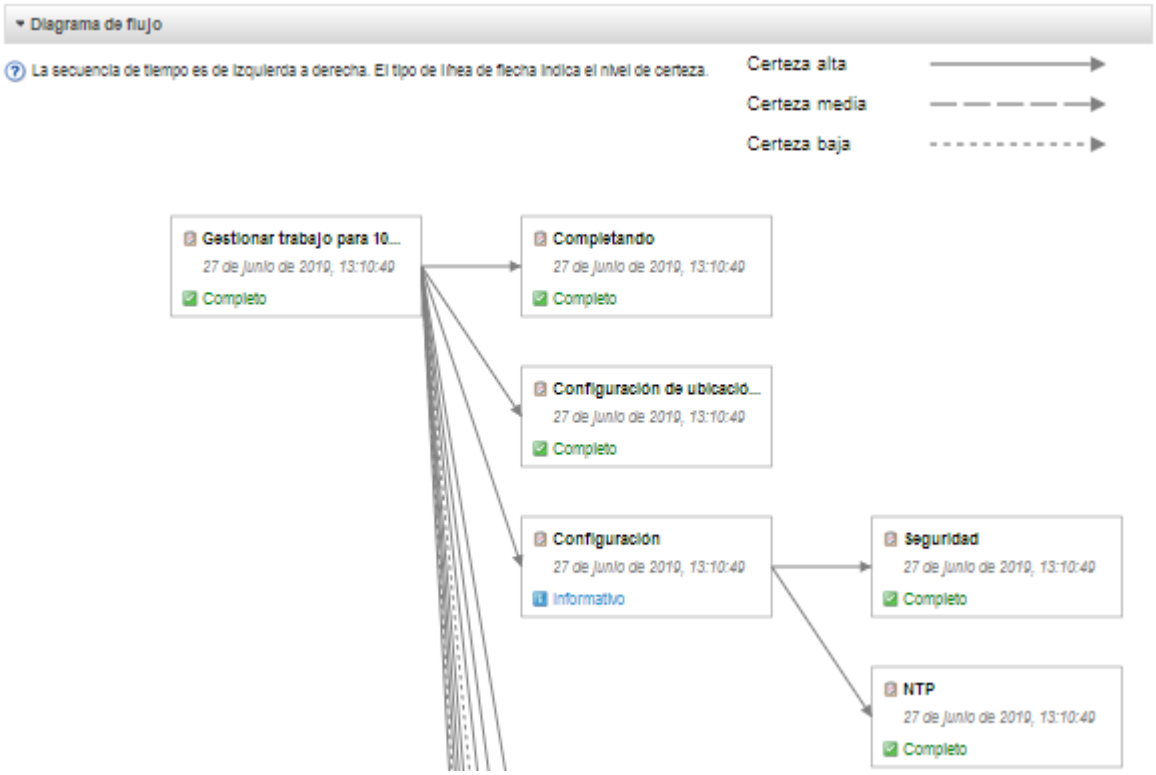
De forma predeterminada, los flujos de actividades están deshabilitados. Debe habilitar los flujos de actividades antes de que estos puedan generarse para una actividad. Puede ver los flujos solo para actividades que se producen cuando se habilitan los flujos de actividad.

Atención: Los flujos de actividades aumentan el uso de la memoria mediante XClarity Administrator. Se recomienda que no habilite los flujos de actividades si XClarity Administrator ya conlleva un uso de memoria alto.

Acerca de esta tarea

El siguiente ejemplo muestra un diagrama de flujo. La secuencia de sucesos fluye de izquierda a derecha. Cada nodo en el flujo representa una sola actividad e incluye la fecha, la descripción de la actividad y el estado. Puede colocar el cursor sobre el nombre del nodo para ver información adicional acerca de la actividad.

El estilo de las líneas entre los nodos de indica la seguridad de la relación de los nodos.
- Las líneas sólidas representan una seguridad alta.
- Las líneas de con guiones largos representan una seguridad media.
- Las líneas con guiones cortos representan una seguridad baja.



Procedimiento

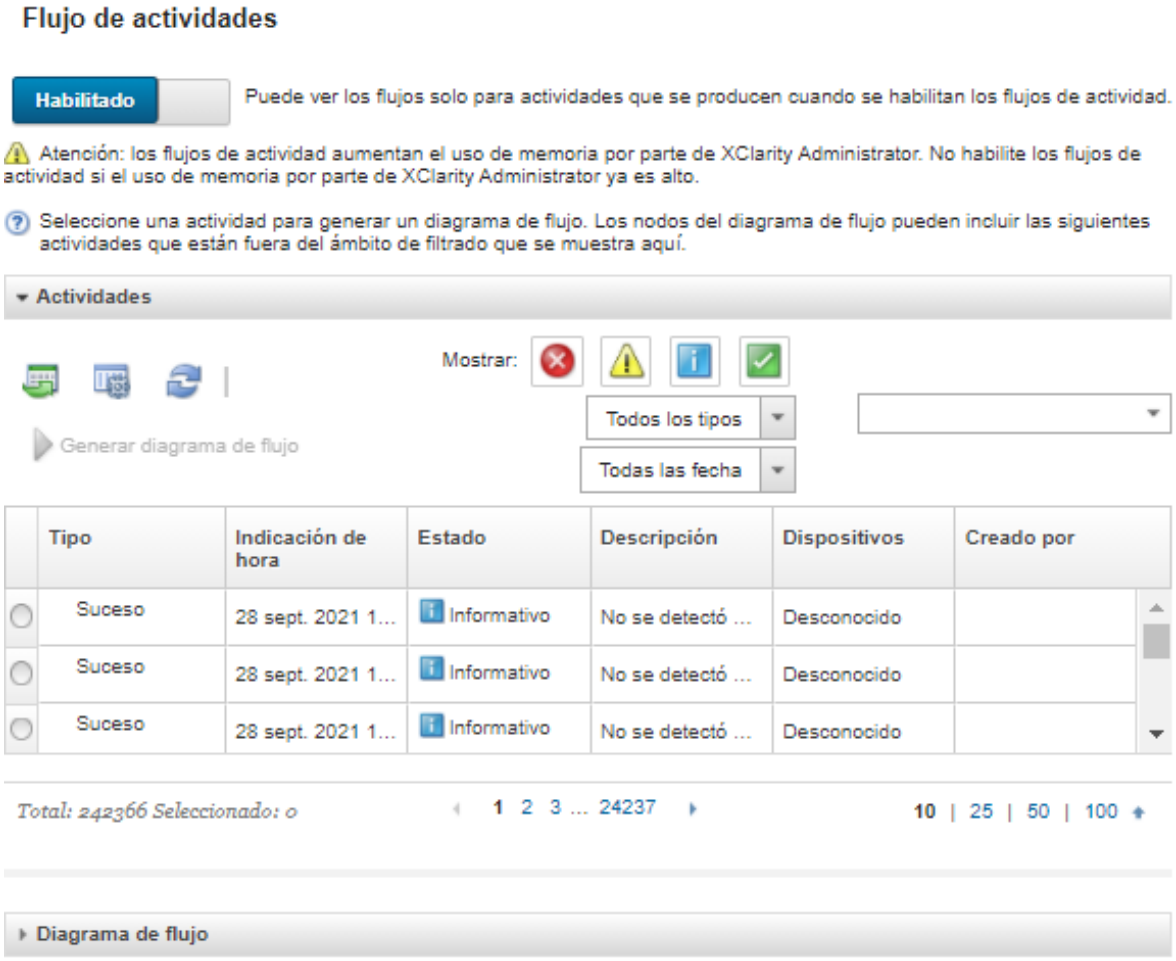
Lleve a cabo los siguientes pasos para ver el diagrama de flujo de una actividad específica.

Paso 1. Desde la barra de menú XClarity Administrator, haga clic en **Monitoreo → Flujo de actividades** para mostrar la página de Flujo de actividades

Paso 2. Habilite los flujos de actividades al seleccionar **Habilitar flujo de actividades**.

Paso 3. En la sección **Actividades**, seleccione el trabajo o un suceso.

Puede ordenar las columnas de la tabla para que sea más fácil encontrar actividades específicas. Además, puede seleccionar un tipo de estado, tipo de actividad, fecha o introducir texto (como un nombre o dirección IP) en el campo **Filtro** y listar solo las actividades que cumplen los criterios seleccionados.



Paso 4. Haga clic en **Generar diagrama de flujo** para mostrar el diagrama de flujo en la sección **Diagrama de flujo**

Después de finalizar

Desde esta página puede llevar a cabo las siguientes acciones:

- Ver información adicional acerca de cada actividad del diagrama de flujo colocando el cursor sobre la actividad.
- Exportar el flujo relacionado con las actividades seleccionadas a un archivo CSV haciendo clic en **Acciones → Exportar a CSV**.

Capítulo 4. 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.

Capítulo 5. Gestión de grupos de recursos

Puede utilizar el grupo de recursos en Lenovo XClarity Administrator para crear un conjunto lógico de dispositivos gestionados que se pueden ver y sobre los cuales puede realizarse acciones de forma conjunta.

Más información: XClarity Administrator: Grupos de recursos

Acerca de esta tarea

Existen tres tipos de grupos de recursos:

- **Static**. Grupos personalizados de dispositivos específicos.
- **Dinámico**. Grupo de dispositivos formados a partir de reglas (por ejemplo, todos los servidores de un tipo específico). Este grupo contiene una lista dinámica de dispositivos basada en un conjunto de propiedades del inventario.

No se puede realizar acciones en un grupo de recursos; sin embargo, se puede seleccionar todos los dispositivos en el grupo y realizar acciones de forma conjunta en todos los dispositivos seleccionados.

Visualización de estado de dispositivos en un grupo de recursos

Puede ver el estado de todos los dispositivos gestionados en un grupo de recursos.

Acerca de esta tarea

Los siguientes iconos de estado se usan para indicar el estado general de todos los dispositivos en el grupo de recursos. El estado general del grupo indica el dispositivo con la máxima gravedad en el grupo.

- Icono **crítico** ( )
- Icono de **advertencia** ( )
- Icono **normal** ( )

Procedimiento

Lleve a cabo los pasos siguientes para ver el estado de los dispositivos en un grupo de recursos.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Panel**. Se muestra la página del panel con una descripción general y el estado de todos los dispositivos gestionados y otros recursos, incluidos los grupos de recursos.

Paso 2. En la barra de menús de XClarity Administrator, haga clic en **Hardware → Grupos de recursos**. Aparecerá la página Todos los grupos de recursos.

La página Todos los grupos de recursos genera una lista de cada grupo de recursos, incluido el nombre del grupo, el número de dispositivos gestionados que están en el grupo y el estado del dispositivo que tiene la máxima gravedad en el grupo.

Desde esta página puede llevar a cabo las siguientes acciones:

- Cree un nuevo grupo de recursos (consulte Creación de un grupo de recursos dinámico y Creación de un grupo de recursos estático)
- Edite la pertenencia a grupos al seleccionar un grupo y, posteriormente, al hacer clic en el icono **Editar** ( ).
- Edite las propiedades de grupo al seleccionar el grupo y al hacer clic en **Todas las acciones → Editar propiedades**.
- Quite un grupo de recursos al seleccionar un grupo y al hacer clic en el icono **Eliminar** ( ).

Nota: Eliminar un grupo solo elimina la definición de mismo. No afecta a los dispositivos que lo componen.

- Exporte información detallada acerca de todos los dispositivos en uno o varios grupos de recursos en un archivo CSV al hacer clic en el icono **Exportar** ( ).

Paso 3. Desde la página Todos los grupos de recursos , haga clic en el nombre de la columna **Grupos** para mostrar la lista de dispositivos de ese grupo.

Desde esta página puede llevar a cabo las siguientes acciones:

- Agregue o quite dispositivos en un grupo de recursos estático al hacer clic en el icono **Editar** ( ).
- Visualice información detallada acerca de un dispositivo específico en el grupo de recursos al hacer clic en el nombre del dispositivo en la columna **Nombre de dispositivo**.
- Exporte información detallada acerca de todos los dispositivos en uno o varios grupos de recursos en un archivo CSV al hacer clic en el icono **Exportar** ( ).

Visualización de los miembros de un grupo de recursos

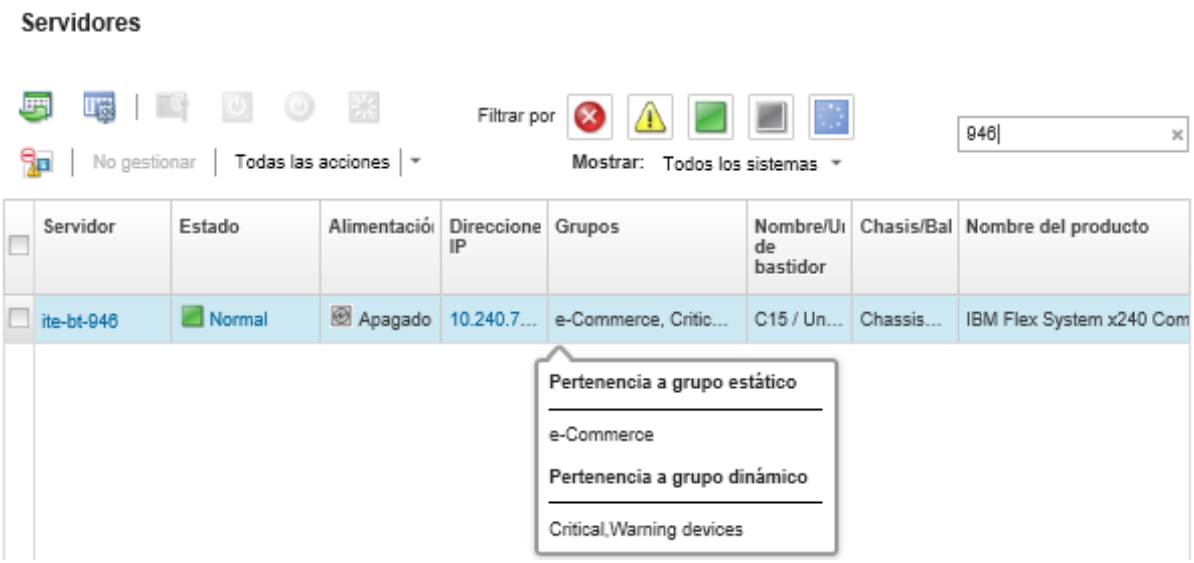
Puede ver información detallada acerca de los grupos de recursos, incluyendo a los miembros del grupo.

Procedimiento

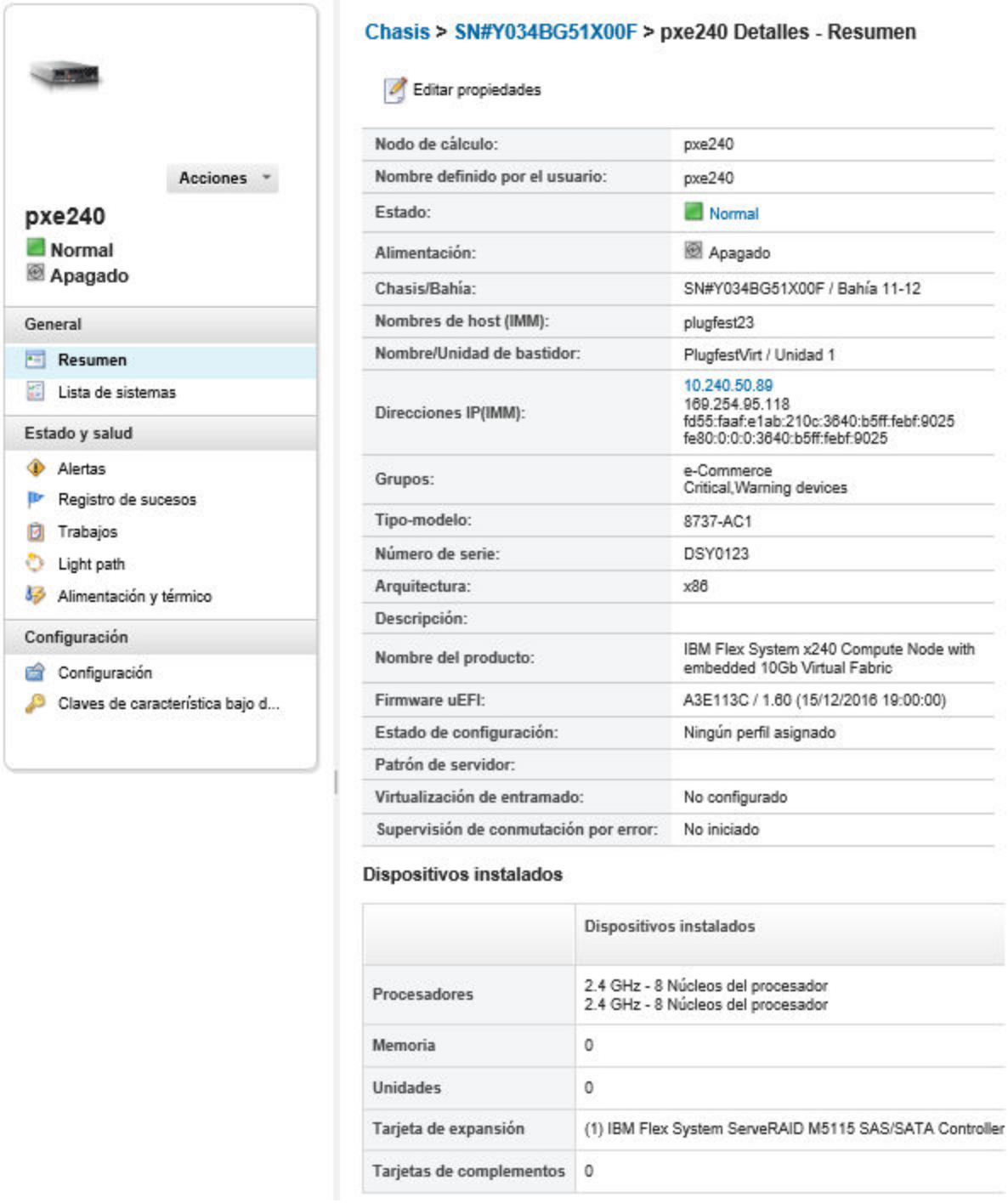
Complete los pasos siguientes para ver la pertenencia al grupo.

- Para ver todos los grupos de los cuales es parte un dispositivo.
  1. Desde la barra de menús de Lenovo XClarity Administrator, haga clic en **Hardware** y, a continuación, haga clic en el tipo de dispositivo para mostrar la página de todos los dispositivos.

     Pose el cursor sobre las listas de grupo en la columna **Grupos** para obtener una lista de los grupos de los que el dispositivo es un miembro.



2. Haga clic en el enlace con el nombre del dispositivo de la primera columna. Se mostrará la página de resumen de dicho dispositivo, lo que incluye una lista de grupos de recursos de los que el dispositivo es un miembro.



- Para ver a los miembros de un grupo.
  1. En la barra de menús de XClarity Administrator, haga clic en **Panel**. Se muestra la página del panel con una descripción general y el estado de todos los dispositivos gestionados y otros recursos, incluidos los bastidores.
  2. En la barra de menús de XClarity Administrator, haga clic en **Hardware → Grupos**. Aparecerá la página Grupos de recursos.

     Esta página muestra el número total de miembros y el número de miembros de cada tipo de dispositivo del grupo.

3. Desde la página Todos los grupos de recursos , haga clic en el nombre de la columna **Grupos** para mostrar los detalles del grupo de recursos.

   Esta página muestra cada dispositivo que es miembro del grupo de recursos.

Creación de un grupo de recursos dinámico

Puede crear un grupo de recursos de un conjunto dinámico de dispositivos gestionados a partir de un conjunto de criterios.

Acerca de esta tarea

Puede crear un grupo de recursos dinámico utilizando uno o más de los siguientes criterios para cada tipo de dispositivo.

Criterios	Chasis	Chasis denso	Servido-res	Conmuta-dor Flex System	Conmuta-dor RackS-witch	Dispositi-vo de almace-namiento
Nombre de tarjeta de complemento			✓ (excepto ThinkSer-ver)			
Contacto	✓		✓		✓	✓

Criterios	Chasis	Chasis denso	Servido-res	Conmuta-dor Flex System	Conmuta-dor RackS-witch	Dispositi-vo de almace-namiento
Descripción	✓	✓	✓		✓	✓
Nombre de dominio completamente calificado	✓		✓			
Nombre de host	✓		✓	✓	✓	
Dirección IPv4*	✓		✓	✓	✓	✓
Dirección IPv6	✓		✓	✓	✓	
Ubicación	✓	✓	✓		✓	✓
Tipo de máquina	✓		✓	✓	✓	✓
Modelo	✓		✓	✓	✓	✓
Estado general	✓		✓	✓	✓	✓
Núcleos del procesador			✓			
Nombre del producto	✓		✓	✓	✓	✓
Bastidor	✓	✓	✓		✓	✓
Sala	✓	✓	✓		✓	✓
Nombre definido por el usuario	✓	✓	✓	✓	✓	✓

Nota: En el caso de las direcciones IPv4, puede especificar una única dirección o un rango de direcciones, separadas por un guion o utilizando un asterisco como comodín (por ejemplo, `1.1.1.*` o `1.1.1.1-1.1.1.255`, sin espacios).

Procedimiento

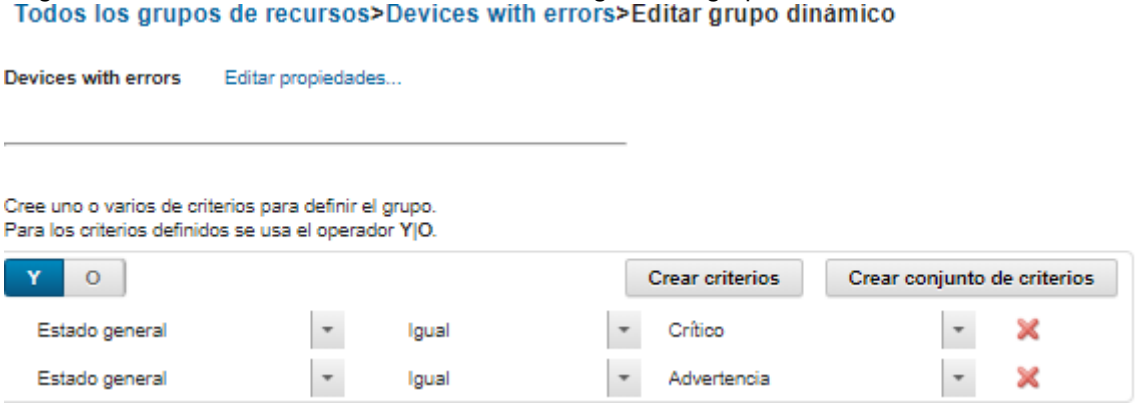
Para crear y rellenar un grupo de recursos dinámico, lleve a cabo los siguientes pasos.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Hardware → Grupos de recursos**. Aparecerá la página Todos los grupos de recursos.

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

Paso 3. Seleccione **Grupo dinámico** para agrupar dispositivos a partir de un conjunto de criterios.

Paso 4. Haga clic en **Crear**. Se muestra el cuadro de diálogo Editar grupo dinámico.



Paso 5. Agregue los criterios para este grupo dinámico.

- Seleccione el operador que se utilizará para el conjunto de grupos. Puede presentar uno de los valores siguientes:
  - **AND**. Los miembros deben cumplir todos los valores especificados.
  - **OR**. Los miembros deben cumplir uno o más de los valores especificados.
- Haga clic en **Crear criterio** para añadir un nuevo criterio al conjunto.
- Haga clic en **Crear conjunto de criterios** para añadir un subconjunto de criterios.

Nota: Los criterios y conjuntos de criterios nuevos siempre se agregan a la parte inferior de la lista.

Paso 6. Haga clic en **Aplicar** para guardar los criterios de un grupo y crear el grupo, o bien haga clic en **Vista previa** para ver los dispositivos que se incluyen en el grupo usando los criterios actuales, sin necesidad de crear el grupo.

Después de finalizar

- Puede ver los grupos de recursos a los que pertenece un dispositivo desde la columna **Grupos** en las páginas todos los dispositivos y las páginas resumen de dispositivo.
- Puede modificar los criterios para el grupo dinámico al seleccionar el grupo de recursos y al hacer clic en el icono **Editar** ( ).
- Puede modificar las propiedades del grupo de recursos al hacer clic en **Todas las acciones → Editar propiedades**.

Creación de un grupo de recursos estático

Puede crear un grupo de recursos que contienen un conjunto personalizado de dispositivos gestionados.

Procedimiento

Para crear y rellenar un grupo de recursos estático, lleve a cabo los siguientes pasos.

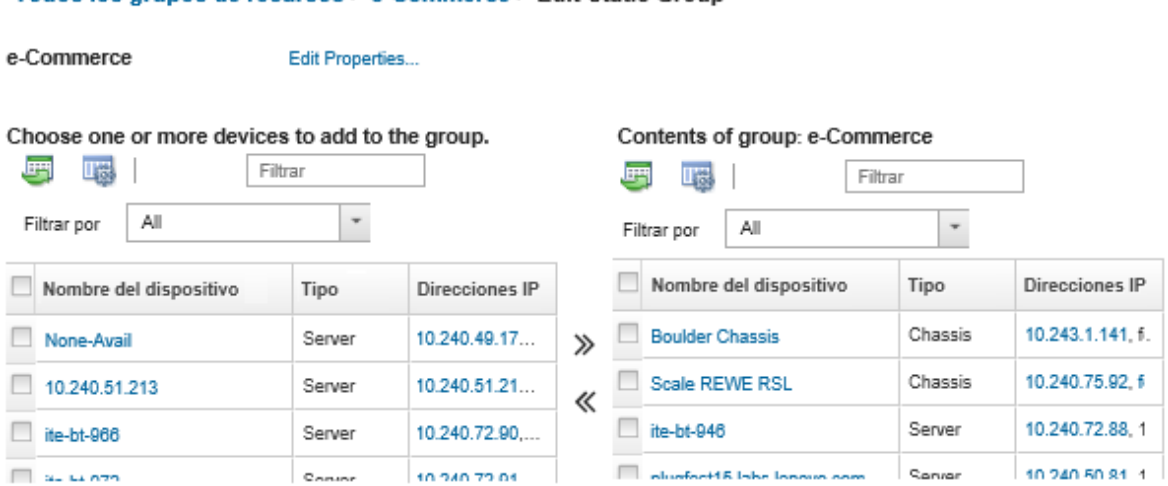
Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Hardware → Grupos de recursos**. Aparecerá la página Grupos de recursos.

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

Paso 3. Especifique el nombre del grupo y una descripción opcional.

Paso 4. Seleccione **Grupo estático** para crear un grupo de dispositivos definidos de forma explícita.

Paso 5. Haga clic en **Crear**. Se muestra la página Editar grupo estático.



Paso 6. Seleccione los dispositivos que desee agregar al grupo de la lista **Todos los dispositivos disponibles fuera del grupo** y haga clic en el icono **Añadir** (») para mover los dispositivos seleccionados para la lista **Contenidos del grupo**.

Notas:

- Puede ordenar las listas para que sea más fácil encontrar dispositivos específicos haciendo clic en los encabezados de columna. Además, puede seleccionar un tipo de dispositivo de la lista desplegable **Filtrar por**, seleccionar un chasis desde la lista desplegable, o introducir texto (como un nombre o dirección IP) en el campo **Filtro** para mostrar solo los dispositivos que cumplen los criterios seleccionados.
- Si elige mover un chasis en el grupo, los dispositivos en el chasis no se agregan automáticamente al grupo. Para añadir todos los componentes del chasis al grupo, seleccione **Chasis → <*chassis_name*>** en el menú desplegable **Mostrar** para enumerar todos los componentes del chasis especificado, seleccione la casilla de verificación junto al encabezado de la columna Nombre de dispositivo para seleccionar todos los dispositivos y luego haga clic en el icono **Añadir** (») para mover los dispositivos seleccionados a la lista **Contenidos del grupo**.

Después de finalizar

- Puede ver los grupos de recursos a los que pertenece un dispositivo desde la columna **Grupos** en las páginas todos los dispositivos y las páginas resumen de dispositivo.
- Puede agregar o quitar un dispositivo de un grupo de recursos estático de las páginas de todos los dispositivos y las páginas de detalles del dispositivo al hacer clic en **Todas las acciones → Grupos → Añadir a grupo** o **Todas las acciones → Grupos → Quitar del grupo**.

  Nota: Puede agregar y quitar dispositivos solo de los grupos de recursos estáticos. No se pueden quitar de los grupos dinámicos.
- Puede modificar las propiedades del grupo de recursos al hacer clic en **Todas las acciones → Editar propiedades**.

Extracción de un grupo de recursos

Puede quitar un grupo de recursos de Lenovo XClarity Administrator.

Acerca de esta tarea

Eliminar un grupo solo elimina la definición de mismo. No afecta a los dispositivos que lo componen.

Procedimiento

Complete los pasos siguientes para quitar un grupo de recursos.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Hardware → Grupos de recursos**. Aparecerá la página Todos los grupos de recursos.

La página Todos los grupos de recursos genera una lista de cada grupo de recursos, incluido el nombre del grupo, el número de dispositivos gestionados que están en el grupo y el estado del dispositivo que tiene la máxima gravedad en el grupo.

Paso 2. Seleccione el grupo de recursos que va a quitar.

Paso 3. Haga clic en el icono **Eliminar** (✖).

Paso 4. Haga clic en **Eliminar**.

Modificación de propiedades de grupo de recursos

Puede modificar las propiedades de grupos de recursos específicos.

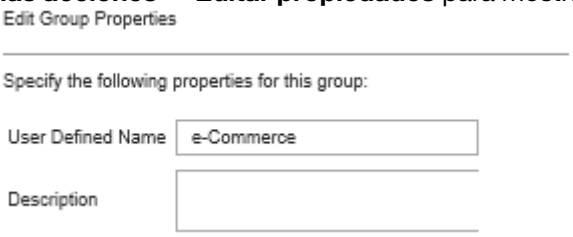
Procedimiento

Complete los pasos siguientes para modificar las propiedades del grupo de recursos.

Paso 1. Desde la barra de menús de XClarity Administrator, haga clic en **Hardware → Grupos de recursos** para mostrar la página Todos los grupos de recursos

Paso 2. Seleccione el grupo de recursos que va a actualizar

Paso 3. Haga clic en **Todas las acciones → Editar propiedades** para mostrar el cuadro de diálogo Editar



grupos de recursos.

Paso 4. Cambie la siguiente información según sea necesario.
- Nombre de grupo
- Descripción

Paso 5. Haga clic en **Guardar**.

Nota: Al cambiar estas propiedades, pueden transcurrir unos instantes antes de que los cambios aparezcan en la interfaz web de XClarity Administrator

Capítulo 6. Gestión de bastidores

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

Antes de empezar

Después de mover un nodo de un chasis a otro, espere 5 a 10 minutos antes de intentar editar los bastidores en XClarity Administrator que contienen el chasis.

Cuando se mueve un dispositivo fuera de un bastidor, se borran el nombre del bastidor y los valores de la unidad más baja del bastidor en el inventario de dispositivos. No se borran los valores de sala y ubicación.

Acerca de esta tarea

En este procedimiento se describe cómo crear y rellenar de forma interactiva un único bastidor con dispositivos gestionados y rellenos.

Si necesita añadir muchos dispositivos a bastidores o bien editar muchos bastidores, plantéese la posibilidad de utilizar una hoja de cálculo para llevar a cabo una importación masiva o para implementar un script de PowerShell para automatizar la tarea. Para obtener más información sobre cómo utilizar la importación masiva, consulte Gestión del chasis y Gestión de servidores. Para obtener más información sobre los scripts de PowerShell, consulte Kit de utilidades PowerShell (LXCAPSTool) en la documentación en línea de XClarity Administrator.

XClarity Administrator reconoce las propiedades del bastidor que se definen en un dispositivo gestionable. Cuando se gestiona dicho dispositivo, XClarity Administrator establece las propiedades del sistema para ese dispositivo y actualiza la vista de bastidores. Si el bastidor no existe en XClarity Administrator, se crea un nuevo bastidor y el dispositivo se agrega al mismo.

Notas:

- Los servidores de System x3500 M5, los servidores NeXtScale nx360 M5, los servidores ThinkServer SD350 y los servidores de torre no se admiten en la vista de bastidores.
- Para sistemas complejos escalables System x3850 X5, debe añadir cada nodo (servidor) al bastidor de forma individual.
- Cuando XClarity Administrator se reinicia, el hardware de demostración no es persistente en las vistas de bastidor.

Procedimiento

Para crear y llenar bastidores, complete los siguientes pasos.

- Cree y rellene un solo bastidor con dispositivos gestionados.
  1. En la barra de menús de XClarity Administrator, haga clic en **Hardware → Bastidores**. Se muestra la página Todos los bastidores.

     En la página Todos los bastidores cada bastidor se muestra como una imagen en miniatura junto con el nombre de los dispositivos gestionados que están en el bastidor, así como el estado del dispositivo que tiene la máxima gravedad.

Notas: Puede filtrar los bastidores por gravedad pulsando en los iconos siguientes de la barra de herramientas. También puede introducir el nombre de un bastidor en el campo **Filtro** para filtrar mejor los bastidores que se muestran.

- Icono **Alertas críticas** ( )
- Icono **Alertas de advertencia** ( )
- Icono **Alertas normales** ( )

2. Haga clic en el icono **Crear** ( ) para crear un bastidor vacío. Se muestra el cuadro de diálogo Crear bastidor vacío.
3. Indique el nombre del bastidor, la altura, la ubicación y la sala en el cuadro de diálogo.

   Notas:

   - Los nombres de bastidor no tienen que ser exclusivos. Puede crear bastidores con el mismo nombre siempre que la ubicación, la sala o ambas sean diferentes.
   - El nombre del bastidor solo puede incluir las letras mayúsculas y minúsculas, los números y los siguientes caracteres especiales: punto (.), guion (-) y carácter de subrayado (_).
   - La ubicación puede tener un máximo de 23 caracteres.
4. Haga clic en **Crear**. Se añade una imagen en miniatura del bastidor nuevo a la página Todos los bastidores.
5. Haga clic en dos veces la imagen en miniatura del bastidor. Se muestra la página Vista del bastidor con una imagen del bastidor vacío y las propiedades de dicho bastidor.

6. Haga clic en **Editar bastidor** para mostrar la página Editar bastidor.

7. Agregue todos los dispositivo gestionados y rellenos adecuados a la vista gráfica.

   Nota: Solo los dispositivos gestionados en estado En línea se pueden agregar al bastidor.

   - Haga clic en la pestaña **Chasis** para ver una lista de chasis gestionados que no se han añadido a un bastidor. Arrastre un chasis gestionado y suéltelo en la ubicación deseada del bastidor para añadir dicho chasis al bastidor.
   - Haga clic en la pestaña **Alojamientos del servidor** para ver una lista de los alojamientos de servidores de bastidor gestionados y de servidores de varios nodos que no se han añadido a un bastidor. Arrastre un servidor de bastidor o varios alojamientos de servidor y suéltelos en la ubicación deseada del bastidor para añadir el servidor de bastidor al bastidor.
   - Haga clic en la pestaña **RackSwitch** para ver una lista de conmutadores RackSwitch gestionados que no se han añadido a un bastidor. Arrastre un conmutador RackSwitch y suéltelo en la ubicación deseada para añadir dicho conmutador al bastidor.
   - Haga clic en la pestaña **Almacenamiento** para ver una lista de diversos dispositivos de almacenamiento. Arrastre el dispositivo de almacenamiento apropiado y suéltelo en la ubicación deseada del bastidor para agregar dicho dispositivo de almacenamiento al bastidor.

– Haga clic en la pestaña **Rellenos** para ver una lista de diversos rellenos. Arrastre el relleno apropiado y suéltelo en la ubicación deseada para añadir dicho relleno al bastidor.

  Un *relleno* es cualquier dispositivo que se encuentre en el bastidor que no está gestionado mediante XClarity Administrator. Existen los siguientes rellenos:
  – Rellenos genéricos
  – RackSwitch genéricos
  – Controladores y alojamientos de controladores de almacenamiento
  – Controladores y alojamientos de almacenamiento de socios (como IBM, NetApp y EMC)

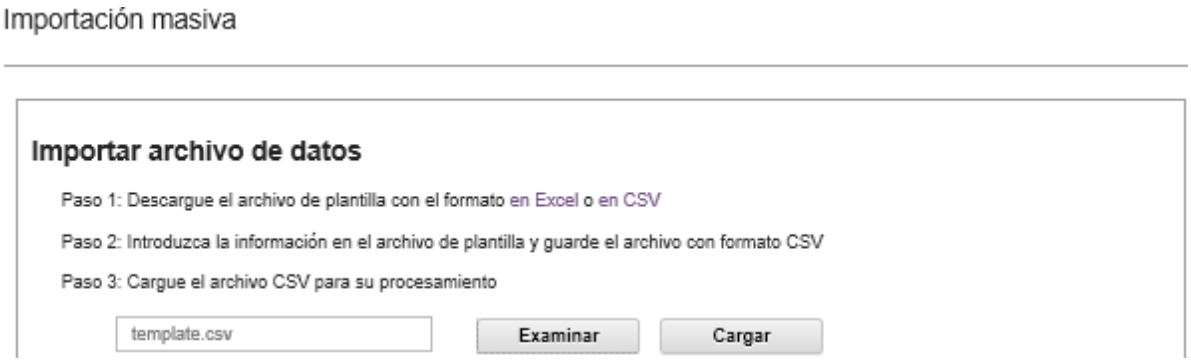
  – Las propiedades de ubicación, sala, bastidor y unidad de bastidor más baja se actualizan para el dispositivo cuando se agregan o quitan dispositivos de un bastidor.
  – Puede ordenar la lista de dispositivos de cada pestaña utilizando la lista desplegable **Ver por**. Además, puede introducir texto (como un nombre o una dirección IP) en el campo **Filtro** para aplicar filtros avanzados a los dispositivos que se muestran.
  – Puede quitar dispositivos y rellenos gestionados del bastidor. Para ello, arrastre los objetos y suéltelos fuera del bastidor.

8. Haga clic en **Guardar** para guardar la configuración del bastidor.

   El proceso de configuración puede tardar varios minutos en finalizar. Durante la configuración, la información del bastidor y de la ubicación se transfiere al CMM o al controlador de gestión de la placa base de los dispositivos gestionados.
9. Personalice los rellenos que ha añadido al bastidor pulsando el relleno y pulsando **Editar propiedades** a continuación. El cuadro de diálogo Editar propiedades le permite especificar un nombre, la unidad de bastidor más baja (LRU) y la URL que debe utilizarse para iniciar la interfaz de usuario de gestión para dicho dispositivo.

   Consejo: una vez guardada la configuración del bastidor, puede iniciar la interfaz de usuario de gestión de un relleno haciendo clic en el mismo en el bastidor y haciendo clic en el vínculo **Abrir URL** a continuación.

- Cree y llene bastidores utilizando un archivo de importación masiva.
  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 **Importación masiva**. Se muestra el cuadro de asistente de Importación masiva.

  3. 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.
  4. Complete la hoja de cálculo de datos en el archivo de plantilla y guarde el archivo en formato CSV.

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 bastidores en el archivo de importación masiva, complete las siguientes columnas requeridas.
- (Columnas A) Especifique el “bastidor” para el tipo de dispositivo.
- (Columnas V) Especifique el nombre del bastidor.
- (Columnas X) Especifique 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.

En la figura siguiente se muestra un ejemplo del archivo de importación masiva con bastidores definidos.

A	V	W	X
Type	Rack name	Lowest rack unit	Height
rack	Rack_01		37
rack	Rack_02		52

Nota: Puede utilizar el mismo archivo de importación masiva para gestionar dispositivos y agregar esos dispositivos a un bastidor (consulte Gestión de sistemas en la documentación en línea de Lenovo XClarity Administrator).

5. 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.
6. Haga clic en **Cargar** para cargar y validar el archivo.
7. Haga clic en **Siguiente** para mostrar la página de Resumen de entrada con una lista de bastidores y otros dispositivos a gestionar y revisar el resumen de los bastidores y otros dispositivos que desee gestionar.
8. Haga clic en **Siguiente** para mostrar la página de Credenciales del dispositivo. 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.

9. 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 página 179.

Después de finalizar

Puede cambiar la preferencia de orden de numeración de bastidor (consulte Establecer preferencias de inventario).

Visualización del estado de los dispositivos de un bastidor

Para cada bastidor, puede visualizar el estado de todos dispositivos gestionados en el bastidor.

Procedimiento

Realice una o varias de las acciones siguientes para ver el estado de todos los dispositivos de un bastidor.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Panel**. Se muestra la página del panel con una descripción general y el estado de todos los dispositivos gestionados y otros recursos, incluidos los bastidores.

Paso 2. En la barra de menús de XClarity Administrator, haga clic en **Hardware → Bastidores**. Se muestra la página Bastidores.

En la página Bastidores cada bastidor se muestra como una imagen en miniatura junto con el nombre de los dispositivos gestionados que están en el bastidor, así como el estado del dispositivo que tiene la máxima gravedad.

Notas: Puede ordenar la lista por nombre de bastidor, número de dispositivos en el bastidor o gravedad para hacer que sea más fácil encontrar bastidores específicos. El orden se ordena de

izquierda a derecha, de arriba hacia abajo. Además, puede filtrar los bastidores por gravedad pulsando los siguientes iconos de la barra de herramientas o introducir el nombre de un bastidor en el campo **Filtro** para filtrar más los bastidores que se muestran.

- Icono **Alertas críticas** ( )
- Icono **Alertas de advertencia** ( )
- Icono **Alertas normales** ( )

Paso 3. En la página Todos los bastidores, haga clic en el nombre del bastidor o haga clic dos veces en la miniatura del bastidor para mostrar la vista gráfica y las propiedades de dicho bastidor.

La *vista de bastidores* es una vista gráfica del bastidor delantero, que muestra todos los dispositivos del bastidor, incluidos los chasis, los servidores de bastidor y de torre, los conmutadores de la parte superior del bastidor y los rellenos. El icono de estado de cada dispositivo indica su estado actual.

Desde esta página puede llevar a cabo las siguientes acciones:

- Agregar o quitar dispositivos en el bastidor pulsando **Editar bastidor**.

  Nota: Al cambiar los componentes del bastidor, pueden transcurrir unos instantes antes de que la información aparezca en la interfaz de XClarity Administrator.
- Modifique las propiedades del dispositivo y del filtro (lo que incluye el nombre, ubicación y la URL para iniciar la interfaz web de gestión) al hacer clic en el dispositivo o relleno y, a continuación, al hacer clic en **Editar propiedades**, ubicado en el panel de resumen del dispositivo.
- Visualice la interfaz web del controlador de gestión para un dispositivo o relleno al hacer clic en el dispositivo o relleno; a continuación, haga clic en el enlace **Abrir URL**, situado en el panel de resumen del dispositivo.

Paso 4. Mostrar un resumen o un estado detallado de un dispositivo o componente:

a. Haga clic en un dispositivo o componente del bastidor para mostrar el resumen de estado y las propiedades y el estado para el dispositivo o el componente.

b. Haga clic en dos veces un dispositivo para visualizar la página de los detalles del dispositivo.

Procedimiento

Puede cambiar la preferencia de orden de numeración de bastidor (consulte Establecer preferencias de inventario).

Eliminación de un bastidor

Puede quitar un bastidor de Lenovo XClarity Administrator.

Procedimiento

Para quitar un bastidor, lleve a cabo los pasos siguientes.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Hardware → Bastidores**. Se muestra la página Todos los bastidores.

En la página Todos los bastidores cada bastidor se muestra como una imagen en miniatura junto con el nombre de los dispositivos gestionados que están en el bastidor, así como el estado del dispositivo que tiene la máxima gravedad.

Notas: Puede ordenar la lista por nombre de bastidor, número de dispositivos en el bastidor o gravedad para hacer que sea más fácil encontrar bastidores específicos. El orden se ordena de izquierda a derecha, de arriba hacia abajo. Además, puede filtrar los bastidores por gravedad pulsando los siguientes iconos de la barra de herramientas o introducir el nombre de un bastidor en el campo **Filtro** para filtrar más los bastidores que se muestran.

- Icono **Alertas críticas** ( )
- Icono **Alertas de advertencia** ( )
- Icono **Alertas normales** ( )

Paso 2. Seleccione la miniatura del bastidor para quitarlo.

Paso 3. Haga clic en el icono **Quitar** ( ).

Paso 4. Haga clic en **Eliminar**.

Resultados

La miniatura del bastidor se quita de la página Todos los bastidores y todos los dispositivos que estaban en el bastidor pueden incluirse ahora en otro bastidor en la página Editar bastidores.

Capítulo 7. Gestión del chasis

Lenovo XClarity Administrator puede gestionar varios tipos de sistemas, incluido el chasis de Flex System.

Más información: XClarity Administrator: detección

Antes de empezar

Nota: Los componentes del chasis (como CMM, nodos de cálculo Flex y conmutadores Flex) 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.

Antes de gestionar los chasis, asegúrese de que se cumplan las siguientes condiciones:

- Revise las consideraciones de gestión antes de gestionar un dispositivo. Para obtener información, consulte Consideraciones de gestión en la XClarity Administrator documentación en línea.
- Algunos puertos deben estar disponibles para comunicarse con el CMM para que el chasis esté gestionado. Asegúrese de que estos puertos estén disponibles antes de intentar gestionar un chasis. Para obtener más información sobre los puertos, consulte Disponibilidad de puertos en la documentación en línea de XClarity Administrator.
- Asegúrese de que el firmware mínimo necesario esté instalado en cada chasis 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 el valor de **Número de sesiones activas simultáneas para usuarios de LDAP** en el CMM esté configurado en 0 (cero) para el chasis. Puede verificar este valor en la interfaz web de CMM haciendo clic en **Gestión del módulo de gestión → Cuentas de usuario**, haga clic en **Valores de inicio de sesión globales** y, a continuación, haga clic en la pestaña **General**.
- 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.
- Para descubrir un chasis que está en una subred *distinta* de XClarity Administrator, asegúrese de que se cumpla una de las siguientes condiciones:
  - 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.
  - Si SLP está deshabilitado en el punto final o en la red, puede utilizar el método de detección de DNS en su lugar al agregar manualmente un registro de servicio (registro SRV) al servidor de nombres de dominio (DNS), como, por ejemplo, para XClarity Administrator.
    ```
    _lxca._tcp.labs.lenovo.com      service = 0 0 443 fvt-xhmc3.labs.lenovo.com.
    ```
    A continuación, habilite el descubrimiento de DNS en CMM desde la interfaz web de gestión, al hacer clic en **Gestión del módulo de gestión → Protocolo de red**, en la pestaña **DNS** y al seleccionar **Usar DNS para descubrir Lenovo XClarity Administrator**.

    Notas:

    - El CMM se debe ejecutar en el nivel de firmware con fecha de mayo de 2017 para admitir descubrimiento automático utilizando DNS.

- Si hay múltiples instancias de XClarity Administrator en su entorno, el chasis se descubrirá solo por la instancia que es la primera a responder a la solicitud de descubrimiento. El chasis no se descubrirá en todas las instancias.

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).

Atención: Si pretende gestionar CMM que están ejecutando un nivel de firmware de la pila Flex versión 1.3.2.1 2PET12K a 2PET12Q y estos han estado en ejecución durante más de tres semanas y se encuentran en una configuración de CMM dual, debe reubicar virtualmente los CMM antes de actualizar el firmware utilizando XClarity Administrator.

Importante: 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.

Acerca de esta tarea

XClarity Administrator puede detectar automáticamente el chasis en su entorno, sondeando los sistemas gestionables que se encuentran en la misma subred IP, como XClarity Administrator. Para detectar los chasis que están en otras subredes, especifique una dirección IP o un rango de direcciones IP, o importe la información de una hoja de cálculo.

Una vez que XClarity Administrator gestiona los chasis, XClarity Administrator sondea todos los chasis gestionados periódicamente para recopilar información, como el inventario, los datos de producto fundamentales y el estado. Puede consultar y supervisar cada chasis gestionado y realizar acciones de gestión (como configurar la información del sistema, los valores de red y la conmutación por error). Para los chasis que están en modo protegido, las acciones de gestión están deshabilitadas.

Se gestiona a los chasis mediante *autenticación gestionada de XClarity Administrator*.

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:

  - 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.

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

  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.

Un dispositivo solo puede estar gestionado 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. Si se produce un error durante el proceso de anulación de la gestión, puede seleccionar la opción **Forzar gestión** durante la gestión del nuevo XClarity Administrator.

Nota: Cuando explora la red en busca de dispositivos gestionables, XClarity Administrator no reconoce si un dispositivo ya está gestionado por otro gestionador hasta después de intentar gestionar el dispositivo.

Durante el proceso de gestión, XClarity Administrator realiza las siguientes acciones:

- Inicia sesión en el chasis utilizando las credenciales proporcionadas.
- Recopila el inventario de todos los componentes de cada chasis, como el CMM, los nodos de cálculo, los dispositivos de almacenamiento y los Conmutadores Flex.

  Nota: Algunos datos del inventario se recopilan una vez completado el proceso de gestión. El chasis permanece en el estado Pendiente hasta que se recopilan todos los datos del inventario. No puede realizar ciertas tareas en un dispositivo gestionado, como el despliegue de un patrón de servidor, hasta que se hayan recopilado todos los datos de inventario para dicho dispositivo y el chasis ya no se encuentre en el estado Pendiente.
- Configura los valores del servidor NTP de forma que todos los dispositivos gestionados utilicen el servidor NTP desde XClarity Administrator.
- Asigna la última política de cumplimiento de firmware editada para el chasis.
- Para los dispositivos Flex de Lenovo, opcionalmente configura las reglas de firewall de los dispositivos para que solo se acepten las solicitudes entrantes de XClarity Administrator.
- Intercambia certificados de seguridad con el CMM, copia el certificado de seguridad del CMM en el almacén de confianza de XClarity Administrator y envía el certificado de seguridad de la CA de XClarity Administrator al CMM. El CMM carga el certificado en el almacén de confianza del CMM y lo distribuye a los procesadores de servicios del nodo de cálculo para incluirlo en sus almacenes de confianza.
- Configura la autenticación gestionada. Se cambian los valores del cliente LDAP del CMM para utilizar XClarity Administrator como servidor de autenticación y se cambian los valores de inicio de sesión globales del CMM a **Servidor de autenticación externo únicamente**. Para obtener más información acerca de autenticación gestionada, consulte Gestión del servidor de autenticación.
- Crea la cuenta de usuario de recuperación (`RECOVERY_ID`). Para obtener más información acerca de la cuenta `RECOVERY_ID`, consulte Gestión del servidor de autenticación.

Atención: Cuando gestiona un chasis, XClarity Administrator cambia el número máximo de conexiones simultáneas en el modo de comandos TCP seguro a 15 y, además, establece el número máximo de

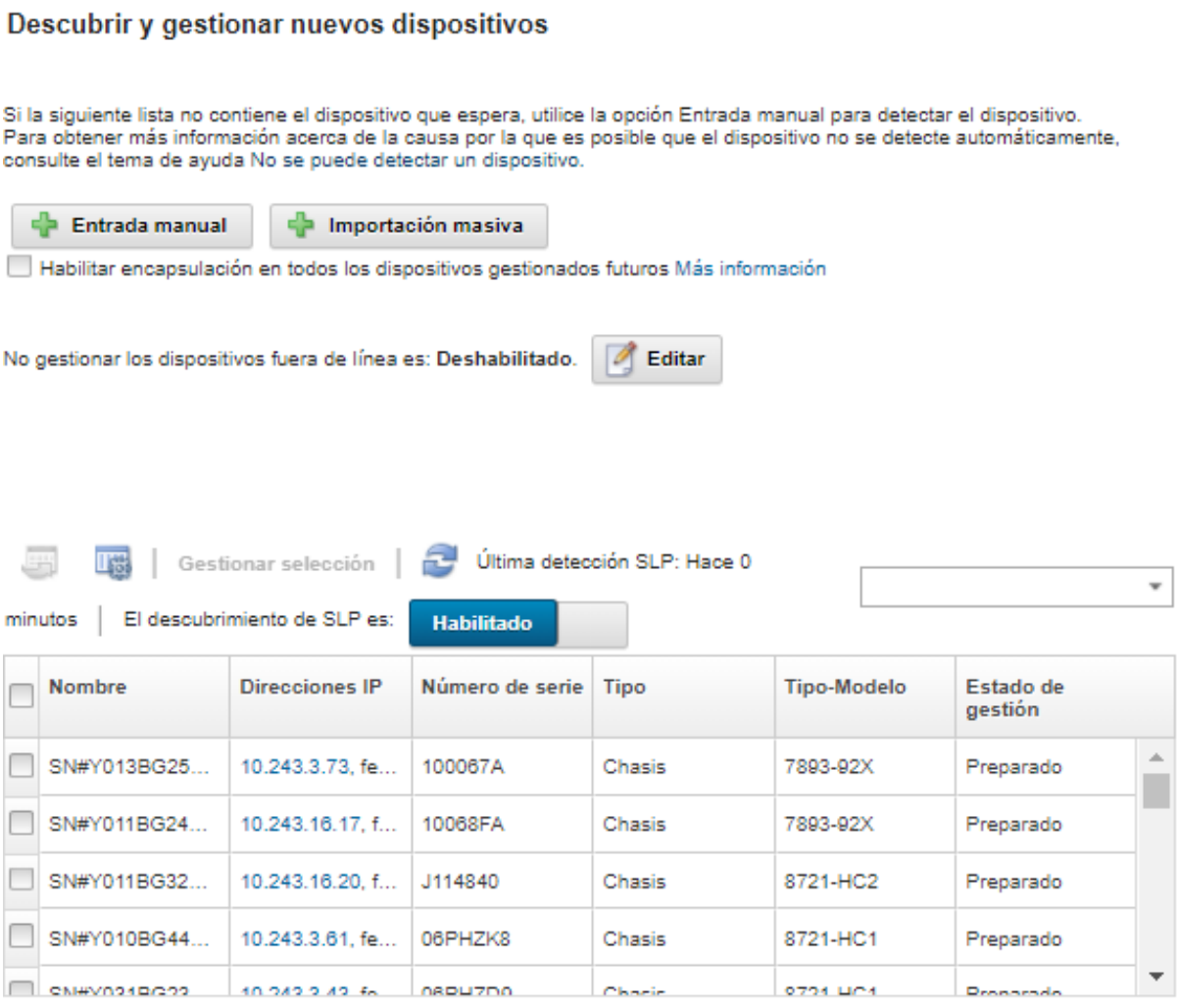
conexiones simultáneas en el modo de comando TCP heredado a 0, lo que anula los valores que haya podido establecer con anterioridad en el CMM.

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 chasis (consulte Configuración de valores de criptografía en el servidor de gestión).

Procedimiento

Lleve a cabo uno de los procedimientos siguientes para detectar y gestionar su chasis utilizando XClarity Administrator.

- Detecte y gestione un gran número de chasis y otros dispositivos utilizando un archivo de importación masiva (consulte Gestión de sistemas en la documentación en línea de Lenovo XClarity Administrator).
- Detecte y gestione chasis que están en la misma subred IP que XClarity Administrator.
  1. En la barra de menús de XClarity Administrator, pulse **Hardware → Detectar y gestionar dispositivos nuevos**. Se muestra la página Detectar y gestionar dispositivos nuevos.



Puede ordenar las columnas de la tabla para que sea más fácil encontrar el chasis que desea gestionar. Además, puede introducir texto (como un nombre de sistema o una dirección IP) en el

campo **Filtro** para filtrar mejor los chasis que se muestran. Puede cambiar las columnas que se muestran el orden predeterminado haciendo clic en el icono **Personalizar columnas** ().

2. Haga clic en el icono **Actualizar** () para descubrir todos los dispositivos gestionables en el dominio XClarity Administrator. La detección puede durar varios minutos.
3. 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.

   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 archivo lenovoMgrAlert.mib y la Recuperación de la gestión con un CMM después de un error en el servidor de gestión.
4. Seleccione el chasis o los chasis que desee gestionar.
5. Haga clic en **Gestionar selección**.
6. Seleccione utilizar autenticación gestionada o autenticación local de XClarity Administrator para este dispositivo. Se selecciona autenticación gestionada de forma predeterminada. Para utilizar autenticación local, elimine la selección de **Autenticación gestionada**.

   Nota: No se admite la autenticación gestionada y local para servidores ThinkServer y System x M4.
7. Elija el tipo de credenciales a utilizar para el dispositivo y especifique las credenciales adecuadas:
   - **Usar credenciales ingresadas manualmente**
     - Especifique el Id. de usuario y la contraseña local con autoridad de **lxc-supervisor** para la autenticación con el CMM.
     - (Opcional) Especifique una contraseña nueva para la cuenta de usuario del CMM si la contraseña del dispositivo caducó.
   - **Usar credenciales almacenadas**

     Seleccione la credencial almacenada con autoridad de **lxc-supervisor** para este dispositivo gestionado. Puede añadir las credenciales almacenadas al hacer clic en **Gestionar las credenciales almacenadas**.

     Nota: Si elige utilizar autenticación local, debe seleccionar una credencial almacenada para gestionar el dispositivo.

   Consejo: se recomienda usar una cuenta de supervisor o administrador para gestionar el dispositivo. Si se utiliza una cuenta con autoridad de nivel inferior, la gestión puede fallar, o la gestión puede finalizar correctamente, pero otras operaciones de XClarity Administrator futuras en el dispositivo pueden fallar (especialmente si el dispositivo se gestiona sin autenticación gestionada).

   Para obtener más información sobre credenciales normales y almacenadas, consulte Gestión de cuentas de usuario, Gestión de credenciales almacenadas.
8. Si se selecciona autenticación gestionada, especifique la contraseña de recuperación.

   Se crea una cuenta de recuperación (`RECOVERY_ID`) en el CMM y se deshabilita todas las cuentas de usuario locales. En caso que se presente un problema con XClarity Administrator y deje de funcionar por alguna razón, *no se puede* iniciar sesión en el CMM utilizando las cuentas de usuarios normales. Sin embargo, puede iniciar sesión utilizando la cuenta `RECOVERY_ID`.

   Nota:

- La contraseña de recuperación es obligatoria si elige utilizar autenticación gestionada, pero no se permite si elige utilizar autenticación local.
- Puede elegir utilizar una cuenta de recuperación local o credenciales de recuperación almacenadas. En cualquier caso, el nombre de usuario siempre es `RECOVERY_ID`.
- 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.

Para obtener más información acerca del Id. de recuperación, consulte Gestión del servidor de autenticación.

9. Haga clic en **Cambiar** para cambiar los grupos de roles que se pueden asignar a los dispositivos.

   Notas:

   - Puede seleccionar desde una lista de grupos de roles que están asignados al usuario actual.
   - Si no cambia los grupos de roles, se utilizan los grupos de roles predeterminados. Para obtener más información acerca de los grupos de roles predeterminados, consulte Cambiar los permisos predeterminados.

10. Haga clic en **Gestionar**.

    Se visualiza un cuadro de diálogo que muestra el progreso de este proceso de gestión. Para asegurarse de que el proceso se completa satisfactoriamente, supervise el progreso.

    Una vez finalizado el proceso, el cuadro de diálogo muestra el número de dispositivos del chasis y el estado de este último.

    Nota: Algunos datos del inventario se recopilan una vez completado el proceso de gestión. El chasis permanece en el estado Pendiente hasta que se recopilan todos los datos del inventario. No puede realizar ciertas tareas en un dispositivo gestionado, como el despliegue de un patrón de servidor, hasta que se hayan recopilado todos los datos de inventario para dicho dispositivo y el chasis ya no se encuentre en el estado Pendiente.

11. Cuando el proceso esté completo, haga clic en **Aceptar**.

    El dispositivo se gestiona ahora mediante XClarity Administrator, que automáticamente sondea los dispositivos gestionados de forma periódica para recopilar información actualizada, como el inventario.

    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.

12. Si se trata de un chasis nuevo, haga clic en **Ir a configuración del chasis** para validar y cambiar los valores de la red de gestión de todo el chasis (incluidos los nodos de cálculo y los conmutadores Flex), así como para configurar 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 los apartados Modificación de los valores IP de gestión de un chasis y Configuración de servidores mediante el uso de patrones de configuración.

- Detecte y gestione chasis que no están en la misma subred IP que XClarity Administrator especificando manualmente las direcciones IP.
  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.

     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 archivo lenovoMgrAlert.mib y la Recuperación de la gestión con un CMM después de un error en el servidor de gestión.
  3. Seleccione **Entrada manual**.
  4. Especifique las direcciones de red de los chasis que desee gestionar:
     - Haga clic en **Sistema único** y especifique una sola dirección IP, nombre de dominio o nombre de dominio totalmente cualificado (FQDN).

       Nota: Para especificar un FQDN, asegúrese de que se haya incluido un nombre de dominio válido en la página de Acceso de red (consulte Configuración del acceso de red).
     - Haga clic en **Varios sistemas** e introduzca un rango de direcciones IP. Para añadir otro rango, haga clic en el icono **Añadir** (). Para quitar un rango haga clic en el icono **Quitar** ().
  5. Haga clic en **Aceptar**.
  6. Seleccione utilizar autenticación gestionada o autenticación local de XClarity Administrator para este dispositivo. Se selecciona autenticación gestionada de forma predeterminada. Para utilizar autenticación local, elimine la selección de **Autenticación gestionada**.

     Nota: No se admite la autenticación gestionada y local para servidores ThinkServer y System x M4.
  7. Elija el tipo de credenciales a utilizar para el dispositivo y especifique las credenciales adecuadas:
     - **Usar credenciales ingresadas manualmente**
       - Especifique el Id. de usuario y la contraseña local con autoridad de **lxc-supervisor** para la autenticación con el CMM.
       - (Opcional) Especifique una contraseña nueva para la cuenta de usuario del CMM si la contraseña del dispositivo caducó.
     - **Usar credenciales almacenadas**

       Seleccione la credencial almacenada con autoridad de **lxc-supervisor** para este dispositivo gestionado. Puede añadir las credenciales almacenadas al hacer clic en **Gestionar las credenciales almacenadas**.

Nota: Si elige utilizar autenticación local, debe seleccionar una credencial almacenada para gestionar el dispositivo.

Consejo: se recomienda usar una cuenta de supervisor o administrador para gestionar el dispositivo. Si se utiliza una cuenta con autoridad de nivel inferior, la gestión puede fallar, o la gestión puede finalizar correctamente, pero otras operaciones de XClarity Administrator futuras en el dispositivo pueden fallar (especialmente si el dispositivo se gestiona sin autenticación gestionada).

Para obtener más información sobre credenciales normales y almacenadas, consulte Gestión de cuentas de usuario, Gestión de credenciales almacenadas.

8. Si se selecciona autenticación gestionada, especifique la contraseña de recuperación.

   Se crea una cuenta de recuperación (`RECOVERY_ID`) en el CMM y se deshabilita todas las cuentas de usuario locales. En caso que se presente un problema con XClarity Administrator y deje de funcionar por alguna razón, *no se puede* iniciar sesión en el CMM utilizando las cuentas de usuarios normales. Sin embargo, puede iniciar sesión utilizando la cuenta `RECOVERY_ID`.

   Nota:

   – La contraseña de recuperación es obligatoria si elige utilizar autenticación gestionada, pero no se permite si elige utilizar autenticación local.
   – Puede elegir utilizar una cuenta de recuperación local o credenciales de recuperación almacenadas. En cualquier caso, el nombre de usuario siempre es `RECOVERY_ID`.
   – 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.

   Para obtener más información acerca del Id. de recuperación, consulte Gestión del servidor de autenticación.

9. Haga clic en **Cambiar** para cambiar los grupos de roles que se pueden asignar a los dispositivos.

   Notas:

   – Puede seleccionar desde una lista de grupos de roles que están asignados al usuario actual.
   – Si no cambia los grupos de roles, se utilizan los grupos de roles predeterminados. Para obtener más información acerca de los grupos de roles predeterminados, consulte Cambiar los permisos predeterminados.

10. Haga clic en **Gestionar**.

    Se visualiza un cuadro de diálogo que muestra el progreso de este proceso de gestión. Supervise el progreso para asegurarse de que el proceso se completa satisfactoriamente.

    Una vez finalizado el proceso, el cuadro de diálogo muestra el número de dispositivos del chasis y el estado de este último.

    Nota: Algunos datos del inventario se recopilan una vez completado el proceso de gestión. El chasis permanece en el estado Pendiente hasta que se recopilan todos los datos del inventario. No puede realizar ciertas tareas en un dispositivo gestionado, como el despliegue de un patrón de servidor, hasta que se hayan recopilado todos los datos de inventario para dicho dispositivo y el chasis ya no se encuentre en el estado Pendiente.

11. Cuando el proceso esté completo, haga clic en **Aceptar**.

    El dispositivo se gestiona ahora mediante XClarity Administrator, que automáticamente sondea los dispositivos gestionados de forma periódica para recopilar información actualizada, como el inventario.

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.

12. Si se trata de un chasis nuevo, haga clic en **Ir a configuración del chasis** para validar y cambiar los valores de la red de gestión de todo el chasis (incluidos los nodos de cálculo y los conmutadores Flex), así como para configurar 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 los apartados Modificación de los valores IP de gestión de un chasis y Configuración de servidores mediante el uso de patrones de configuración.

Después de finalizar

- Detecte y gestione dispositivos adicionales.
- Despliegue las imágenes del sistema operativo en los servidores que todavía no tienen un sistema operativo instalado. Para obtener más información, consulte el apartado Instalación de sistemas operativos en servidores sin sistema operativo.
- Actualice el firmware de los dispositivos que no cumplen las políticas actuales (consulte Actualización de firmware en dispositivos gestionados).
- Agregue los dispositivos recién gestionados al bastidor adecuado para reflejar el entorno físico (consulte Gestión de bastidores).
- Supervise el estado y los detalles del hardware (consulte Visualización del estado de un servidor gestionado).
- Descubra sucesos y alertas (consulte Trabajo con sucesos y Trabajo con alertas).

Visualización del estado de un chasis gestionado

Puede ver un resumen y el estado detallado del chasis gestionado y de los componentes que tiene instalados desde Lenovo XClarity Administrator.

Más información:

- XClarity Administrator: inventario
- XClarity Administrator: supervisión

Acerca de esta tarea

Los siguientes iconos de estado se usan para indicar el estado general del dispositivo. Si los certificados no coinciden, se agrega “(no es de confianza)” se agrega al estado de cada dispositivo aplicable, por ejemplo Advertencia (no es de confianza). Si existe un problema de conectividad o si la conexión del dispositivo no tiene confianza, “(Conectividad)” se agrega al estado del dispositivo aplicable, por ejemplo, Advertencia (Conectividad).

- () Crítico
- () Advertencia
- () Pendiente
- () Informativo
- () Normal
- () Fuera de línea
- () Desconocido

Procedimiento

Lleve a cabo los pasos siguientes para ver el estado de un chasis gestionado.

- Vea información detallada acerca del chasis haciendo clic en el enlace **Detalles** o haciendo clic en **Acciones → Vistas → Detalles**.
- Inicie la interfaz web del CMM del chasis al hacer clic en el vínculo **Dirección IP** (consulte Inicio de la interfaz web del CMM para un chasis).
- Modificar la información (como el contacto con el soporte, la ubicación y la descripción) haciendo clic en **Acciones → Inventario → Editar propiedades**.
- Modificar los valores IP de gestión de todo el chasis, incluidos los nodos de cálculo y los conmutadores Flex, al hacer clic en **Acciones → Inventario → Editar direcciones IP de gestión**.
- Exportar información detallada acerca de uno o varios chasis a un archivo CSV único al seleccionar el chasis y hacer clic en **Acciones → Inventario → Exportar inventario**.

  Nota: Puede exportar datos de inventario para un máximo de 60 dispositivos por vez.

  Consejo: Al importar un archivo CSV en Microsoft Excel, Excel trata los valores de texto que contienen solo números como valores numéricos (por ejemplo, para UUID). Formatee cada celda como texto para corregir este error.
- Solucionar los problemas que puedan surgir entre el certificado de seguridad de Lenovo XClarity Administrator y el certificado de seguridad del CMM del chasis seleccionando un chasis y haciendo clic en **Acciones → Seguridad → Resolver certificados no fiables**.

Visualización de los detalles de un chasis gestionado

Puede ver información detallada sobre el chasis gestionado desde Lenovo XClarity Administrator, incluidos los niveles de firmware, las direcciones IP y el Identificador único universal (UUID).

Más información:

-  XClarity Administrator: inventario
-  XClarity Administrator: supervisión

Acerca de esta tarea

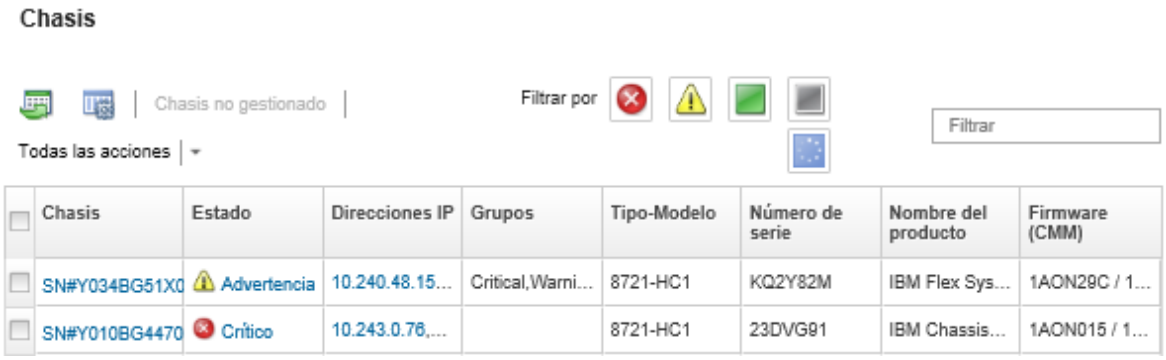
La temperatura del aire en el nivel del sistema se mide mediante un sensor físico en la parte frontal del servidor. Esta temperatura representa la temperatura del aire de entrada que recibe el servidor. Tenga en cuenta que la temperatura del aire notificada por XClarity Administrator y el CMM puede variar si dicha temperatura se captura en diferentes momentos.

Procedimiento

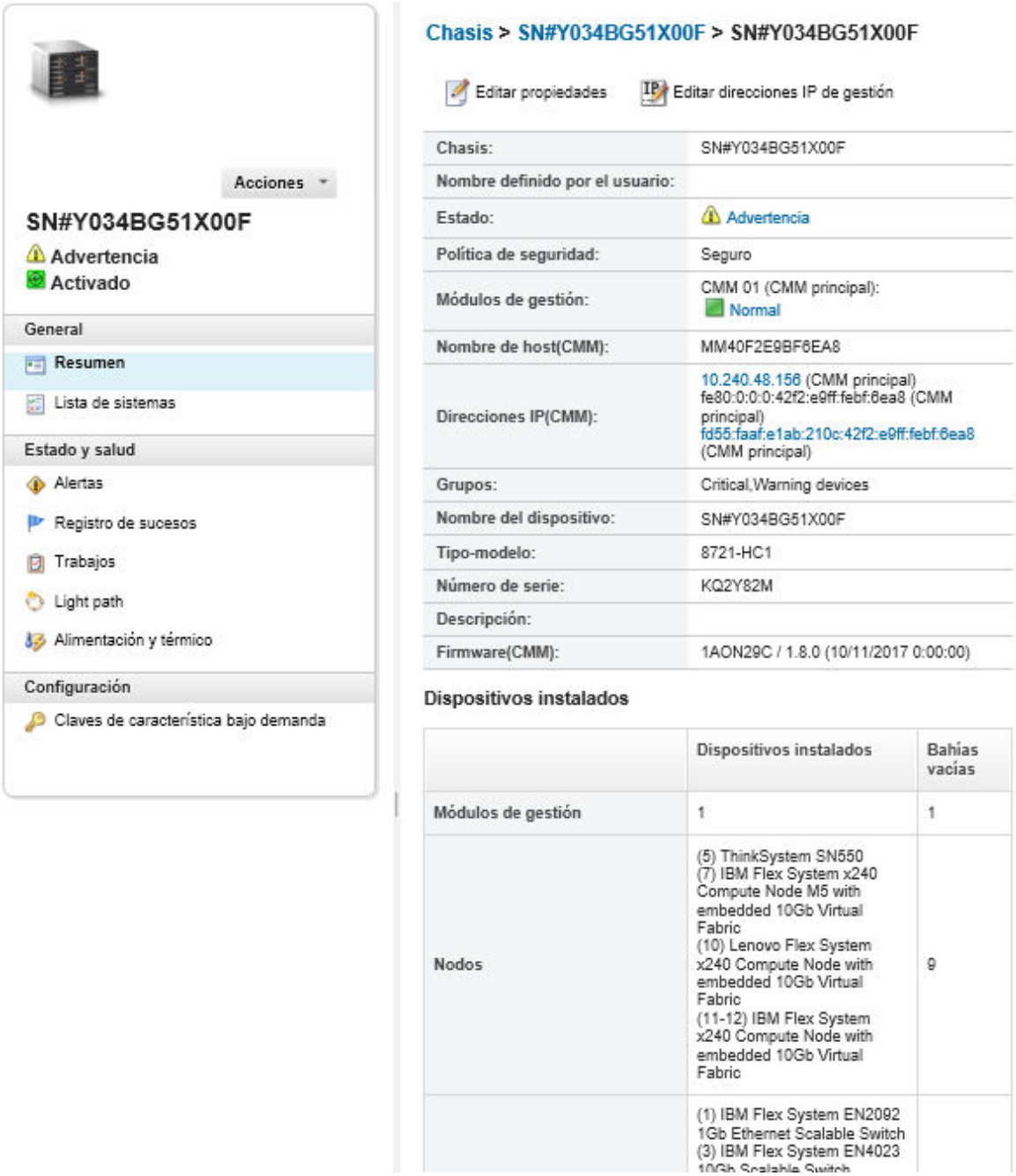
Lleve a cabo los pasos siguientes para ver los detalles de un chasis gestionado.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Hardware → Chasis**. Se muestra la página Chasis con una vista de tabla de todos los chasis gestionados.

Puede ordenar las columnas de la tabla para que sea más fácil encontrar el chasis que desea gestionar. Además, puede introducir texto (como un nombre de chasis o una dirección IP) en el campo **Filtro** para filtrar mejor los chasis que se muestran.



Paso 2. Haga clic en el nombre del chasis en la columna **Chasis**. Aparece la página de resumen de estado de dicho chasis, donde se muestran las propiedades del chasis y una lista de los componentes que están instalados en él.



Paso 3. Lleve a cabo una o más de las acciones siguientes:

- Pulse **Resumen** para ver un resumen del chasis, incluida información del sistema y los componentes instalados (consulte Visualización del estado de un chasis gestionado).
- Haga clic en **Detalles del inventario** para ver detalles sobre los componentes del chasis, incluidos:
  - Niveles de firmware de todos los componentes del chasis.
  - Detalles del CMM, como nombre de host, dirección IPv4, dirección IPv6 y direcciones MAC.
  - Detalles de los activos del chasis y el CMM instalados en el chasis, incluidos el nombre el Identificador único universal (UUID) y la ubicación.

- Pulse **Alertas** para mostrar la lista de las alertas actuales de este chasis (consulte Trabajo con alertas).
- Pulse **Registro de sucesos** para mostrar la lista de los sucesos actuales de este chasis (consulte Supervisión de sucesos en el registro de sucesos).
- Pulse **Trabajos** para mostrar una lista de trabajos asociados con el chasis (consulte Supervisión de trabajos).
- Haga clic en **Light Path** para mostrar el estado actual de los LED del chasis, incluidas la ubicación, los fallos y la información. Esto equivale a ver el panel frontal del chasis.
- Haga clic en **Alimentación y térmico** para mostrar los detalles sobre la alimentación y el flujo de aire.

  Consejo: utilice el botón Actualizar de su navegador web para recopilar los datos de alimentación y térmicos más recientes. La recopilación de datos puede durar varios minutos.
- Haga clic en **Claves de característica bajo demanda** para acceder a la información necesaria para solicitar una clave de característica bajo demanda y otra información sin agentes (consulte Ver claves de Características bajo demanda).

Después de finalizar

Además de mostrar un resumen e información detallada sobre un chasis, también puede realizar las siguientes acciones:

- Ver un chasis en una vista gráfica de bastidores o de chasis haciendo clic en **Acciones → Vistas → Mostrar en vista de bastidores** o **Acciones → Vistas → Mostrar en vista de chasis**.
- Inicie la interfaz web del CMM al hacer clic en el vínculo **Dirección IP** (consulte Inicio de la interfaz web del CMM para un chasis).
- Modificar la información (como el contacto con el soporte, la ubicación y la descripción) pulsando **Editar propiedades** (consulte Modificación de las propiedades del sistema de un chasis).
- Modifique los valores IP de gestión de todo el chasis, incluidos los nodos de cálculo y los conmutadores Flex, al hacer clic en **Todas las acciones → Inventario → Editar direcciones IP de gestión** (consulte Modificación de los valores IP de gestión de un chasis).
- Exporte la información detallada acerca del chasis a un archivo CSV al hacer clic en **Acciones → Inventario → Exportar inventario**.

  Notas:

  – Para obtener más información sobre datos de inventario en el archivo CSV, consulte GET /chassis/*<UUID_list>* en la documentación en línea de XClarity Administrator.

  – Al importar un archivo CSV en Microsoft Excel, Excel trata los valores de texto que contienen solo números como valores numéricos (por ejemplo, para UUID). Formatee cada celda como texto para corregir este error.
- Anular la gestión de un chasis (consulte Anulación de la gestión de un chasis).
- Habilite o deshabilite los cambios de la regla de firewall en un chasis que limita las solicitudes entrantes a las procedentes de XClarity Administrator al seleccionar el chasis y al hacer clic en **Acciones → Seguridad → Habilitar encapsulación** o **Acciones → Seguridad → Deshabilitar encapsulación**.

  Los valores globales de la encapsulación están deshabilitados de forma predeterminada. Cuando está deshabilitado, el modo de encapsulación del dispositivo se establece como “normal” y las reglas de firewall no se cambian como parte del proceso de gestión.

  Los valores globales de la encapsulación están deshabilitados de forma predeterminada. Cuando está deshabilitado, el modo de encapsulación del dispositivo se establece como “normal” y las reglas de firewall no se cambian como parte del proceso de gestión.

Cuando los valores globales de encapsulación están habilitados y el dispositivo admite la encapsulación, XClarity Administrator se comunica con el dispositivo durante el proceso de gestión para cambiar el modo de encapsulación del dispositivo a “encapsulationLite” y para cambiar las reglas de firewall en el dispositivo para limitar las solicitudes entrantes a únicamente las que se reciben de XClarity Administrator.

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 archivo lenovoMgrAlert.mib y la Recuperación de la gestión con un CMM después de un error en el servidor de gestión.

- Solucione los problemas que puedan surgir entre el certificado de seguridad de XClarity Administrator y el certificado de seguridad del CMM del chasis seleccionando un chasis y al hacer clic en **Acciones → Seguridad → Resolver certificados no fiables** (consulte Resolución de un certificado de servidor no fiable).

Creación de copia de seguridad y restauración de datos de configuración de CMM

Lenovo XClarity Administrator no incluye funciones integradas de copia de seguridad de datos para la configuración de CMM. En su lugar, utilice las funciones de copia de seguridad disponibles para los CMM gestionados.

Utilice la interfaz web de gestión o la interfaz de la línea de comandos (CLI) para crear una copia de seguridad y restaurar CMM.

- Creación de copia de seguridad de los datos de configuración del CMM
  - En la interfaz web de la gestión, haga clic en **Gestión del módulo de gestión → Configuración → Configuración de copia de seguridad**. Para obtener más información, consulte el apartado Guardar una configuración de CMM a través de la interfaz web en la documentación en línea de Flex Systems.
  - En la CLI, utilice el mandato `write`. Para obtener más información, consulte Comando CMM write en la documentación en línea de Flex System
- Restauración de datos de configuración del CMM
  - Desde la página de inicio de la interfaz web de gestión, haga clic en **Gestión del módulo de gestión → Configuración → Restaurar configuración desde archivo**. Para obtener más información, consulte el apartado Restauración de una configuración de CMM a través de la interfaz web en la documentación en línea de Flex Systems.
  - En la CLI, utilice el mandato `read`. Para obtener más información, consulte el apartado Comando CMM read en la documentación en línea de Flex System.

Nota: Consejo: encontrará información adicional acerca de cómo realizar una copia de seguridad de los componentes del chasis y restaurarlos en la Guía de prácticas recomendadas para la copia de seguridad y restauración de PureFlex y Flex System.

Inicio de la interfaz web del CMM para un chasis

Puede iniciar la interfaz web del CMM para un chasis específico desde Lenovo XClarity Administrator.

Procedimiento

Lleve a cabo los pasos siguientes para iniciar una interfaz web del CMM.

Nota: No se admite el inicio de esta interfaz web del CMM desde XClarity Administrator mediante el navegador web Safari.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Hardware → Chasis** para mostrar la página Chasis.

Puede ordenar las columnas de la tabla para que sea más fácil encontrar el chasis que desea gestionar. Además, puede introducir texto (como un nombre de chasis o una dirección IP) en el campo **Filtro** para filtrar mejor los chasis que se muestran.

Paso 2. Haga clic en el vínculo del chasis en la columna **Chasis**. Se muestra la página de resumen de estado de ese chasis.

Paso 3. Haga clic en **Todas las acciones → Iniciar → Interfaz web de gestión**. Se inicia la interfaz web del CMM.

Consejo: también puede hacer clic en la dirección IP para iniciar el CMM.

Paso 4. Inicie sesión en la interfaz web del CMM utilizando sus credenciales de usuario de XClarity Administrator.

Modificación de las propiedades del sistema de un chasis

Puede modificar las propiedades del sistema de un chasis específico.

Procedimiento

Lleve a cabo los pasos siguientes para modificar las propiedades del sistema.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Hardware → Chasis** para mostrar la página Chasis.

Paso 2. Seleccione el chasis que va a actualizar.

Paso 3. Haga clic en **Todas las acciones → Inventario → Editar propiedades**para mostrar el cuadro de diálogo Editar.

Paso 4. Cambie la siguiente información según sea necesario.
- Nombre del servidor
- Contacto de soporte
- Descripción

Nota: Las propiedades de ubicación, sala, bastidor y unidad de bastidor más baja se actualizan mediante XClarity Administrator cuando se agregan o quitan dispositivos de un bastidor en la interfaz web (consulte Gestión de bastidores).

Paso 5. Haga clic en **Guardar**.

Nota: Al cambiar estas propiedades, pueden transcurrir unos instantes antes de que los cambios aparezcan en la interfaz web de XClarity Administrator.

Modificación de los valores IP de gestión de un chasis

Puede modificar los valores IP de gestión de todo el chasis, incluidos los nodos de cálculo, los dispositivos de almacenamiento y los Conmutadores Flex.

Procedimiento

Lleve a cabo los pasos siguientes para modificar los valores IP de gestión.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Hardware → Chasis** para mostrar la página Chasis.

Paso 2. Seleccione el chasis.

Paso 3. Haga clic en **Todas las acciones → Inventario → Editar direcciones IP de gestión** para mostrar la página Valores IP del chasis y los componentes.

Paso 4. Cambie los siguientes valores globales según sea necesario.

- Elija entre habilitar o deshabilitar las direcciones IPv4.

  Si habilita las direcciones IPv4, especifique los siguientes valores. Los valores globales de IPv4 se aplican a un componente cuando se actualiza su dirección IPv4.
  - (Opcional) Elija obtener direcciones IP utilizando direcciones IP asignadas estáticamente.
  - Especifique la dirección de la máscara de subred y la puerta de enlace.
- Especifique los siguientes valores para direcciones IPv6. Los valores globales de IPv6 se aplican a un componente cuando se actualiza su dirección IPv6.
  - (Opcional) Elija obtener direcciones IP utilizando direcciones IP asignadas estáticamente.

    Si se utilizan direcciones IP estáticas, también puede elegir utilizar la configuración automática de direcciones IP sin estado y la configuración de dirección IP con estado.
  - Especifique la dirección de la longitud de prefijo y la puerta de enlace.
- Elija entre habilitar o deshabilitar los servidores DNS.

  Si habilita los servidores DNS:
  - Elija la preferencia de búsqueda de servidores DNS.
  - Introduzca las direcciones IP a utilizar para el orden de búsqueda de DNS.
  - Especifique el nombre del dominio.

Paso 5. Cambie los siguientes valores IP del CMM.

- Introduzca el nombre de host y la dirección IP del CMM.
- Haga clic en **Generación automática de direcciones IP** para crear direcciones IP para los nodos de cálculo, los dispositivos de almacenamiento y los Conmutadores Flex utilizando la dirección IP del CMM como punto de partida.

Paso 6. Introduzca el nombre de host y las direcciones IP de cada nodo de cálculo del chasis.

Paso 7. Introduzca el nombre de host y las direcciones IP de cada dispositivo de almacenamiento del chasis.

Paso 8. Introduzca las direcciones IP de cada Conmutador Flex del chasis.

Paso 9. Haga clic en **Guardar**. Se muestra un cuadro de diálogo con un resumen de los valores de red.

Paso 10. Haga clic en **Aplicar**.

Todos los componentes existentes en el chasis se actualizan a los valores globales especificados. Cuando la actualización se ha completado, el cuadro de diálogo muestra los valores que se han cambiado.

Nota: Al cambiar esta información, pueden transcurrir unos instantes antes de que la información aparezca en la interfaz de Lenovo XClarity Administrator.

Paso 11. Pulse **Cerrar**.

Configurar conmutación por error del CMM

Cuando instala un segundo CMM en un chasis, el segundo CMM se configura automáticamente como CMM en espera de manera predeterminada. Si el CMM principal produce un error, la dirección IP del CMM en espera cambia a la misma dirección IP que se utilizó para el CMM principal, mientras que el CMM en espera asume la gestión del chasis. No obstante, puede realizar otras configuraciones de conmutación por error avanzada desde la interfaz web del controlador de gestión del chasis.

Acerca de esta tarea

Por ejemplo, puede optar por:

- Deshabilite la interfaz de red del CMM en espera para evitar una conmutación por error.
- Habilite la interfaz de red para el CMM en espera y permita el intercambio de direcciones IP entre los dos CMM durante la conmutación por error.
- Habilite la interfaz de red para el CMM en espera y evite el intercambio de direcciones IP entre los dos CMM durante la conmutación por error.

Para obtener más información acerca de las funciones de conmutación por error avanzada del CMM, consulte el Comando advfailover en la documentación en línea de CMM.

Procedimiento

Para permitir que las direcciones IP de los CMM principal y en espera sean intercambiables, lleve a cabo los pasos siguientes.

Paso 1. En la interfaz web del controlador de gestión del chasis, haga clic en **Gestión del módulo de gestión → Red → Ethernet** para mostrar la página Configuración de Ethernet.

Paso 2. Seleccione **IPv4** o **IPv6** para su sistema.

Paso 3. En **Configurar dirección IP**, seleccione la opción para utilizar una dirección IP estática. Repita los pasos para el otro protocolo.

Paso 4. Haga clic en **Gestión del módulo de gestión → Propiedades → Conmutación por error avanzada** y, a continuación, habilite la opción de conmutación por error avanzada.

Paso 5. Seleccione **Cambiar dirección IP de módulo de gestión**.

Paso 6. Desarrolle los escenarios de prueba para verificar que la conmutación por error funciona correctamente y que Lenovo XClarity Administrator puede conectarse al CMM principal y de copia de seguridad.

Reinicio de un CMM

Puede reiniciar un Chassis Management Module (CMM) desde Lenovo XClarity Administrator.

Procedimiento

Lleve a cabo el procedimiento siguiente para reiniciar un chasis.

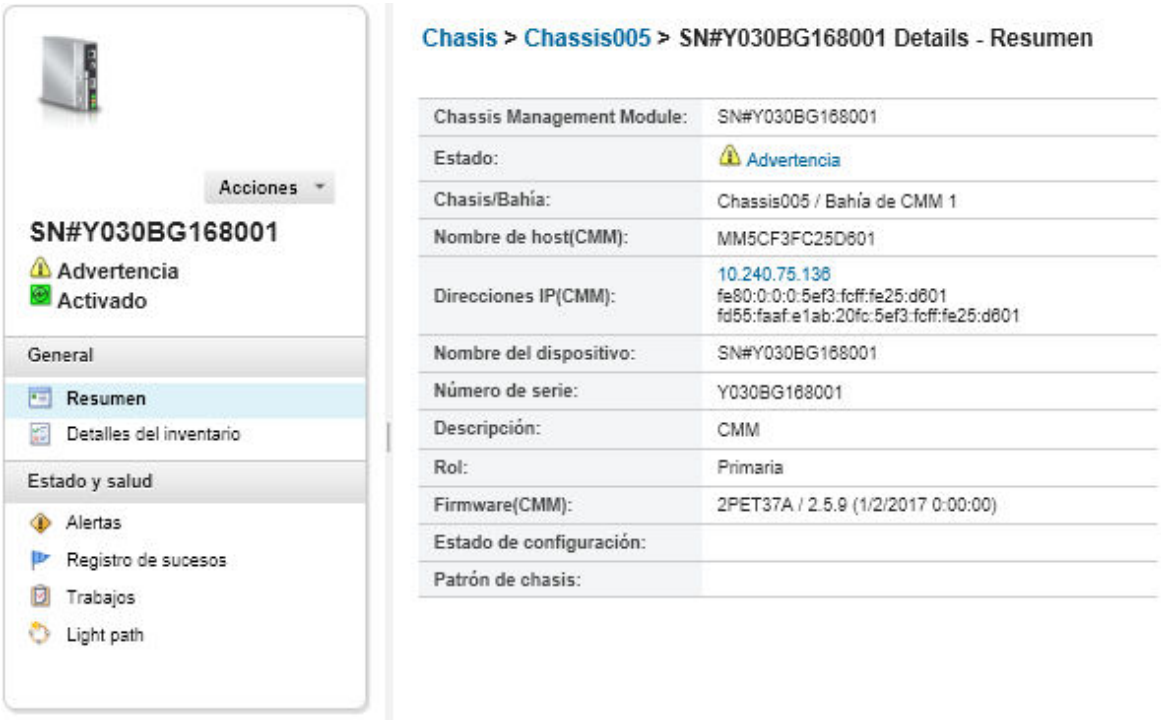
Nota: Cuando el CMM se reinicie, todas las conexiones de red existentes con el CMM se perderán temporalmente.

Paso 1. En el menú de XClarity Administrator haga clic en **Hardware → Chasis**. Se muestra la página Chasis con una vista de tabla de todos los chasis gestionados.

Paso 2. Haga clic en el nombre del chasis en la columna **Chasis** para mostrar la vista gráfica del chasis.

Paso 3. Haga clic en en el gráfico del CMM para mostrar el CMM en la página Resumen del CMM.

Consejo: también puede hacer clic en **Vista de tabla** y, continuación, hacer clic en el nombre del CMM dentro de la columna **Nombre** para mostrar la página Resumen del CMM.



Paso 4. Haga clic en **Acciones → Acciones de alimentación → Reiniciar**.

Paso 5. Haga clic en **Reiniciar de inmediato**.

Esta operación puede tardar unos minutos en completarse y es posible que deba actualizar la página para ver los resultados.

Reubicación virtual de un CMM

Puede simular la eliminación y la reinserción de un Chassis Management Module (CMM) dentro de un chasis.

Acerca de esta tarea

Durante la reubicación virtual, se pierden todas las conexiones de red al CMM existentes y el estado de alimentación de los cambios del CMM.

Atención: Antes de realizar una reubicación virtual, asegúrese de haber guardado todos los datos del usuario en el CMM.

Procedimiento

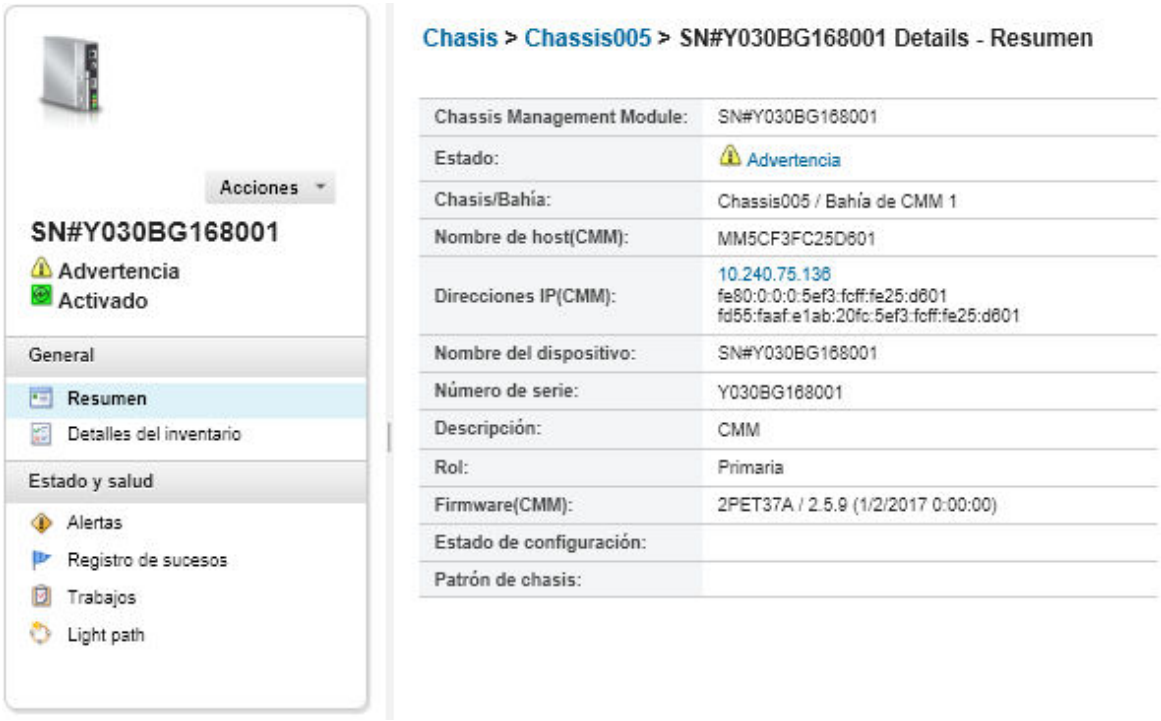
Lleve a cabo los pasos siguientes para reubicar virtualmente un CMM.

Paso 1. En el menú de Lenovo XClarity Administrator haga clic en **Hardware → Chasis**. Se muestra la página Chasis con una vista de tabla de todos los chasis gestionados.

Paso 2. Haga clic en el nombre del chasis en la columna **Chasis** para mostrar la vista gráfica del chasis.

Paso 3. Haga clic en en el gráfico del CMM para mostrar el CMM en la página Resumen del CMM.

Consejo: también puede hacer clic en **Vista de tabla** y, continuación, hacer clic en el nombre del CMM dentro de la columna **Nombre** para mostrar la página Resumen del CMM.



Paso 4. Haga clic en **Acciones → Servicio → Reubicación virtual**.

Paso 5. Haga clic en **Reubicación virtual**.

Resolución de credenciales almacenadas caducadas o no válidas para un chasis

Cuando una credencial almacenada caduca o deja de funcionar en un dispositivo, el estado de ese dispositivo pasa a ser “Fuera de línea.”

Procedimiento

Para resolver una credencial almacenada caducada o no válida para un chasis.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Hardware → Chasis**. Se muestra la página Chasis con una vista de tabla de todos los chasis gestionados.

Paso 2. Haga clic en el encabezado de la columna **Alimentación** para agrupar todos los chasis fuera de línea en la parte superior de la tabla.

Puede ordenar las columnas de la tabla para que sea más fácil encontrar el chasis que desea gestionar. Además, puede introducir texto (como un nombre de chasis o una dirección IP) en el campo **Filtro** para filtrar mejor los chasis que se muestran.

Paso 3. Seleccione el chasis que va a resolver.

Paso 4. Haga clic en **Todas las acciones → Seguridad → Edtiar las credenciales almacenadas**.

Paso 5. Cambie la contraseña de la credencial almacenada o seleccione otra credencial almacenada a utilizar en el dispositivo gestionado.

Nota: Si gestionó más de un dispositivo utilizando las mismas credenciales almacenadas y cambiar la contraseña de las credenciales almacenadas, la cambiar la contraseña afecta a todos los dispositivos que estén utilizando las credenciales almacenadas.

Recuperación de la gestión con un CMM tras un error de servidor de gestión

Si el chasis se está gestionando mediante Lenovo XClarity Administrator y XClarity Administrator produce un error, puede restaurar las funciones de gestión y las cuentas de usuarios locales para un CMM hasta que el nodo de gestión se restaure o se sustituya.

Procedimiento

Lleve a cabo uno de los procedimientos siguientes para restaurar la gestión en un CMM.

- Si la instancia de sustitución de XClarity Administrator utiliza la misma dirección IP que la instancia de XClarity Administrator que ha producido el error, vuelva a gestionar el dispositivo utilizando la cuenta y la contraseña del RECOVERY_ID y la opción **Forzar gestión** (consulte el Gestión del chasis).
- Restablezca el CMM a los valores predeterminados de fábrica presionando el botón de agujerito del CMM con un clip durante al menos 10 segundos. Para obtener más información acerca de cómo restablecer el CMM, incluidos algunos avisos importantes, consulte Restablecimiento del CMM en la documentación en línea de Flex System.
- Restablezca la configuración del CMM llevando a cabo los pasos siguientes:
  1. Abra una interfaz de la línea de comandos de gestión del chasis mediante una sesión SSH e inicie sesión con la cuenta `RECOVERY_ID`.

     Nota: La palabra de la cuenta `RECOVERY_ID` se estableció al seleccionar el chasis para gestión en la página Dominio de gestión. Para obtener más información acerca de la gestión de cuentas central, consulte el Gestión del chasis.

     Si es la primera vez que utiliza la cuenta `RECOVERY_ID` para iniciar sesión en CMM, debe cambiar la contraseña.
  2. Cuando se le pida, escriba la nueva contraseña para la cuenta `RECOVERY_ID`.
  3. Lleve a cabo uno de los siguientes pasos para restaurar la configuración del CMM:
     - Si está ejecutando una versión de firmware del CMM de junio de 2015 o posterior, ejecute el siguiente comando:

`read -f unmanage -T mm[p]`
Para obtener más información, consulte el Comando read en la documentación en línea de CMM

– Si está ejecutando una versión de firmware del CMM anterior a junio de 2015, ejecute los siguientes comandos en el orden mostrado:

a. `env -T mm[p]`
b. `sslcfg -client disabled -tc1 remove`
c. `accseccfg -am local`
d. `ldapcfg -i1 -p1 -rd "" -usa "" -gsa "" -lpa ""`
e. `ntp -en disabled -i 0.0.0.0 -v3en disabled`
f. `cimsub -clear all`
g. `fsmcm -off`

El comando `fsmcm` deshabilita la gestión de cuentas de usuarios de XClarity Administrator y le permite utilizar cuentas de usuarios locales de CMM para autenticarse en CMM y en cualquier procesador de gestión que esté instalado en el chasis.

Una vez que ejecute el mandato `fsmcm -off`, la cuenta `RECOVERY_ID` se quita del registro de usuarios del CMM. Al ejecutar el mandato `fsmcm -off`, finaliza la sesión CLI del CMM. Ahora puede autenticarse en CMM y otros componentes del chasis utilizando las credenciales locales del CMM, así como utilizar las credenciales locales del CMM para acceder a la interfaz web del CMM o a la CLI del chasis hasta que la gestión de usuarios se restaure mediante XClarity Administrator.

Para obtener más información, consulte el Comando fsmcm en la documentación en línea de CMM

Una vez que se haya restaurado o sustituido XClarity Administrator, puede volver a gestionar el chasis (consulte el Gestión del chasis). Se conserva toda la información acerca del chasis (como los valores de red).

Anulación de la gestión de un chasis

Puede quitar un chasis de la gestión mediante Lenovo XClarity Administrator. Este proceso se denomina *anular la gestión* (no gestionar). Una vez que se anula la gestión del chasis, puede iniciar sesión en el CMM para el chasis utilizando las cuentas de usuarios locales del CMM.

Antes de empezar

Puede habilitar XClarity Administrator para que se anule automáticamente la gestión de los dispositivos que están fuera de línea durante un período de tiempo específico. Esto está deshabilitado de forma predeterminada. Para habilitar la anulación automática de gestión de dispositivos fuera de línea, haga clic en **Hardware → Detectar y gestionar dispositivos nuevos** en el menú de XClarity Administrator y, a continuación, haga clic en **Editar**, ubicado junto a la opción **No gestionar los dispositivos fuera de línea está Deshabilitado**. A continuación, seleccione **Habilitar dispositivos no gestionados fuera de línea** y establezca el intervalo de tiempo. De manera predeterminada, se anula la gestión de los dispositivos después de estar fuera de línea durante 24 horas.

Antes de anular la gestión de un chasis, asegúrese de que no hay trabajos activos en ejecución en ninguno de los dispositivos que están instalados en el chasis.

Si la opción Llamar a casa está habilitada en XClarity Administrator, Llamar a casa se deshabilita en todos los chasis y servidores gestionados para evitar que se produzca una duplicación de los registros de problemas. Si tiene intención dejar de utilizar XClarity Administrator para gestionar sus dispositivos, puede

volver a habilitar la función Llamar a casa en todos los dispositivos gestionados desde XClarity Administrator, en lugar de volver a habilitar Llamar a casa posteriormente para cada dispositivo individual (consulte Nueva habilitación de Llamar a casa en todos los dispositivos gestionados en la documentación en línea de XClarity Administrator).

Acerca de esta tarea

Cuando se anula la gestión de un chasis, XClarity Administrator realiza las siguientes acciones:

- Borra la configuración que se utiliza para la gestión de usuarios centralizada.
- Elimina el certificado de seguridad del CMM desde el almacén de confianza de XClarity Administrator.
- Si la Encapsulación está habilitada en el dispositivo, configura las reglas de firewall de los dispositivos con los valores que tenía el dispositivo antes de que se gestionara.
- Elimina el acceso al servidor NTP desde el CMM.
- Elimina las suscripciones CIM al CMM desde la configuración de XClarity Administrator, de forma que XClarity Administrator ya no recibe los sucesos de ese chasis.

Cuando se anula la gestión de un chasis, XClarity Administrator conserva determinada información sobre el chasis. Esta información se vuelve a aplicar cuando se gestiona de nuevo el mismo chasis.

Cuando se anula la gestión de un chasis, los sucesos que se enviaron desde los componentes del chasis se descartan. Puede conservar dichos sucesos reenviándolos a un repositorio externo, como Syslog (consulte Reenvío de sucesos).

Consejo: todos los dispositivos de demostración que se añaden opcionalmente durante la configuración inicial son nodos en un chasis. Para anular la gestión de los dispositivos de demostración, anule la gestión del chasis utilizando la opción **Forzar anulación de gestión incluso si no se puede acceder al dispositivo**.

Procedimiento

Para anular la gestión de un chasis, lleve a cabo los pasos siguientes.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Hardware → Chasis** para mostrar la página Chasis.

Paso 2. Seleccione uno o más chasis de las listas de chasis gestionados.

Paso 3. Haga clic en **No gestionar chasis**. Se muestra el cuadro de diálogo No gestionar.

Paso 4. **Opcional:** seleccione **Forzar anulación de gestión aunque el dispositivo no esté accesible**.

Importante: Asegúrese de seleccionar esta opción si está anulando la gestión de un hardware de demostración.

Paso 5. Haga clic en **No gestionar**.El cuadro de diálogo No gestionar muestra el progreso de cada paso en el proceso de anulación de la gestión.

Paso 6. Cuando el proceso de anulación de la gestión esté completo, haga clic en **Aceptar**.

Después de finalizar

Una vez que se ha completado el proceso de anulación de la gestión, puede iniciar sesión en el CMM utilizando las cuentas de usuarios locales del CMM. Si no recuerda los nombres de usuario o las contraseñas de alguna de las cuentas de usuarios del CMM, restablezca los valores predeterminados de fábrica para iniciar sesión en el CMM. Para obtener información sobre el restablecimiento de los valores predeterminados de fábrica del CMM, consulte Restablecimiento del CMM en la documentación en línea de Flex System en la documentación de producto del CMM.

Recuperación de un chasis en el que no se ha anulado la gestión correctamente

Si la gestión de un chasis no se ha anulado correctamente, debe recuperar el chasis antes de poder gestionarlo de nuevo.

Procedimiento

Lleve a cabo uno de los procedimientos siguientes para restaurar la gestión en un CMM.

- Si la instancia de sustitución de XClarity Administrator utiliza la misma dirección IP que la instancia de XClarity Administrator que ha producido el error, vuelva a gestionar el dispositivo utilizando la cuenta y la contraseña del RECOVERY_ID y la opción **Forzar gestión** (consulte el Gestión del chasis).
- Restablezca el CMM a los valores predeterminados de fábrica presionando el botón de agujerito del CMM con un clip durante al menos 10 segundos. Para obtener más información acerca de cómo restablecer el CMM, incluidos algunos avisos importantes, consulte Restablecimiento del CMM en la documentación en línea de Flex System.
- Restablezca la configuración del CMM llevando a cabo los pasos siguientes:
  1. Abra una interfaz de la línea de comandos de gestión del chasis mediante una sesión SSH e inicie sesión con la cuenta `RECOVERY_ID`.

     Nota: La palabra de la cuenta `RECOVERY_ID` se estableció al seleccionar el chasis para gestión en la página Dominio de gestión. Para obtener más información acerca de la gestión de cuentas central, consulte el Gestión del chasis.

     Si es la primera vez que utiliza la cuenta `RECOVERY_ID` para iniciar sesión en CMM, debe cambiar la contraseña.
  2. Cuando se le pida, escriba la nueva contraseña para la cuenta `RECOVERY_ID`.
  3. Lleve a cabo uno de los siguientes pasos para restaurar la configuración del CMM:
     - Si está ejecutando una versión de firmware del CMM de junio de 2015 o posterior, ejecute el siguiente comando:
       ```
       read -f unmanage -T mm[p]
       ```
       Para obtener más información, consulte el Comando read en la documentación en línea de CMM
     - Si está ejecutando una versión de firmware del CMM anterior a junio de 2015, ejecute los siguientes comandos en el orden mostrado:
       a. `env -T mm[p]`
       b. `sslcfg -client disabled -tc1 remove`
       c. `accseccfg -am local`
       d. `ldapcfg -i1 -p1 -rd "" -usa "" -gsa "" -lpa ""`
       e. `ntp -en disabled -i 0.0.0.0 -v3en disabled`
       f. `cimsub -clear all`
       g. `fsmcm -off`

          El comando `fsmcm` deshabilita la gestión de cuentas de usuarios de XClarity Administrator y le permite utilizar cuentas de usuarios locales de CMM para autenticarse en CMM y en cualquier procesador de gestión que esté instalado en el chasis.

          Una vez que ejecute el mandato `fsmcm -off`, la cuenta `RECOVERY_ID` se quita del registro de usuarios del CMM. Al ejecutar el mandato `fsmcm -off`, finaliza la sesión CLI del CMM. Ahora puede autenticarse en CMM y otros componentes del chasis utilizando las credenciales locales del CMM, así como utilizar las credenciales locales del CMM para acceder a la interfaz web del

CMM o a la CLI del chasis hasta que la gestión de usuarios se restaure mediante XClarity Administrator.

Para obtener más información, consulte el Comando fsmcm en la documentación en línea de CMM

Una vez que se haya restaurado o sustituido XClarity Administrator, puede volver a gestionar el chasis (consulte el Gestión del chasis). Se conserva toda la información acerca del chasis (como los valores de red).

Capítulo 8. Gestión de servidores

Lenovo XClarity Administrator puede gestionar varios tipos de sistemas, lo que incluye los servidores ThinkAgile, ThinkSystem, Converged, Flex System, NeXtScale, System x® y ThinkServer®.

Más información: XClarity Administrator: detección

Antes de empezar

Nota: Los nodos de cálculo Flex se detectan y gestionan automáticamente cuando gestiona el chasis que los contiene. No puede detectar ni gestionar nodos de cálculo Flex de forma independiente del chasis.

Antes de gestionar servidores, asegúrese de que se cumplan las siguientes condiciones:

- Revise las consideraciones de gestión antes de gestionar un dispositivo. Para obtener información, consulte Consideraciones de gestión en la XClarity Administrator documentación en línea.
- Algunos puertos deben estar disponibles para comunicarse con los dispositivos. Asegúrese de que todos los puertos requeridos estén disponibles antes de intentar gestionar servidores. Para obtener más información sobre los puertos, consulte Disponibilidad de puertos en la documentación en línea de XClarity Administrator.
- Asegúrese de que el firmware mínimo necesario esté instalado en cada servidor 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 el CIM sobre HTTPS esté habilitado en el dispositivo.
  1. Inicie sesión en la interfaz web de gestión del servidor, utilizando la cuenta de usuario `RECOVERY_ID`.
  2. Haga clic en **Gestión de IMM → Seguridad**.
  3. Haga clic en la pestaña **CIM sobre HTTPS** y asegúrese de que **Habilitar CIM sobre HTTPS** está activado.
- Para servidores ThinkSystem SR635 y SR655:
  - Asegúrese de que se haya instalado un sistema operativo y de que el servidor se haya arrancado en el SO, en el medio de arranque montado o efishell al menos una vez, de modo que el XClarity Administrator pueda recopilar el inventario de dichos servidores.
  - Asegúrese de que IPMI sobre LAN esté habilitado. IPMI sobre LAN está deshabilitado de forma predeterminada en estos servidores y debe habilitarse manualmente antes de poder gestionar los servidores. Para habilitar IPMI sobre LAN utilizando TSM, haga clic en **Valores → Configuración IPMI**. Es posible que tenga que reiniciar el servidor para activar el cambio.
- Si el certificado de servidor del dispositivo se firma por una entidad de certificación externa, asegúrese de que el certificado de la entidad de certificación y todos los certificados intermedios se importen al almacén de confianza de XClarity Administrator (consulte Despliegue de certificados de servidor personalizados en dispositivos gestionados).
- Para descubrir un servidor que está en una subred *distinta* de XClarity Administrator, asegúrese de que se cumpla una de las siguientes condiciones:
  - 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.

  - Si SLP está deshabilitado en el punto final o en la red, puede utilizar el método de detección de DNS en su lugar al agregar manualmente un registro de servicio (registro SRV) al servidor de nombres de dominio (DNS), como, por ejemplo, para XClarity Administrator
    `_lxca._tcp.labs.lenovo.com  service = 0 0 443 fvt-xhmc3.labs.lenovo.com.`

    A continuación, habilite el descubrimiento de DNS en la consola de gestión de la placa base desde la interfaz web de gestión, al hacer clic en **Gestión de IMM → Protocolo de red**, en la pestaña **DNS** y, después, en **Usar DNS para descubrir Lenovo XClarity Administrator**.

    Notas:

    - El controlador de gestión se debe ejecutar en el nivel de firmware con fecha de mayo de 2017 o posterior para admitir descubrimiento automático utilizando DNS.
    - Si hay múltiples instancias de XClarity Administrator en su entorno, el servidor se descubrirá solo por la instancia que es la primera a responder a la solicitud de descubrimiento. El servidor no se descubrirá en todas las instancias.
- Para detectar y gestionar servidores ThinkServer, asegúrese de que se cumplan los siguientes requisitos. Para obtener más información, consulte No se puede detectar un dispositivo y No puede gestionar un dispositivo en la documentación en línea de XClarity Administrator.
  - Se debe configurar el nombre de host del servidor mediante un nombre de host o dirección IP válida si desea que XClarity Administrator detecte automáticamente los servidores.
  - La red de configuración debe permitir el tráfico SLP entre XClarity Administrator y el servidor.
  - Se requiere SLP de difusión única.
  - Si desea que XClarity Administrator descubra automáticamente los servidores ThinkServer, se requiere SLP de multidifusión. Además, se debe habilitar SLP en ThinkServer System Manager (TSM).
  - Si los servidores ThinkServer están en una red distinta de XClarity Administrator, asegúrese de que la red se configure para permitir UDP entrante mediante el puerto 162 para que XClarity Administrator pueda recibir sucesos para esos dispositivos.
- Para ThinkAgile, ThinkSystem, Converged, Flex System. Para servidores NeXtScale y System x, si quita, sustituye o configura cualquier adaptador en el servidor, debe reiniciar el servidor al menos una vez para actualizar la nueva información del adaptador en el controlador de gestión de la placa base y los informes de XClarity Administrator (Encendido y apagado de un servidor).
- Cuando se realizan las acciones de gestión en un servidor, asegúrese de que el servidor está apagado o encendido en la configuración de BIOS/UEFI o ejecutando un sistema operativo. (Puede arrancar la configuración de BIOS/UEFI desde la página Servidores en XClarity Administrator y pulsando **Todas las acciones → Acciones de alimentación → Reiniciar a la configuración de BIOS/UEFI**). Si el servidor está encendido sin un sistema operativo, el controlador de gestión restablece continuamente el servidor en un intento por encontrar un sistema operativo.
- Asegúrese de que todos los valores `UEFI_Ethernet_*` y `UEFI_Slot_*` estén habilitados en los valores del servidor de la UEFI. Para verificar los valores, reinicie el servidor y cuando se visualice el indicador `<F1> Setup`, presione `F1` para iniciar la utilidad de configuración. Navegue hasta **System Settings → Devices and I/O Ports → Enable / Disable Adapter Option ROM Support** y, a continuación, ubique la sección **Enable / Disable UEFI Option ROM(s)** para verificar que los valores estén habilitados.

  Nota: Si se admite, también puede utilizar la función de consola remota en la interfaz de gestión de la placa base para revisar y modificar los valores de forma remota.
- Los servidores System x3950 X6 se deben gestionar como dos alojamientos 4U, cada uno con su propio controlador de gestión de la placa base.

Acerca de esta tarea

XClarity Administrator puede detectar automáticamente bastidores y servidores de torre en el entorno, sondeando los dispositivos gestionables que se encuentran en la misma subred IP, como XClarity Administrator. Para detectar los bastidores y servidores de torre que están en otras subredes, especifique una dirección IP o un rango de direcciones IP, o importe la información de una hoja de cálculo.

Importante: Para servidores System x3850 y x3950 X6, es preciso gestionar cada servidor en el entorno de bastidor escalable.

Una vez que XClarity Administrator gestiona los servidores, Lenovo XClarity Administrator sondea periódicamente todos los servidores gestionados para recopilar información, como el inventario, los datos de producto fundamentales y el estado. Puede consultar y supervisar cada servidor gestionado y realizar acciones de gestión (como configurar los valores del sistema, desplegar imágenes del sistema operativo y encenderlo y apagarlo).

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:

  – 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.

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

  – 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.

  – 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).

  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.

Un dispositivo solo puede estar gestionado 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. Si se produce un error durante el proceso de anulación de la gestión, puede seleccionar la opción **Forzar gestión** durante la gestión del nuevo XClarity Administrator.

Nota: Cuando explora la red en busca de dispositivos gestionables, XClarity Administrator no reconoce si un dispositivo ya está gestionado por otro gestionador hasta después de intentar gestionar el dispositivo.

Nota: Cuando explora la red en busca de dispositivos gestionables, XClarity Administrator no sabe si un dispositivo de ThinkServer ya está gestionado; por lo tanto, los dispositivos gestionados de ThinkServer pueden aparecer en la lista de dispositivos gestionables.

Durante el proceso de gestión, XClarity Administrator realiza las siguientes acciones:

- Inicia sesión en el servidor utilizando las credenciales proporcionadas.
- Recopila el inventario de cada servidor.

  Nota: Algunos datos del inventario se recopilan una vez completado el proceso de gestión. No puede realizar ciertas tareas en un servidor gestionado (como el despliegue de un patrón de servidor), hasta que se hayan recopilado todos los datos de inventario para dicho servidor y el servidor ya no se encuentre en el estado Pendiente.
- Configura los valores del servidor NTP de forma que todos los dispositivos gestionados utilicen la misma configuración del servidor NTP especificado en XClarity Administrator.
- (Únicamente servidores System x y NeXtScale) Asigna la última política de cumplimiento de firmware editada para el servidor.
- (Únicamente para servidores Lenovo System x y NeXtScale) Opcionalmente configura las reglas de firewall de los dispositivos para que solo se acepten las solicitudes entrantes de XClarity Administrator.
- (Únicamente servidores System x y NeXtScale) Intercambia certificados de seguridad con el controlador de gestión, copiando el certificado de servidor CIM y el certificado de cliente LDAP del controlador de gestión en el almacén de confianza de XClarity Administrator y enviando el certificado de seguridad de la CA de XClarity Administrator y los certificados de confianza de LDAP al controlador de gestión. El controlador de gestión carga los certificados en el almacén de confianza del controlador de gestión, de forma que el controlador de gestión pueda confiar en las conexiones a los servidores LDAP y CIM en XClarity Administrator.

  Nota: Si el certificado de servidor CIM o el certificado de cliente LDAP no existen todavía, se crean durante el proceso de gestión.
- Configura la autenticación gestionada, si corresponde. Para obtener más información acerca de autenticación gestionada, consulte Gestión del servidor de autenticación.
- Crea la cuenta de usuario de recuperación (`RECOVERY_ID`), cuando corresponde. Para obtener más información acerca de la cuenta `RECOVERY_ID`, consulte Gestión del servidor de autenticación.

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 que se haya gestionado el servidor (consulte Configuración de valores de criptografía en el servidor de gestión).

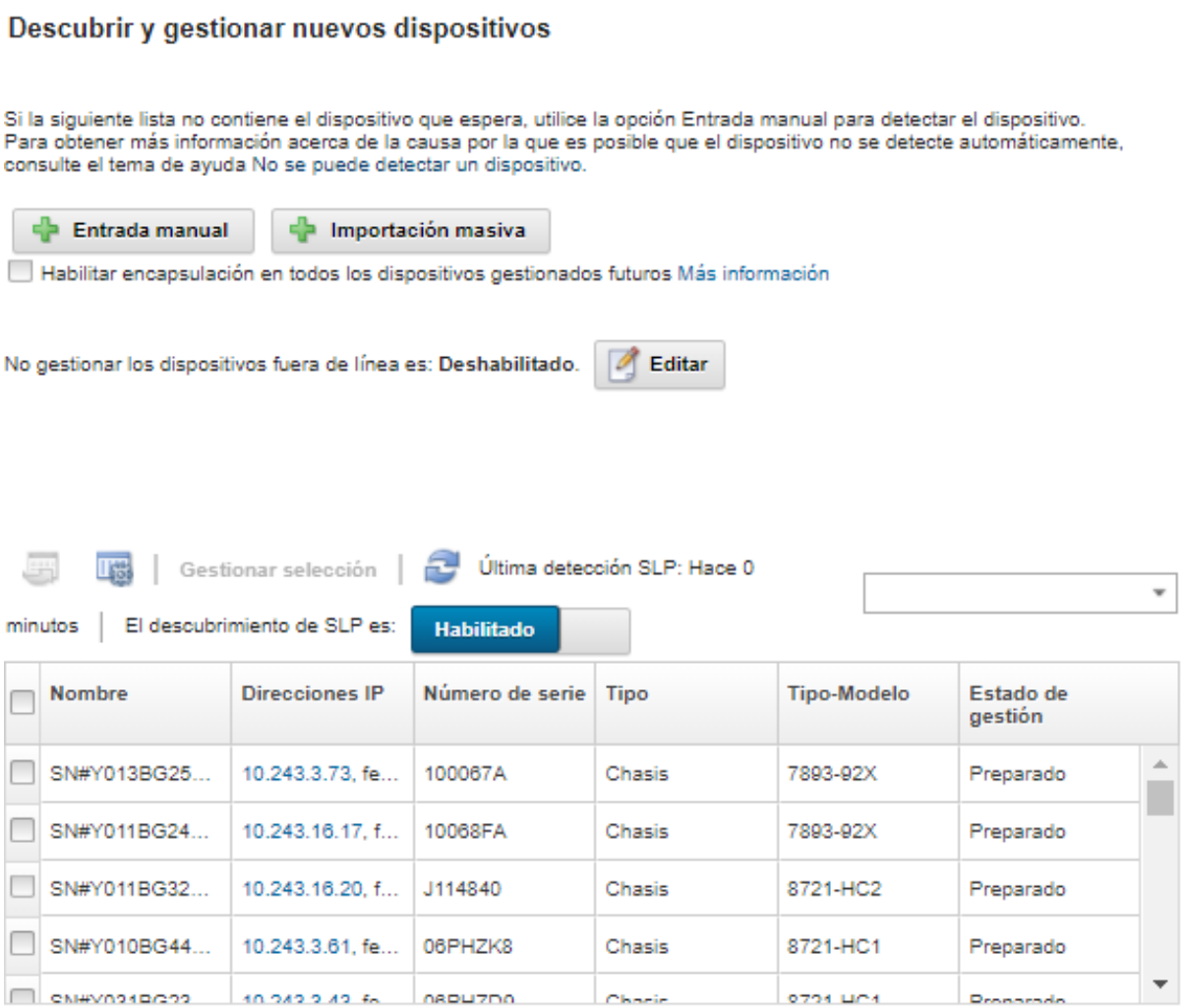
Importante: Si cambia la dirección IP de un servidor después de que el servidor está gestionado por XClarity Administrator, XClarity Administrator reconoce la nueva dirección IP y continúa gestionando el servidor. Sin embargo, XClarity Administrator no reconoce el cambio de dirección IP para algunos 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**.

Procedimiento

Para gestionar sus servidores de bastidor y de torre mediante XClarity Administrator, realice uno de los procedimientos siguientes.

- Detecte y gestione un gran número de servidores de torre y de bastidor y otros dispositivos utilizando un archivo de importación masiva (consulte Gestión de sistemas en la documentación en línea de XClarity Administrator).
- Detecte y gestione servidores de bastidor y de torre que estén en la misma subred IP que XClarity Administrator.

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 dispositivos nuevos.



   Puede ordenar las columnas de la tabla para que sea más fácil encontrar los servidores que desea gestionar. Además, puede introducir texto (como un nombre o una dirección IP) en el campo **Filtro** para filtrar mejor los servidores que se muestran. Puede cambiar las columnas que se muestran el orden predeterminado haciendo clic en el icono **Personalizar columnas** ( ).

2. Haga clic en el icono **Actualizar** ( ) para descubrir todos los dispositivos gestionables en el dominio XClarity Administrator. La detección puede durar varios minutos.
3. 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.

   La encapsulación se puede habilitar o deshabilitar en dispositivos específicos después de que se hayan gestionado.

Nota: 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.

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 archivo lenovoMgrAlert.mib y la Recuperación de la gestión con un CMM después de un error en el servidor de gestión.

4. Seleccione uno o más servidores que desee gestionar.
5. Haga clic en **Gestionar selección**. Se muestra el cuadro de diálogo Gestionar.
6. Seleccione utilizar autenticación gestionada o autenticación local de XClarity Administrator para este dispositivo. Se selecciona autenticación gestionada de forma predeterminada. Para utilizar autenticación local, elimine la selección de **Autenticación gestionada**.
7. Elija el tipo de credenciales a utilizar para autenticar en el dispositivo y especifique las credenciales adecuadas:
   - **Usar credenciales ingresadas manualmente**
     - Especifique el Id. de usuario y la contraseña para su autenticación en el servidor.
     - (Opcional) Si la contraseña en el dispositivo caducó, establezca una nueva contraseña para el nombre de usuario especificado.

     Nota: Para utilizar las credenciales introducidas manualmente, debe seleccionar la autenticación gestionada de XClarity Administrator.
   - **Usar credenciales almacenadas**

     Seleccione la credencial almacenada a utilizar para este dispositivo gestionado. Puede crear una nueva credencial almacenada al hacer clic en **Crear nuevo**.
   - **Utilice el sistema de gestión de identidades externo**.

     Seleccione el sistema de gestión de identidades que desea utilizar para este dispositivo gestionado. A continuación, rellene los campos restantes, incluidos la dirección IP o el nombre de host del servidor gestionado, el nombre de usuario y, opcionalmente, el ID de aplicación, el seguro 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.

     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.

   Se recomienda usar una cuenta de supervisor o administrador para gestionar el dispositivo. Si se utiliza una cuenta con autoridad de nivel inferior, la gestión puede fallar, o la gestión puede finalizar correctamente, pero otras operaciones de XClarity Administrator en el dispositivo pueden fallar (especialmente si el dispositivo se gestiona sin autenticación gestionada).

   Para obtener más información sobre credenciales normales y almacenadas, consulte Gestión de cuentas de usuario, Gestión de credenciales almacenadas.
8. Si se selecciona autenticación gestionada, especifique la contraseña de recuperación.

   Cuando se especifica una contraseña, la cuenta de recuperación (`RECOVERY_ID`) se crea en el servidor y se deshabilitan todas las cuentas de usuario local. Si hay un problema con XClarity Administrator y

deja de funcionar por alguna razón, *tampoco podrá* iniciar sesión en el controlador de gestión utilizando las cuentas de usuarios normales. Sin embargo, puede iniciar sesión utilizando la cuenta de recuperación.

Notas:

- La contraseña de recuperación es opcional si elige utilizar autenticación gestionada, pero no se permite si elige utilizar autenticación local.
- Puede elegir utilizar una cuenta de recuperación local o credenciales de recuperación almacenadas. En cualquier caso, el nombre de usuario siempre es `RECOVERY_ID`.
- 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.

Para obtener más información sobre el ID de recuperación, consulte Gestión del servidor de autenticación.

9. Haga clic en **Cambiar** para cambiar los grupos de roles que se pueden asignar a los dispositivos.

   Notas:

   - Puede seleccionar desde una lista de grupos de roles que están asignados al usuario actual.
   - Si no cambia los grupos de roles, se utilizan los grupos de roles predeterminados. Para obtener más información acerca de los grupos de roles predeterminados, consulte Cambiar los permisos predeterminados.

10. Haga clic en **Gestionar**.

    Se visualiza un cuadro de diálogo que muestra el progreso de este proceso de gestión. Para asegurarse de que el proceso se completa satisfactoriamente, supervise el progreso.

11. Cuando el proceso esté completo, haga clic en **Aceptar**.

    El dispositivo se gestiona ahora mediante XClarity Administrator, que automáticamente sondea los dispositivos gestionados de forma periódica para recopilar información actualizada, como el inventario.

    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.

- Detecte y gestione servidores de bastidor y de torre que no estén en la misma subred IP que XClarity Administrator especificando las direcciones IP manualmente.

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.

   La encapsulación se puede habilitar o deshabilitar en dispositivos específicos después de que se hayan gestionado.

   Nota: 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.

   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 archivo lenovoMgrAlert.mib y la Recuperación de la gestión con un CMM después de un error en el servidor de gestión.
3. Seleccione **Entrada manual**.
4. Especifique las direcciones de red de los servidores que desea gestionar:
   - Haga clic en **Sistema único** y especifique una sola dirección IP, nombre de dominio o nombre de dominio totalmente cualificado (FQDN).

     Nota: Para especificar un FQDN, asegúrese de que se haya incluido un nombre de dominio válido en la página de Acceso de red (consulte Configuración del acceso de red).
   - Haga clic en **Varios sistemas** e introduzca un rango de direcciones IP. Para añadir otro rango, haga clic en el icono **Añadir** (). Para quitar un rango haga clic en el icono **Quitar** ().
5. Haga clic en **Aceptar**. Se muestra el cuadro de diálogo Gestionar
6. Seleccione utilizar autenticación gestionada o autenticación local de XClarity Administrator para este dispositivo. Se selecciona autenticación gestionada de forma predeterminada. Para utilizar autenticación local, elimine la selección de **Autenticación gestionada**.
7. Elija el tipo de credenciales a utilizar para autenticar en el dispositivo y especifique las credenciales adecuadas:
   - **Usar credenciales ingresadas manualmente**
     - Especifique el Id. de usuario y la contraseña para su autenticación en el servidor.
     - (Opcional) Si la contraseña en el dispositivo caducó, establezca una nueva contraseña para el nombre de usuario especificado.

     Nota: Para utilizar las credenciales introducidas manualmente, debe seleccionar la autenticación gestionada de XClarity Administrator.
   - **Usar credenciales almacenadas**

     Seleccione la credencial almacenada a utilizar para este dispositivo gestionado. Puede crear una nueva credencial almacenada al hacer clic en **Crear nuevo**.
   - **Utilice el sistema de gestión de identidades externo**.

     Seleccione el sistema de gestión de identidades que desea utilizar para este dispositivo gestionado. A continuación, rellene los campos restantes, incluidos la dirección IP o el nombre de host del servidor gestionado, el nombre de usuario y, opcionalmente, el ID de aplicación, el seguro 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.

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.

Se recomienda usar una cuenta de supervisor o administrador para gestionar el dispositivo. Si se utiliza una cuenta con autoridad de nivel inferior, la gestión puede fallar, o la gestión puede finalizar correctamente, pero otras operaciones de XClarity Administrator en el dispositivo pueden fallar (especialmente si el dispositivo se gestiona sin autenticación gestionada).

Para obtener más información sobre credenciales normales y almacenadas, consulte Gestión de cuentas de usuario, Gestión de credenciales almacenadas.

8. Si se selecciona autenticación gestionada, especifique la contraseña de recuperación.

   Cuando se especifica una contraseña, la cuenta de recuperación (`RECOVERY_ID`) se crea en el servidor y se deshabilitan todas las cuentas de usuario local. Si hay un problema con XClarity Administrator y deja de funcionar por alguna razón, *tampoco podrá* iniciar sesión en el controlador de gestión utilizando las cuentas de usuarios normales. Sin embargo, puede iniciar sesión utilizando la cuenta de recuperación.

   Notas:

   - La contraseña de recuperación es opcional si elige utilizar autenticación gestionada, pero no se permite si elige utilizar autenticación local.
   - Puede elegir utilizar una cuenta de recuperación local o credenciales de recuperación almacenadas. En cualquier caso, el nombre de usuario siempre es `RECOVERY_ID`.
   - 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.

   Para obtener más información sobre el ID de recuperación, consulte Gestión del servidor de autenticación.

9. Haga clic en **Cambiar** para cambiar los grupos de roles que se pueden asignar a los dispositivos.

   Notas:

   - Puede seleccionar desde una lista de grupos de roles que están asignados al usuario actual.
   - Si no cambia los grupos de roles, se utilizan los grupos de roles predeterminados. Para obtener más información acerca de los grupos de roles predeterminados, consulte Cambiar los permisos predeterminados.

10. Haga clic en **Gestionar**.

    Se visualiza un cuadro de diálogo que muestra el progreso de este proceso de gestión. Para asegurarse de que el proceso se completa satisfactoriamente, supervise el progreso.

11. Cuando el proceso esté completo, haga clic en **Aceptar**.

    El dispositivo se gestiona ahora mediante XClarity Administrator, que automáticamente sondea los dispositivos gestionados de forma periódica para recopilar información actualizada, como el inventario.

    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.

Después de finalizar

- Detecte y gestione dispositivos adicionales.
- Para configurar la información del sistema, el almacenamiento local, los adaptadores de E/S, los temas sobre el arranque y los valores de firmware, cree y despliegue patrones de servidor (consulte Configuración de servidores mediante el uso de patrones de configuración).
- Despliegue las imágenes del sistema operativo en los servidores que todavía no tienen un sistema operativo instalado (consulte Instalación de sistemas operativos en servidores sin sistema operativo).
- Actualice el firmware de los dispositivos que no cumplen las políticas actuales (consulte Actualización de firmware en dispositivos gestionados).
- Agregue los dispositivos al bastidor adecuado para reflejar el entorno físico (consulte Gestión de bastidores).
- Supervise el estado y los detalles del hardware (consulte Visualización del estado de un servidor gestionado).
- Descubra sucesos y alertas (consulte Trabajo con sucesos y Trabajo con alertas).
- Borre el registro de SEL para un servidor haciendo clic en **Hardware → Servidores** en la barra de menú XClarity Administrator, luego seleccione el servidor y haga clic en **Todas las acciones → Seguridad → Borrar registro de SEL**.Esta acción solo es compatible con servidores ThinkSystem y ThinkAgile.
- Resuelva credenciales almacenadas caducadas o no válidas (consulte Gestión de credenciales almacenadas).
- Habilite o deshabilite el inicio de sesión único para todos los servidores ThinkSystem y ThinkAgile gestionados haciendo clic en **Administración → Seguridad** desde la barra de menú de XClarity Administrator, haciendo clic en **Sesiones activas** y habilitando o deshabilitando el **inicio de sesión único**.
- 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.

Visualización del estado de un servidor gestionado

Puede ver un resumen y el estado detallado de los servidores gestionados y de los componentes que tienen instalados desde Lenovo XClarity Administrator.

Más información:

- XClarity Administrator: inventario
- XClarity Administrator: supervisión

Acerca de esta tarea

Los siguientes iconos de estado se usan para indicar el estado general del dispositivo. Si los certificados no coinciden, se agrega “(no es de confianza)” se agrega al estado de cada dispositivo aplicable, por ejemplo Advertencia (no es de confianza). Si existe un problema de conectividad o si la conexión del dispositivo no tiene confianza, “(Conectividad)” se agrega al estado del dispositivo aplicable, por ejemplo, Advertencia (Conectividad).

- ( ) Crítico
- ( ) Advertencia
- ( ) Pendiente
- ( ) Informativo
- ( ) Normal
- ( ) Fuera de línea
- ( ) Desconocido

Un dispositivo puede estar en uno de los siguientes estados de alimentación:

- Activado
- Apagado
- Apagar
- En espera
- Hibernar
- Desconocido

Procedimiento

Realice una o más de las acciones siguientes para ver el estado de un servidor gestionado.

- En la barra de menús de XClarity Administrator, pulse **Panel**. Se muestra la página del panel con una descripción general y el estado de todos los dispositivos gestionados y otros recursos.

- En la barra de menús de XClarity Administrator, haga clic en **Hardware → Servidores**. Se muestra la página Servidores con una vista de tabla de todos los servidores gestionados (servidores de bastidor y de torre y nodos de cálculo).

  Puede ordenar las columnas de la tabla para que sea más fácil encontrar servidores específicos. Además, puede seleccionar un tipo de sistema de la lista desplegable **Todos los sistemas**, introducir texto (como un nombre o dirección IP) en el campo **Filtro** y hacer clic en los iconos de estado para mostrar solo los servidores que cumplen los criterios seleccionados.

  Desde esta página puede llevar a cabo las siguientes acciones:

  – Ver información detallada sobre el servidor y sus componentes (consulte Visualización de los detalles de un servidor gestionado).

  – Vea un servidor en una vista gráfica de bastidores o de chasis haciendo clic en **Todas las acciones → Vistas → Mostrar en vista de bastidores** o **Todas las acciones → Vistas → Mostrar en vista de chasis**.

- Iniciar la interfaz web del controlador de gestión del servidor al hacer clic en el vínculo **Dirección IP** (consulte Inicio de la interfaz del controlador de gestión para un servidor).
- Gestionar remotamente el servidor (consulte Utilizar un control remoto para gestionar servidores convergidos, Flex System, NeXtScale y System x).
- Encender y apagar el servidor (consulte Encendido y apagado de un servidor).
- Modificar la información del sistema seleccionando un servidor y haciendo clic en **Todas las acciones → Inventario → Editar propiedades**.
- Actualizar el inventario al seleccionar un servidor y hacer clic en **Todas las acciones → Inventario → Actualizar inventario**.
- Exportar información detallada acerca de uno o varios servidores a un archivo CSV único al seleccionar los servidores y hacer clic en **Todas las acciones → Inventario → Exportar inventario**.

  Nota: Puede exportar datos de inventario para un máximo de 60 dispositivos por vez.

  Consejo: Al importar un archivo CSV en Microsoft Excel, Excel trata los valores de texto que contienen solo números como valores numéricos (por ejemplo, para UUID). Formatee cada celda como texto para corregir este error.
- Anular la gestión de un servidor (consulte Anulación de la gestión de un servidor de bastidor o de torre).
- Restablezca los adaptadores de almacenamiento local a su valor de fábrica predeterminado al hacer clic en **Todas las acciones → Servicio → Restablecer valores predeterminados de almacenamiento local**.
- Cambiar el estado del LED de ubicación en un servidor para que se encienda, apague o parpadee al seleccionar el servidor y hacer clic en **Todas las acciones → Servicio → Alternar el estado del LED de ubicación**, seleccionar el estado y posteriormente hacer clic en **Aplicar**.
  - No se admite la alternar el LED de ubicación para los servidores ThinkSystem SR635 y SR655.
  - El LED de ubicación en los servidores ThinkServer pueden estar encendidos o apagados. El parpadeo no es compatible.
- Reubicar virtualmente el servidor (consulte Reubicar virtualmente un servidor en un chasis de almacenamiento de Flex System).
- Excluir los sucesos que no sean de su interés de todas las páginas en las que se muestran sucesos haciendo clic en el icono **Excluir sucesos** () (consulte Exclusión de sucesos).
- Reinicie el servidor mediante una interrupción no enmascarable (NMI) al hacer clic en **Todas las acciones → Servicio → Activar NMI**
- Habilite o deshabilite los cambios de reglas de firewall en un servidor que limita las solicitudes entrantes a únicamente las procedentes de XClarity Administrator al seleccionar el servidor y hacer clic en **Todas las acciones → Seguridad → Habilitar Encapsulación** o **Acciones → Seguridad → Deshabilitar Encapsulación**.Los valores globales de la encapsulación están deshabilitados de forma predeterminada. Cuando está deshabilitado, el modo de encapsulación del dispositivo se establece como “normal” y las reglas de firewall no se cambian como parte del proceso de gestión.

  Cuando los valores globales de encapsulación están habilitados y el dispositivo admite la encapsulación, XClarity Administrator se comunica con el dispositivo durante el proceso de gestión para cambiar el modo de encapsulación del dispositivo a “encapsulationLite” y para cambiar las reglas de firewall en el dispositivo para limitar las solicitudes entrantes a únicamente las que se reciben de XClarity Administrator.

  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

archivo lenovoMgrAlert.mib y la Recuperación de la gestión con un CMM después de un error en el servidor de gestión.

- (Solo servidores Converged, Flex System, NeXtScale, System x y ThinkSystem) Solucionar los problemas que puedan surgir entre el certificado de seguridad de XClarity Administrator y el certificado de seguridad del controlador de gestión de la placa base del servidor seleccionando un servidor y haciendo clic en **Todas las acciones → Seguridad → Resolver certificados no fiables** (consulte Resolución de un certificado de servidor no fiable).
- Resolver credenciales almacenadas caducadas o no válidas para un dispositivo en el grupo (consulte Resolución de credenciales almacenadas caducadas o no válidas para un servidor).
- Agregue o quite un servidor de un grupo de recursos estático haciendo clic en **Todas las acciones → Grupos → Añadir a grupo** o **Todas las acciones → Grupos → Quitar del grupo**.

Visualización de los detalles de un servidor gestionado

Puede ver información detallada acerca de los servidores gestionados desde Lenovo XClarity Administrator, incluidos los niveles de firmware, el nombre del servidor y el identificador único universal (UUID).

Más información:

- XClarity Administrator: inventario
- XClarity Administrator: supervisión

Acerca de esta tarea

El uso de la CPU es una medida de la residencia de estado C agregada. Se mide como porcentaje de la residencia C0 usada y máxima, por segundo.

El uso de la memoria es una medición de los volúmenes de lectura/escritura agregados de todos los canales de memoria. Se calcula como porcentaje del ancho de banda de memoria usado y máximo que se encuentra disponible, por segundo.

La temperatura del aire en el nivel del sistema se mide mediante un sensor físico en la parte frontal del servidor. Esta temperatura representa la temperatura del aire de entrada que recibe el servidor. Tenga en cuenta que la temperatura del aire notificada por XClarity Administrator y el CMM puede variar si dicha temperatura se captura en diferentes momentos.

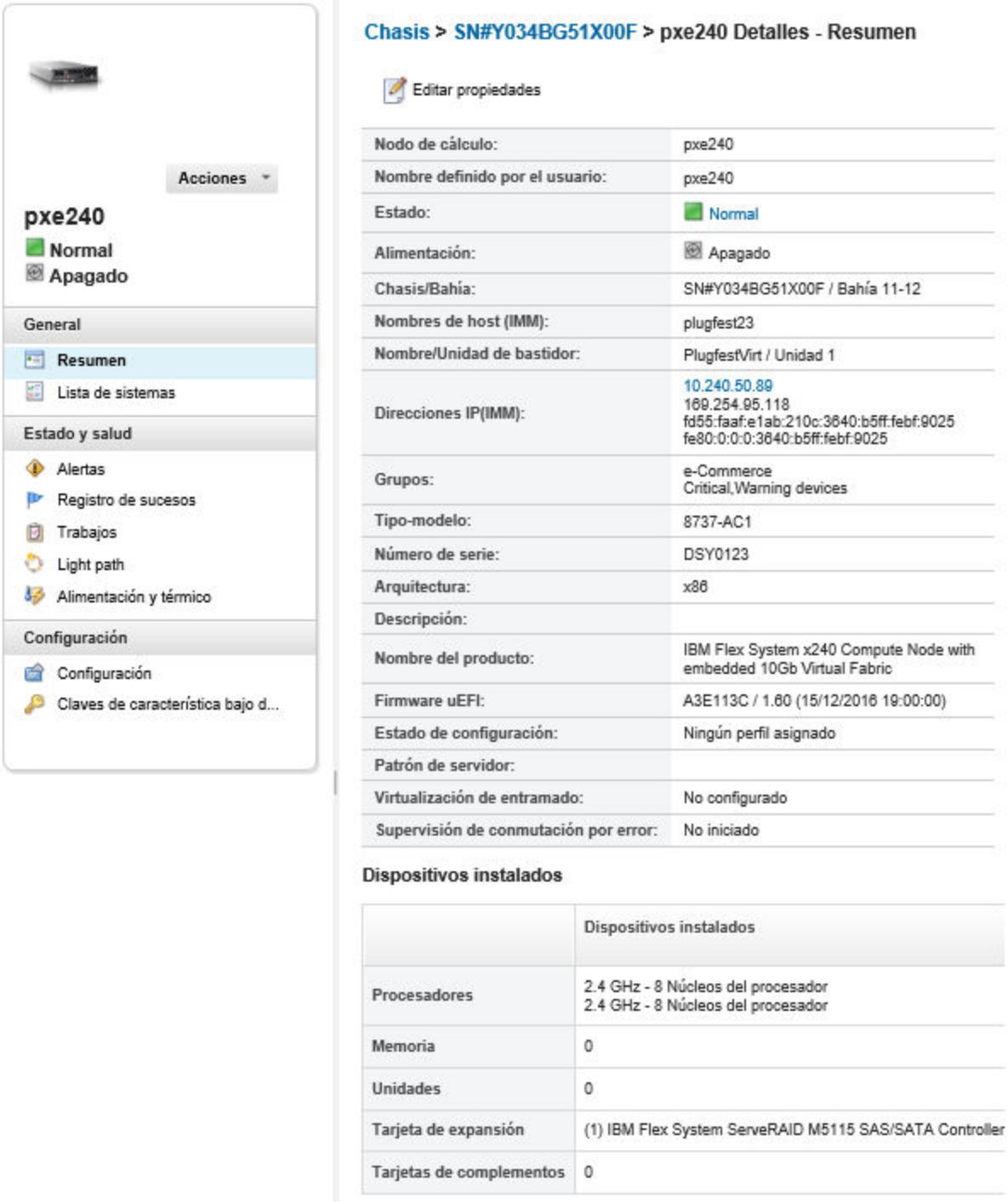
Procedimiento

Lleve a cabo los pasos siguientes para ver los detalles de un servidor gestionado.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Hardware → Servidores**. Se muestra la página Servidores con una vista de tabla de todos los servidores gestionados (servidores de bastidor y nodos de cálculo).

Puede ordenar las columnas de la tabla para que sea más fácil encontrar los servidores específicos. Además, puede seleccionar un tipo de sistema en la lista desplegable **Todos los sistemas** e introducir texto (como un nombre de sistema o una dirección IP) en el campo **Filtro** para filtrar mejor los servidores que se muestran.

Paso 2. Haga clic en el enlace relativo al servidor en la columna **Servidor**. Aparece la página de resumen de estado de dicho servidor, donde se muestran las propiedades del servidor y una lista de los componentes que están instalados en él.



Nota: Para servidores System x y NeXtScale, la dirección LAN sobre USB se muestra en esta página; no obstante, no puede cambiar dicha dirección desde XClarity Administrator. En su lugar, debe utilizar la interfaz del controlador de gestión de la placa base para el servidor. Para obtener más información, consulte “Acceso al IMM2 utilizando la interfaz LAN sobre USB” de la documentación del producto del servidor. Encontrará la documentación del producto de su servidor en Documentación en línea de BladeCenter.

Paso 3. Lleve a cabo una o más de las acciones siguientes:

- Haga clic en **Resumen** para ver un resumen del servidor, incluida información del sistema y los componentes instalados (consulte Visualización del estado de un servidor gestionado).

- Haga clic en **Detalles del inventario** para ver detalles sobre los componentes del servidor, incluidos:
  - Niveles de firmware para el servidor y el controlador de gestión.
  - Detalles de la red del módulo de gestión, como nombre de host, dirección IPv4, dirección IPv6 y direcciones MAC.
  - Detalles de los activos, incluidos el nombre del servidor, el identificador único universal (UUID) y la ubicación.
  - Detalles de los componentes, incluidas la CPU, la memoria, las unidades y las tarjetas de expansión.

  Notas:

  - Se enumeran todas las direcciones IP del servidor. La dirección IP del controlador de gestión del servidor se lista primero. Si la dirección IP del controlador de gestión está disponible, se utiliza para conectarse al servidor.
  - Si no hay datos disponibles para un adaptador específico, algunos campos para el adaptador (como el nombre del producto) pueden estar vacíos.
  - Si se instaló un nuevo adaptador en el servidor, el servidor se debe reiniciar para que el adaptador se muestre en el inventario.
  - En algunas tarjetas de complemento, se muestra información función a pedido (FoD) bajo el nombre del dispositivo.
  - Puede colocar el cursor sobre los vínculos incluidos en la columna Type (Tipo) para obtener más información acerca de componentes determinados, como la memoria de Intel Optain DCPMM.
- Pulse **Alertas** para mostrar la lista de las alertas actuales de este servidor (consulte Trabajo con alertas).

  Nota: Puede definir preferencias de umbral para generar alertas y sucesos cuando un valor, como la duración de una SSD en un servidor ThinkSystem o ThinkServer, supera un nivel crítico o de advertencia (consulte Configuración de preferencias de umbral para generar alertas y sucesos).
- Pulse **Registro de sucesos** para mostrar la lista de los sucesos actuales de este servidor (consulte Supervisión de sucesos en el registro de sucesos).
- Pulse **Trabajos** para mostrar una lista de trabajos asociados con el servidor (consulte Supervisión de trabajos).
- Haga clic en **Light Path** para mostrar el estado actual de los LED del servidor, incluidos la ubicación, los fallos y la información. Esto equivale a ver el panel frontal del servidor.
- Haga clic en **Alimentación y térmico** para mostrar los detalles acerca del uso de alimentación y la temperatura del aire.

  Consejo: utilice el botón Actualizar de su navegador web para recopilar los datos de alimentación y térmicos más recientes. La recopilación de datos puede durar varios minutos.
- Haga clic en **Configuración** para ver la información actual de configuración del servidor (incluidos el almacenamiento local, los adaptadores de E/S, la configuración de arranque de SAN y los valores de firmware) y su cumplimiento con el patrón de configuración asignado (consulte Configuración de servidores mediante el uso de patrones de configuración).
- Haga clic en **Claves de característica bajo demanda** para ver una lista de las claves de característica bajo demanda que se encuentran instaladas en la actualidad en el servidor gestionado (consulte Ver claves de Características bajo demanda).

Después de finalizar

Además de mostrar un resumen e información detallada sobre un servidor, también puede realizar las siguientes acciones:

- Vea el bastidor o un chasis que está asociado con el servidor haciendo clic en el nombre del bastidor o de chasis desde la página de resumen.
- Vea un servidor seleccionado en una vista gráfica de bastidores o de chasis haciendo clic en **Todas las acciones → Vistas → Mostrar en vista de bastidores** o **Todas las acciones → Vistas → Mostrar en vista de chasis**.
- Iniciar la interfaz web del controlador de gestión del servidor seleccionado al hacer clic en el vínculo **Dirección IP** (consulte Inicio de la interfaz del controlador de gestión para un servidor).
- Acceder remotamente a un servidor (consulte Utilizar un control remoto para gestionar servidores convergidos, Flex System, NeXtScale y System x).
- Encender un servidor seleccionado (consulte Encendido y apagado de un servidor).
- Modificar la información de un servidor seleccionado haciendo clic en **Editar propiedades**.
- Actualizar el inventario de un servidor seleccionado haciendo clic en **Acciones → Inventario → Actualizar inventario**.
- Exportar información detallada acerca de los servidores a un archivo CSV al hacer clic en **Acciones → Inventario → Exportar inventario**.

  Notas:

  – Para obtener más información sobre datos de inventario en el archivo CSV, consulte GET /nodes/*<UUID_list>* en la documentación en línea de XClarity Administrator.

  – Al importar un archivo CSV en Microsoft Excel, Excel trata los valores de texto que contienen solo números como valores numéricos (por ejemplo, para UUID). Formatee cada celda como texto para corregir este error.
- Excluya los sucesos que no sean de su interés de todas las páginas en las que se muestran sucesos al hacer clic en el icono **Acciones → Restablecer servicio → Excluir sucesos** (consulte Exclusión de sucesos).
- Reinicie un servidor seleccionado mediante una interrupción no enmascarable (NMI) al hacer clic en **Acciones → Servicio → Activar NMI**
- Cambie el estado del LED de ubicación en un servidor seleccionado para que se encienda, apague o parpadee, haciendo clic en **Acciones → Servicio → Alternar estado del LED de ubicación**, posteriormente seleccione el estado y haga clic en **Aplicar**.

  Notas:
  – No se admite la alternar el LED de ubicación para los servidores ThinkSystem SR635 y SR655.
  – El LED de ubicación en los servidores ThinkServer pueden estar encendidos o apagados. El parpadeo no es compatible.
- Deshabilitar o habilitar el inicio de sesión único para un servidor ThinkSystem y ThinkAgile seleccionado haciendo clic en **Todas las acciones → Seguridad → Habilitar el inicio de sesión único** o **Todas las acciones → Seguridad → Deshabilitar el inicio de sesión único**.

  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.

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

- Habilitar o deshabilitar los cambios de la regla de firewall en un servidor seleccionado que limita las solicitudes entrantes a únicamente las procedentes de XClarity Administrator al seleccionar el servidor y hacer clic en **Acciones → Seguridad → Habilitar encapsulación** o **Acciones → Seguridad → Deshabilitar encapsulación**. Los valores globales de la encapsulación están deshabilitados de forma predeterminada. Cuando está deshabilitado, el modo de encapsulación del dispositivo se establece como "normal" y las reglas de firewall no se cambian como parte del proceso de gestión.

  Cuando los valores globales de encapsulación están habilitados y el dispositivo admite la encapsulación, XClarity Administrator se comunica con el dispositivo durante el proceso de gestión para cambiar el modo de encapsulación del dispositivo a "encapsulationLite" y para cambiar las reglas de firewall en el dispositivo para limitar las solicitudes entrantes a únicamente las que se reciben de XClarity Administrator.

  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 archivo lenovoMgrAlert.mib y la Recuperación de la gestión con un CMM después de un error en el servidor de gestión.
- (Solo servidores no-ThinkServer) Resuelva los problemas que puedan surgir entre el certificado de seguridad de Lenovo XClarity Administrator y el certificado de seguridad del controlador de gestión en el servidor seleccionado haciendo clic en **Acciones → Seguridad → Resolver certificados no fiables** (consulte Resolución de un certificado de servidor no fiable).

Creación de copia de seguridad y restauración de datos de configuración de servidor

Lenovo XClarity Administrator no incluye funciones integradas de copia de seguridad de datos para la configuración de servidor. En su lugar, utilice las funciones de copia de seguridad disponibles para los servidores gestionados.

- **Servidores Converged, Flex System, System x, ThinkSystem y NeXtScale**
  - Creación de copia de seguridad de datos de configuración del servidor

    Utilice la interfaz web de la gestión o la CLI para hacer una copia de seguridad del firmware.
    - En la interfaz web del IMM, haga clic en **Gestión de IMM → Configuración de IMM**.
    - En la CLI, utilice el mandato `backup`.

    Para obtener más información acerca de cómo realizar una copia de seguridad de los servidores utilizando el IMM, consulte la Documentación en línea de Integrated Management Module II.

    Utilice las herramientas que se proporcionan con el sistema operativo para realizar una copia de seguridad de las aplicaciones que se encuentren en ejecución en el servidor. Para obtener más información, consulte la documentación incluida con su sistema operativo.

    En el caso de dispositivos de cálculo Flex System, asegúrese de realizar una copia de seguridad de los valores relativos a las opciones que se han instalado en dichos nodos. Puede realizar una copia de seguridad de todos los valores de los nodos de cálculo, incluidos los valores de las opciones, utilizando la aplicación Advanced Setup Utility (ASU). Para obtener más información sobre la aplicación ASU, consulte Sitio web de la utilidad de valores avanzados (ASU).
  - Restaurar los datos de configuración de servidor

    Utilice la interfaz web de la gestión o la CLI para restaurar el firmware. Para obtener más información sobre la restauración de los servidores a través del BMC, consulte Documentación en línea de Integrated Management Module II.

Utilice la documentación que se proporciona con el sistema operativo y con cualquier aplicación que se encuentre en ejecución en el servidor para restaurar el software que está instalado en el servidor.

- En la interfaz web del IMM, haga clic en **Gestión de IMM → Configuración de IMM**.
- En la CLI, utilice el mandato `restore`.

Nota: Consejo: encontrará información adicional acerca de cómo realizar una copia de seguridad de los componentes del chasis y restaurarlos en la Guía de prácticas recomendadas para la copia de seguridad y restauración de PureFlex y Flex System.

- **Servidores ThinkServer**Los procedimientos de restauración varían en función del tipo de servidor ThinkServer de que se trate. Consulte la documentación del producto que se proporciona con el servidor para obtener información acerca de cómo restaurar el dispositivo.

Habilitar protección del sistema

La función de protección del sistema supervisa las desviaciones en el inventario de hardware para los servidores ThinkSystem con XCC2.

Acerca de esta tarea

El inventario supervisado incluye procesadores, memoria, adaptadores PCI, unidades, placas del sistema y tarjetas de expansión. No se detectan cambios en los niveles de firmware ni en los valores de configuración.

Cuando la protección del sistema está habilitada, se toma una instantánea del inventario de hardware como referencia de confianza para cada dispositivo seleccionado. Cuando se reinicia un dispositivo, el controlador de gestión de la placa base del dispositivo recopila la configuración actual del sistema y la compara con la instantánea. Cuando se detecta una desviación para uno o más componentes, la función de protección del sistema genera un suceso. Si se detecta una desviación para un procesador o una memoria, la función de protección del sistema genera un suceso y, opcionalmente, evita que el servidor arranque en el SO.

Procedimiento

Para habilitar la protección del sistema en un servidores con XCC2 más, lleve a cabo los pasos siguientes.

Paso 1. En el menú de XClarity Administrator, haga clic en **Hardware → Servidores**. Se muestra la página Servidores con una vista de tabla de todos los servidores gestionados.

Paso 2. Seleccione uno o más servidores con XCC2.

Paso 3. Haga clic en **Todas las acciones → Seguridad → Habilitar protección del sistema** para mostrar el cuadro de diálogo Habilitar protección del sistema.

Paso 4. Elija la acción que debe realizarse cuando la protección del sistema esté habilitada, se detecte un cambio en el inventario y el servidor deje de ser conforme.

- **Habilitar y mantener el comportamiento predeterminado del sistema**. Se utiliza el comportamiento actual. . El comportamiento predeterminado es generar un suceso.
- **Habilitar y evitar el arranque del SO cuando es no conforme**. Se genera un evento. Si intenta arrancar en el SO, recibirá una advertencia si la función de protección del sistema detecta cambios de configuración en los procesadores o la memoria. En este caso, se le solicitará que inicie sesión en el controlador de gestión de la placa base si los cambios son inesperados. De lo contrario, puede continuar con el proceso de arranque o apagado. Si no responde en menos de 5 minutos, el servidor se apagará de forma predeterminada.
- **Habilitar y generar un suceso cuando es no conforme**. Se genera un suceso, pero no se realiza ninguna otra acción.

Paso 5. Haga clic en **Aplicar**.

Se crea un trabajo para crear instantáneas de inventario para el servidor seleccionado. Puede monitorear el progreso del trabajo desde el registro de trabajos. En la barra de menús de XClarity Administrator, haga clic en **Supervisión → Trabajos**. Para obtener más información sobre el registro de trabajos, consulte Supervisión de trabajos.

Después de finalizar

Para deshabilitar la función de protección del sistema en los servidores seleccionados, haga clic en **Todas las acciones → Seguridad → Deshabilitar protección del sistema** y luego haga clic en **Aplicar**.

Borrado seguro de los datos de la unidad

Lenovo XClarity Administrator puede borrar de forma segura los datos de todas las unidades en servidores ThinkSystem y ThinkAgile seleccionados ejecutando la versión 22B y posterior. Esta operación reescribe permanentemente cada unidad rellenando toda la unidad con datos binarios cero, binarios o aleatorios, lo que dificulta el descubrimiento de lo que se ha guardado en la unidad.

Atención:

- Esta operación borra *de forma permanente* e *irreversible* todos los datos de las unidades.
- No hay forma de cancelar esta operación después de enviar el trabajo.

Antes de empezar

Debe tener autoridad de **lxc-supervisor** para eliminar los datos de la unidad.

Asegúrese de que la contraseña de administrador de UEFI no se encuentra establecida en los servidores gestionados para borrarse. Si la contraseña de administrador de UEFI está establecida en cualquier servidor, las unidades de esos servidores no se borran.

De manera predeterminada, puede borrar de forma segura los datos de la unidad para hasta tres servidores a la vez. Puede configurar el número de servidores permitidos al mismo tiempo haciendo clic en **Administración → Preferencias de inventario** y estableciendo el **Número máximo de servidores que se pueden borrar en un proceso por lotes** en el valor deseado. Puede elegir un número de los servidores `3 - 100`.

Solo se permite un trabajo de eliminación segura al mismo tiempo. Debe esperar a que el trabajo actual se complete antes de iniciar otro trabajo de eliminación segura.

Se pueden tardar varias horas en borrar unidades de gran tamaño.

No se pueden borrar de forma segura los volúmenes SATA SDD que estén conectados a los controladores RAID Marvell. En su lugar, considere las siguientes recomendaciones.

- Para SSD SATA de 7 mm, conéctese a los controladores RAID Broadcom para realizar una eliminación segura.
- Para SSD SATA M.2, conéctese a los controladores no RAID Marvell (como el kit de habilitación de 2 bahías de ThinkSystem M.2 SATA/NVMe) para realizar una eliminación segura.

Acerca de esta tarea

Puede borrar los datos de las unidades siguientes.
- NVMe
- SAS
- SAS HBA

- SAS RAID
- SATA
- Dispositivos de almacenamiento de conexión externa
  - Lenovo Storage D1212 (MT 4587)
  - Lenovo Storage D1224 (MT 4587)
  - Lenovo Storage D3284 (MT 6413)

La operación de borrado seguro crea una entrada en el registro de auditoría. Puede reenviar estos sucesos mediante la función de reenvío de sucesos (consulte Enviar sucesos a syslog, en el gestor remoto de SNMP, correo electrónico y otros servicios de sucesos).

Para resolver los problemas de eliminación segura, consulte No se pueden borrar de forma segura los datos de la unidad en las unidades de disco duro y No se pueden borrar de forma segura volúmenes de SDD SATA cuando se conectan a RAID Marvell en la documentación en línea de XClarity Administrator.

Procedimiento

Para borrar de forma segura todas las unidades de servidores gestionados específicos, realice los pasos siguientes.

Paso 1. En el menú de XClarity Administrator, haga clic en **Hardware → Servidores**. Se muestra la página Servidores con una vista de tabla de todos los servidores gestionados.

Paso 2. Seleccione el servidor.

Paso 3. Haga clic en **Todas las acciones → Servicio → Borrado seguro de unidad (HDD/SDD)**.

Paso 4. Ingrese su contraseña de supervisor para confirmar que desea borrar todas las unidades de los servidores seleccionados.

Paso 5. Haga clic en **Borrar**.

Si elige realizar una eliminación masiva de la unidad en más de tres servidores, se le pedirá que introduzca su Id. de usuario y contraseña. Introduzca las mismas credenciales de usuario que utilizó para iniciar sesión en XClarity Administrator.

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

Uso del control remoto

Desde la interfaz web de Lenovo XClarity Administrator, puede abrir una sesión de control remoto a un servidor gestionado como si estuviera en una consola local. Puede utilizar una sesión de control remoto para realizar operaciones como encendido o apagado del servidor y para montar lógicamente una unidad remota o local.

Para iniciar una sesión de control remoto para cualquier dispositivo, debe tener privilegios de **lxc-supervisor**, **lxc-admin**, **lxc-security-admin**, **lxc-fw-admin**, **lxc-os-admin**, **lxc-hw-admin**, **lxc-service-admin** o **lxc-hw-manager**.

Uso del control remoto para gestionar servidores ThinkSystem o ThinkAgile

Desde la interfaz web de Lenovo XClarity Administrator, puede abrir una sesión de control remoto a un servidor ThinkSystem o ThinkAgile gestionado como si estuviera en una consola local. Puede utilizar la sesión de control remoto para realizar operaciones de encendido y para montar lógicamente una unidad local o de red.

Antes de empezar

La encapsulación se debe deshabilitar en el servidor.

Para abrir una sesión de control remoto de un servidor, este debe encontrarse en los estados En línea o Normal. Si un servidor tiene cualquier otro estado de acceso, la sesión de control remoto no se puede conectar al servidor. Para obtener más información acerca de cómo ver el estado del servidor, consulte Visualización de los detalles de un servidor gestionado.

Revise las siguientes consideraciones para los servidores ThinkSystem SR635 y SR655.
- Se requiere el firmware v2.94 o posterior del controlador de gestión de la placa base.
- Solo se admite el modo de varios usuarios; no se admite el modo de usuario único.
- Internet Explorer 11 no es compatible.
- No puede encender ni apagar un servidor desde una sesión de control remoto.

Acerca de esta tarea

Puede iniciar una sesión de control remoto en un solo servidor ThinkSystem o ThinkAgile desde XClarity Administrator.

Para obtener más información acerca de cómo utilizar la consola remota de ThinkSystem y las funciones de soportes, consulte la documentación del servidor ThinkSystem o ThinkAgile.

Nota: Para los servidores ThinkSystem y ThinkAgile, no se requiere un entorno Java Runtime Environment (JRE) con compatibilidad con Java WebStart.

Procedimiento

Complete los pasos siguientes para abrir una sesión de control remoto en un servidor determinado.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Hardware → Servidores**. Se muestra la página Servidores con una vista de tabla de todos los servidores gestionados (servidores de bastidor y nodos de cálculo).

Puede ordenar las columnas de la tabla para que sea más fácil encontrar servidores específicos. Además, puede seleccionar un tipo de sistema en la lista desplegable **Todos los sistemas** e introducir texto (como un nombre o una dirección IP) en el campo **Filtro** para filtrar mejor los servidores que se muestran.

Paso 2. Seleccione el servidor en el que desea abrir una sesión de control remoto.

Paso 3. Haga clic en el icono **Control remoto** ().

Paso 4. Acepte las advertencias de seguridad del navegador web.

Después de finalizar

Si la sesión de control remoto no se abre correctamente, consulte Problemas con el Control remoto en la documentación en línea de XClarity Administrator.

Utilizar un control remoto para gestionar servidores ThinkServer y NeXtScale sd350 M5

Desde la interfaz web de Lenovo XClarity Administrator, puede abrir una sesión de control remoto para gestionar servidores ThinkServer y NeXtScale sd350 M5 como si estuviera en una consola local. Puede utilizar una sesión de control remoto para realizar operaciones de alimentación y restablecimiento, para montar lógicamente una unidad de red o local en el servidor y crear capturas de pantalla y grabar video.

Antes de empezar

- El control remoto de estos servidores requiere un entorno Java Runtime Environment (JRE) con compatibilidad con Java WebStart instalada en el cliente. Se recomienda encarecidamente un JDK de código abierto. Si utiliza JRE o JDK de un proveedor, asegúrese de que está debidamente autorizado para uso comercial. Se admiten los siguientes JRE.
  - Oracle JRE 7 (consulte Sitio web de descarga de Oracle Java)

    Atención:
    - Java 7 requiere un mínimo de compatibilidad con TLSv1.2 (consulte Configuración de valores de criptografía en el servidor de gestión).
    - El soporte para Java 7 se desaprobará en un futuro.
  - Oracle JRE 8, que requiere una licencia pagada (consulte Sitio web de descarga de Oracle Java)
  - Adoptium OpenJDK 8 con el complemento IcedTea-Web v1.8 (consulte Sitio web de Adoptium OpenJDK).
  - Amazon Corretto 8 (consulte Sitio web de descarga de Amazon Corretto 8)

  Java WebStart no está incluido en los paquetes de instalación de OpenJDK o Coretto y se debe instalar por separado. IcedTea-Web u OpenWebStart pueden utilizarse bajo la licencia GNU GPLV2 (consulte Sitio web de descarga de IcedTea OpenJDK y Sitio web de OpenWebStart).
- Para el control remoto se requiere que se haya instalado una clave de Características bajo demanda para ThinkServer System Manager Premium Upgrade en los servidores ThinkServer. Para obtener más información acerca las claves de característica bajo demanda (FoD) que están instaladas en los servidores, consulte Ver claves de Características bajo demanda

Acerca de esta tarea

Puede iniciar una sesión de control remoto en un solo servidor ThinkServer desde XClarity Administrator.

Para abrir una sesión de control remoto de un servidor, este debe encontrarse en los estados En línea o Normal. Si un servidor tiene cualquier otro estado de acceso, la sesión de control remoto no se puede conectar al servidor. Para obtener más información acerca de cómo ver el estado del servidor, consulte Visualización de los detalles de un servidor gestionado.

Para obtener más información sobre cómo utilizar la consola remota de ThinkServer y las funciones de soportes, consulte la documentación del servidor ThinkServer.

Procedimiento

Complete los pasos siguientes para abrir una sesión de control remoto en un servidor determinado.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Hardware → Servidores**. Se muestra la página Servidores con una vista de tabla de todos los servidores gestionados (servidores de bastidor y nodos de cálculo).

Puede ordenar las columnas de la tabla para que sea más fácil encontrar servidores específicos. Además, puede seleccionar un tipo de sistema en la lista desplegable **Todos los sistemas** e introducir texto (como un nombre o una dirección IP) en el campo **Filtro** para filtrar mejor los servidores que se muestran.

Paso 2. Seleccione el servidor en el que desea abrir una sesión de control remoto.

Paso 3. Haga clic en el icono **Control remoto** ().

Paso 4. Acepte las advertencias de seguridad del navegador web.

Después de finalizar

Si la sesión de control remoto no se abre correctamente, consulte Problemas con el Control remoto en la documentación en línea de XClarity Administrator.

Utilizar un control remoto para gestionar servidores convergidos, Flex System, NeXtScale y System x

Desde la interfaz web de Lenovo XClarity Administrator, puede abrir una sesión de control remoto para gestionar servidores convergidos, Flex System, NeXtScale y System x como si estuviera en una consola local.

Antes de empezar

Más información: XClarity Administrator: control remoto

- El control remoto de estos servidores requiere un entorno Java Runtime Environment (JRE) con compatibilidad con Java WebStart instalada en el cliente. Se recomienda encarecidamente un JDK de código abierto. Si utiliza JRE o JDK de un proveedor, asegúrese de que está debidamente autorizado para uso comercial. Se admiten los siguientes JRE.
  - Oracle JRE 7 (consulte Sitio web de descarga de Oracle Java)

    Atención:
    - Java 7 requiere un mínimo de compatibilidad con TLSv1.2 (consulte Configuración de valores de criptografía en el servidor de gestión).
    - El soporte para Java 7 se desaprobará en un futuro.
  - Oracle JRE 8, que requiere una licencia pagada (consulte Sitio web de descarga de Oracle Java)
  - Adoptium OpenJDK 8 con el complemento IcedTea-Web v1.8 (consulte Sitio web de Adoptium OpenJDK).
  - Amazon Corretto 8 (consulte Sitio web de descarga de Amazon Corretto 8)

  Java WebStart no está incluido en los paquetes de instalación de OpenJDK o Coretto y se debe instalar por separado. IcedTea-Web u OpenWebStart pueden utilizarse bajo la licencia GNU GPLV2 (consulte Sitio web de descarga de IcedTea OpenJDK y Sitio web de OpenWebStart).
- Se puede iniciar una sesión de control remoto en los servidores que ejecutan los siguientes sistemas operativos (de 32 bits o de 64 bits):
  - Microsoft Windows 7
  - Microsoft Windows 8
  - Microsoft Windows 10
- Para el control remoto se requiere que se haya instalado una clave de Características bajo demanda de presencia remota en los servidores convergidos, NeXtScale y System x. Si no se detecta la clave de característica bajo demanda (FoD) en un servidor, la sesión de control remoto muestra el mensaje `Falta la clave de activación` para el servidor al mostrar la lista de servidores disponibles. 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). Para obtener más información sobre las claves de FoD que están instaladas en los servidores, consulte Ver claves de Características bajo demanda.
- La cuenta de usuario utilizada para iniciar la sesión de control remoto debe ser válida y haberse definido en el servidor de autenticación de XClarity Administrator. La cuenta de usuario también debe tener suficiente autoridad de usuario para acceder a un servidor y gestionarlo.
- Revise las consideraciones de seguridad, rendimiento y teclado antes de abrir una sesión de control remoto. Para obtener más información sobre estas consideraciones, consulte Consideraciones sobre el control remoto.
- En el cuadro de diálogo Control remoto se utilizan los valores de entorno local e idioma de pantalla definidos para el sistema operativo en el sistema local.Si el sistema local utiliza Windows, consulte Sitio web de Java para obtener información acerca de cómo cambiar el valor del entorno local. Para cambiar el

idioma de pantalla, instale una copia de Windows traducida o bien un paquete de idioma desde Sitio web de Windows.

Acerca de esta tarea

Puede iniciar varias sesiones de control remoto desde Lenovo XClarity Administrator. Cada sesión puede gestionar varios servidores.

Para abrir una sesión de control remoto de un servidor, este debe encontrarse en los estados En línea o Normal. Si un servidor tiene cualquier otro estado de acceso, la sesión de control remoto no se puede conectar al servidor. Para obtener más información acerca de cómo ver el estado del servidor, consulte Visualización de los detalles de un servidor gestionado.

Puede abrir una sesión de control remoto sin destino haciendo clic en **Aprovisionamiento → Control remoto** en la barra de menús de Lenovo XClarity Administrator. A continuación, acepte las advertencias de seguridad del navegador web.

Nota: Para nodos de cálculo Flex System x280, x480 y x880, puede iniciar una sesión de control remoto únicamente en el nodo principal. Si intenta iniciar una sesión de control remoto en un nodo no principal en un sistema de varios nodos, se abre el cuadro de diálogo Control remoto, pero no se muestra ningún vídeo.

Procedimiento

Siga estos pasos para iniciar una sesión de control remoto en un servidor convergido, Flex System, NeXtScale y System x específico.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Hardware → Servidores**. Se muestra la página Servidores con una vista de tabla de todos los servidores gestionados (servidores de bastidor y nodos de cálculo).

Puede ordenar las columnas de la tabla para que sea más fácil encontrar servidores específicos. Además, puede seleccionar un tipo de sistema en la lista desplegable **Todos los sistemas** e introducir texto (como un nombre o una dirección IP) en el campo **Filtro** para filtrar mejor los servidores que se muestran.

Paso 2. Seleccione el servidor en el que desea abrir una sesión de control remoto.

Paso 3. Haga clic en el icono **Control remoto** ().

Paso 4. Acepte las advertencias de seguridad del navegador web.

Paso 5. De manera opcional, seleccione guardar el icono de Control remoto en su Escritorio. Puede usar este icono para iniciar una sesión de control remoto sin iniciar sesión en la interfaz web de XClarity Administrator.

Paso 6. Cuando el sistema se lo pide, seleccione uno de los siguientes modos de conexión:

- **Modo de usuario único**. Establece una sesión de control remoto exclusiva con el servidor. El resto de las sesiones de control remoto de ese servidor se bloquearán hasta que se desconecte de dicho servidor. Esta opción solo está disponible si no hay otras sesiones de control remoto establecidas en el servidor.
- **Modo multiusuario**. Permite establecer varias sesiones de control remoto con el mismo servidor. XClarity Administrator admite hasta seis sesiones de control remoto simultáneas en el mismo servidor.

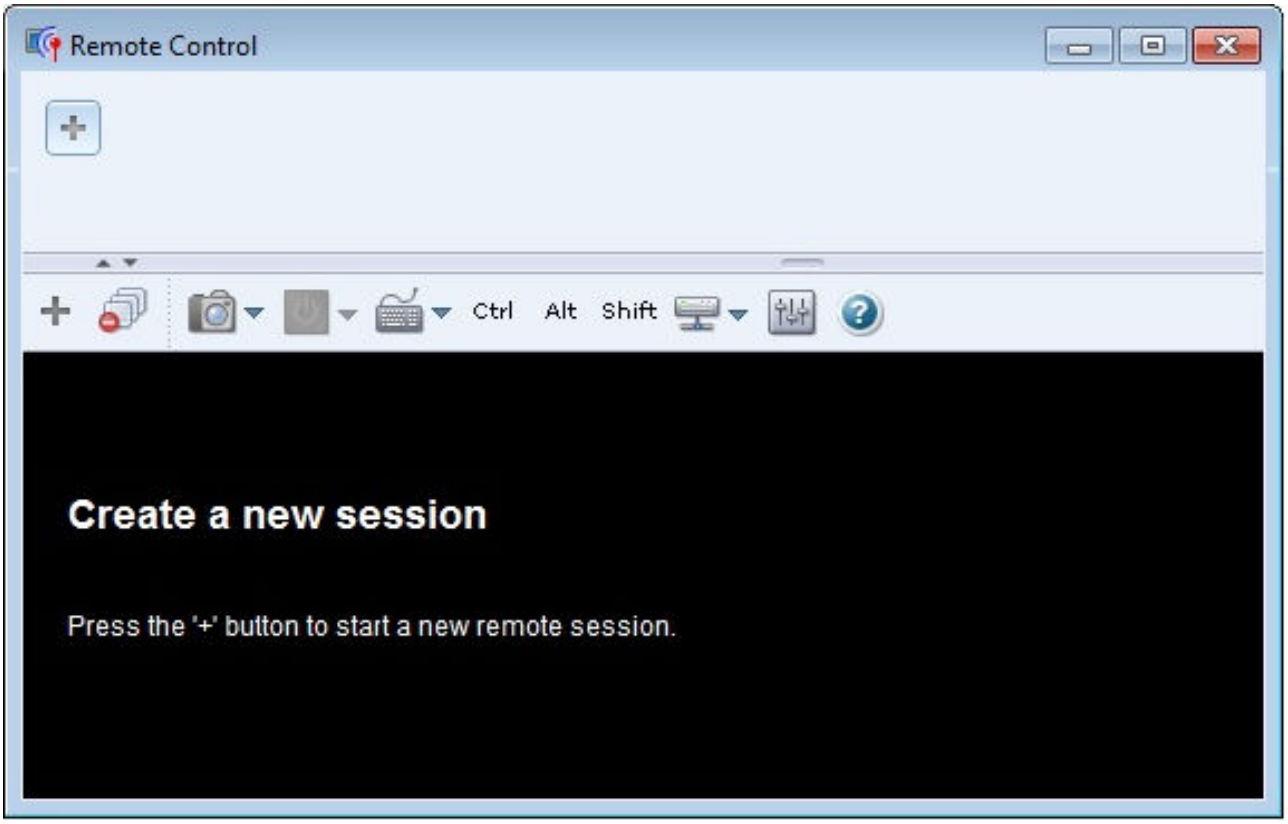
Paso 7. Cuando el sistema se lo pida, elija si desea guardar un acceso directo a la sesión de control remoto en el sistema local.

Si guarda el acceso directo, puede utilizarlo para abrir una sesión de control remoto en el servidor especificado sin tener que iniciarlo desde la interfaz web de XClarity Administrator. No obstante, el sistema local debe tener acceso a XClarity Administrator para validar la cuenta de usuario con el servidor de autenticación de XClarity Administrator.

El acceso directo contiene un enlace que abre una sesión de control remoto a la que se pueden añadir servidores manualmente.

Resultados

Aparece la ventana Control remoto.



En el área de miniaturas se muestran las miniaturas de todas las sesiones de servidor que actualmente se están gestionando mediante la sesión de control remoto.

Puede visualizar varias sesiones de servidor y desplazarse por ellas pulsando una miniatura, que muestra la consola del servidor en el área de sesiones de vídeo. Si está accediendo a más servidores de los que caben en el área de miniaturas, haga clic en los iconos **Desplazamiento hacia la derecha** ( ) y **Desplazamiento hacia la izquierda** ( ) para desplazarse por otras miniaturas de servidores. Haga clic en el icono **Todas las sesiones** ( ) para ver una lista de todas las sesiones de servidor abiertas.

En el área de miniaturas, haga clic en el icono **Añadir servidor** ( ) para añadir un servidor nuevo a la lista de servidores que está gestionando. Para obtener más información sobre cómo añadir una sesión, consulte Adición de una consola de servidor a una sesión de control remoto. Puede controlar la visualización del área

de miniaturas y la frecuencia con la que se actualizan desde la página Miniatura. Para obtener más información sobre los valores de miniaturas, consulte Definición de las preferencias del control remoto.

Después de finalizar

Si la sesión de control remoto no se abre correctamente, consulte Problemas con el Control remoto en la documentación en línea de XClarity Administrator.

En el cuadro de diálogo Control remoto, puede llevar a cabo las siguientes acciones:

- Añadir una sesión en otros servidores a la sesión de control remoto actual (consulte Adición de una consola de servidor a una sesión de control remoto).
- Ocultar o mostrar el área de miniaturas pulsando el icono **Alternar miniaturas** ().
- Mostrar la sesión de control remoto en una ventana o a pantalla completa; para ello, haga clic en el icono **Pantalla** () y haga clic en **Activar pantalla completa** o **Desactivar pantalla completa**.
- Utilizar las teclas Ctrl, Alt y Mayús en una sesión de control remoto (consulte Uso de las teclas Ctrl, Alt y Mayús).
- Definir las secuencias de teclas personalizadas, denominadas teclas programables (consulte Definición de teclas programables).
- Realizar una captura de pantalla de la sesión de servidor seleccionada en la actualidad y guardarla en distintos formatos; para ello, haga clic en el icono **Pantalla** () y, a continuación, haga clic en **Captura de pantalla**.
- Montar un medio remoto (como un dispositivo CD, DVD o USB, una imagen de disco o una imagen de CD (ISO)) en el servidor seleccionado, o bien mover un dispositivo montado a otro servidor (consulte Montaje o traslado de un medio remoto).
- Cargar imágenes a un servidor a partir de un medio remoto (consulte Carga de una imagen en el servidor).
- Encender o apagar el servidor desde una consola remota (consulte Encendido y apagado de un servidor desde una sesión de control remoto).
- Cambiar las preferencias del control remoto (consulte Definición de las preferencias del control remoto).

Consideraciones sobre el control remoto

Tenga en cuenta las consideraciones de seguridad, rendimiento y teclado relacionadas con el acceso a los servidores gestionados mediante una sesión de control remoto.

Consideraciones de seguridad

La cuenta de usuario utilizada para iniciar la sesión de control remoto debe ser válida y haberse definido en el servidor de autenticación de Lenovo XClarity Administrator. La cuenta de usuario también debe tener suficiente autoridad de usuario para acceder a un servidor y gestionarlo.

De manera predeterminada, se pueden establecer varias sesiones de control remoto en un servidor. No obstante, al iniciar una sesión de control remoto, tiene la opción de iniciar la sesión en modo de usuario único, que establece una sesión exclusiva con el servidor. El resto de las sesiones de control remoto de dicho servidor se bloquean hasta que se desconecta de dicho servidor.

Nota: Esta opción solo está disponible si actualmente no hay otras sesiones de control remoto establecidas en el servidor.

Para utilizar la normativa federal de procesamiento de la información (FIPS) 140, debe habilitarla manualmente llevando a cabo los siguientes pasos en el sistema local:

1. Busque el nombre del proveedor criptográfico certificado de FIPS 140 que está instalado en el sistema local.

   Consejo: para obtener más información acerca del cumplimiento con FIPS 140, consulte la Sitio web de modo de conformidad con FIPS 140 para SunJSSE.
2. Edite el archivo `$(java.home)/lib/security/java.security`.
3. Modifique la línea que incluye `com.sun.net.ssl.internal.ssl.Provider` agregando el nombre de su proveedor criptográfico certificado de FIPS 140. Por ejemplo, cambie:
   `security.provider.4=com.sun.net.ssl.internal.ssl.Provider`
   a:
   `security.provider.4=com.sun.net.ssl.internal.ssl.Provider SunPKCS11-NSS`

Consideraciones de rendimiento

Si una sesión de control remoto se vuelve lenta o no responde, cierre todas las sesiones de vídeo de y de medios remotos que haya establecido con el servidor seleccionado para reducir el número de conexiones de servidor abiertas. Además, puede aumentar el rendimiento modificando las preferencias siguientes. Para obtener más información, consulte el apartado Definición de las preferencias del control remoto.

- **KVM**
  - Disminuya el porcentaje de ancho de banda de video que utiliza la aplicación. Se reducirá la calidad de la imagen de la sesión de control remoto.
  - Disminuya el porcentaje de fotogramas que actualiza la aplicación. Se reducirá la frecuencia de actualización de la sesión de control remoto.
- **Miniaturas**
  - Aumente el intervalo de actualización de las miniaturas. La aplicación actualizará las miniaturas a un ritmo más lento.
  - Desactive la visualización de las miniaturas por completo.

El tamaño de la sesión de control remoto y el número de sesiones activas podrían afectar a los recursos de la estación de trabajo, como la memoria y el ancho de banda de la red, que pueden influir en el rendimiento. La sesión de control remoto utiliza un límite flexible de 32 sesiones abiertas. Si hay más de 32 sesiones abiertas, el rendimiento podría degradarse gravemente y es posible que la sesión de control remoto no responda. También podría experimentar una degradación del rendimiento con menos de 32 sesiones abiertas si los recursos, incluido el ancho de banda de la red y la memoria local, no son suficientes.

Consideraciones acerca del teclado

La sesión de control remoto admite los siguientes tipos de teclado:
- Belga de 105 teclas
- Brasileño
- Chino
- Francés de 105 teclas
- Alemán de 105 teclas
- Italiano de 105 teclas
- Japonés de 109 teclas
- Coreano
- Portugués
- Ruso
- Español de 105 teclas
- Suizo de 105 teclas
- Inglés de 105 teclas
- Estadounidense de 104 teclas

Para obtener información sobre las preferencias de teclado, consulte Definición de las preferencias del control remoto.

Adición de una consola de servidor a una sesión de control remoto

Puede añadir una o varias consolas de servidor a la sesión de control remoto actual.

Procedimiento

Lleve a cabo los pasos siguientes para añadir una o varias consolas de servidor a la sesión de control remoto actual.

Paso 1. En la ventana Control remoto, haga clic en el icono **Nueva sesión** ().

Se muestra un cuadro de diálogo con una lista de los chasis y servidores de bastidor disponibles que están gestionados por Lenovo XClarity Administrator y que su cuenta de usuario tiene permiso para gestionar.

Consejo: si no aparecen servidores en la lista, consulte Problemas con el Control remoto en la documentación en línea de XClarity Administrator para conocer procedimientos que pueden ayudarle a solucionar el problema.

Paso 2. Seleccione uno o varios servidores a los que desee conectarse.

Puede filtrar los servidores mostrados seleccionando un tipo de sistema en la lista desplegable **Tipo** y especificando un texto (por ejemplo, el nombre del sistema o del alojamiento) en el campo **Filtro**.

Puede seleccionar **Seleccionar todo** para seleccionar todos los servidores de la lista.

Paso 3. **Opcional:** seleccione **Modo de usuario único** para abrir una sesión exclusiva con cada servidor seleccionado.

Si selecciona esta opción, todas las demás sesiones de control remoto con los servidores seleccionados se bloquearán hasta que se desconecte de ellos. Esta opción solo está disponible si no hay otras sesiones de control remoto establecidas para los servidores seleccionados.

Si no seleccione esta opción, se utiliza el modo multiusuario de forma predeterminada.

Paso 4. Pulse **Conectar**.

Encendido y apagado de un servidor desde una sesión de control remoto

Puede encender y apagar un servidor desde una sesión de control remoto.

Procedimiento

Lleve a cabo los pasos siguientes para encender y apagar un servidor.

Paso 1. En la ventana Control remoto, haga clic en la miniatura del servidor que desee encender o apagar.

Paso 2. Pulse el icono **Alimentación** (); a continuación, pulse una de las acciones de encendido o apagado siguientes:

- **Encender**
- **Apagar normalmente**
- **Apagar inmediatamente**
- **Reiniciar normalmente**
- **Reiniciar de inmediato**
- **Activar NMI**

- **Reiniciar a configuración del sistema** (únicamente servidores Lenovo Converged, Flex System, NeXtScale y System x)

Consejo: el icono **Alimentación** se muestra en verde si el servidor está encendido en ese momento.

Definición de teclas programables

Puede definir sus propias secuencias de teclas personalizadas, que se denominan *teclas programables*, para la sesión de control remoto actual.

Antes de empezar

Para mostrar la lista actual de definiciones de teclas programables, haga clic en el icono **Teclado** ().

Las definiciones de las teclas programables se almacenan en el sistema desde el que inició la sesión de control remoto. Por lo tanto, si inicia la sesión de control remoto desde otro sistema, tendrá que definir de nuevo las teclas programables.

Si lo desea, puede exportar valores de usuario (incluidas las teclas programables), desde la pestaña **Valores de usuario** del cuadro de diálogo Preferencias. Para obtener más información, consulte el apartado Importación y exportación de valores de usuario.

Nota: Si utiliza un teclado internacional y define teclas programables que requieren la tecla AltGr, asegúrese de que el sistema operativo de la estación de trabajo que utiliza para invocar la aplicación de control remoto tenga el mismo tipo de sistema operativo que el servidor al que va a acceder de forma remota. Por ejemplo, si el servidor ejecuta Linux, asegúrese de invocar la sesión de control remoto desde una estación de trabajo que ejecute Linux.

Procedimiento

Para añadir una tecla programable, siga este procedimiento.

Paso 1. En la ventana Control remoto, haga clic en el icono **Teclado** (); a continuación, haga clic en **Añadir tecla programable**. Se muestra la pestaña **Programador de teclas programables** en el cuadro de diálogo Preferencias.

Paso 2. Haga clic en **Nuevo**.

Paso 3. Presione la secuencia de teclas que desee definir.

Paso 4. Pulse **Aceptar**. La nueva tecla programable se añade a la lista de teclas programables.

Uso de las teclas Ctrl, Alt y Mayús

Algunos sistemas operativos interceptan determinadas teclas en lugar de transferirlas al servidor remoto. Puede utilizar los botones de teclas especiales para enviar pulsaciones de tecla directamente al servidor que está gestionando.

Procedimiento

Para enviar combinaciones de las teclas Ctrl o Alt, pulse el botón **Ctrl** o **Alt** en la barra de herramientas, sitúe el cursor en el área de sesiones de vídeo y pulse una tecla del teclado.

Por ejemplo, para enviar una combinación de las teclas Ctrl+Alt+Supr, siga estos pasos:

1. Haga clic en **Ctrl** en la barra de herramientas.
2. Haga clic en **Alt** en la barra de herramientas.
3. Haga clic en con el botón izquierdo en cualquier parte dentro del área de sesiones de video.

4. Presione la tecla Suprimir del teclado.

Nota: si está habilitado el modo de captura de ratón, presione la tecla Alt izquierda para mover el cursor fuera del área de sesiones de video. Aunque el modo de captura de ratón está deshabilitado de forma predeterminada, puede habilitarlo desde la página Barra de herramientas (consulte Definición de las preferencias del control remoto).

Al pulsar el botón **Ctrl**, **Alt** o **Mayús** en la barra de herramientas para activar la tecla, esta permanece activa hasta que se pulsa una tecla del teclado o se vuelve a pulsar el botón.

Montaje o traslado de un medio remoto

Puede usar la función de medio remoto para montar en el servidor seleccionado un medio remoto, como un dispositivo CD, DVD o USB, una imagen de disco o una imagen de CD (ISO), que se encuentre en el sistema local. Además, puede cargar una imagen al almacenamiento local que esté disponible en el controlador de gestión de la placa base (BMC).

Antes de empezar

Solo es posible montar y cargar datos en el sistema de almacenamiento local del controlador de gestión por un usuario cada vez. El resto de usuarios no podrán acceder al sistema de almacenamiento local del controlador de gestión mientras se estén montando o cargando datos en él.

En un servidor que esté ejecutando el sistema operativo Linux, no se permite montar más de una imagen ISO.

Procedimiento

Lleve a cabo los pasos siguientes para montar o mover un medio remoto.

Paso 1. En la ventana Control remoto, haga clic en el icono **Medio remoto** ().

Paso 2. Haga clic en una de las acciones siguientes:

- **Montar medio remoto**

  Con esta acción, los recursos de los medios locales están disponibles para el servidor seleccionado. Un recurso de medios solo se puede montar en un servidor cada vez, dentro de una única sesión de control remoto.

  Al hacer clic en **Montar medio remoto**, están disponibles las opciones siguientes:

  – **Seleccionar una imagen para montarla**. La imagen estará disponible para el servidor seleccionado hasta que desmonte el dispositivo o cierre la sesión de control remoto. Se pueden montar varias imágenes en un único servidor y cada imagen se puede montar en varios servidores.

  – **Seleccionar una unidad, como un CD, DVD o dispositivo USB para montarlo**. El dispositivo estará disponible para el servidor seleccionado hasta que desmonte la unidad o cierre la sesión de control remoto. Se pueden montar varios dispositivos en un único servidor, pero cada dispositivo solo se puede montar en un servidor cada vez.

    Nota: si selecciona una unidad, asegúrese de desmontarla antes de quitar el medio de la unidad.

  – **Cargar la imagen al IMM**. Utilice esta opción para almacenar una imagen en el sistema de almacenamiento local del controlador de gestión para el servidor seleccionado. La imagen permanece en el controlador de gestión aunque finalice la sesión de control remoto o en el caso de que se reinicie el servidor.

    Puede almacenar aproximadamente 50 MB de datos en el controlador de gestión.

Puede cargar varias imágenes en el controlador de gestión siempre que el espacio total que se utilice para todas las imágenes sea inferior a 50 MB.

Cada imagen que se carga en el controlador de gestión se monta automáticamente en el servidor. Después de cargar una imagen en el controlador de gestión, también puede moverla al controlador de gestión para otro servidor. Si mueve la imagen, la imagen cargada previamente se quita del servidor actual y se carga en un servidor seleccionado.

- **Mover medio remoto**

  Con esta acción se mueve un recurso de medios montado previamente entre los servidores.

  Lleve a cabo los pasos siguientes para hacer que un recurso quede disponible para un servidor:

  1. Seleccione uno o varios recursos.
  2. Haga clic en **Añadir** para mover los recursos a la lista **Recursos seleccionados**.
  3. Haga clic en **Montar** para montar los recursos y utilizarlos en el servidor. La sesión de control remoto define un dispositivo para el recurso y lo asocia a un punto de montaje para el servidor seleccionado. Tiene la opción de proteger contra escritura el medio montado.

Carga de una imagen en el servidor

Puede cargar una imagen al sistema de almacenamiento local que esté disponible en el controlador de gestión de la placa base (BMC) para el servidor seleccionado.

Acerca de esta tarea

La imagen permanece en el controlador de gestión aunque finalice la sesión de control remoto o en el caso de que se reinicie el servidor.

Puede almacenar aproximadamente 50 MB de datos en el controlador de gestión.

Puede cargar varias imágenes en el controlador de gestión siempre que el espacio total que se utilice para todas las imágenes sea inferior a 50 MB.

Cada imagen que se carga en el controlador de gestión se monta automáticamente en el servidor. Después de cargar una imagen en el controlador de gestión, también puede moverla al controlador de gestión para otro servidor. Si mueve la imagen, la imagen cargada previamente se quita del servidor actual y se carga en un servidor seleccionado.

Procedimiento

Lleve a cabo los pasos siguientes para cargar una imagen en el servidor.

Paso 1. En la ventana Control remoto, haga clic en el icono **Medio remoto** ().

Paso 2. Pulse **Montar medio remoto**.

Paso 3. Pulse **Cargar la imagen al IMM**.

Importación y exportación de valores de usuario

Puede optar por importar o exportar los valores de usuario de la sesión de control remoto actual.

Acerca de esta tarea

Al exportar los valores de usuario, todos los valores de usuario de la sesión de control remoto actual se almacenan en un archivo de propiedades en el sistema local. Puede copiar este archivo de propiedades en otro sistema e importar los valores en la aplicación de control remoto para utilizarlos.

Procedimiento

Lleve a cabo los siguientes pasos para importar o exportar los valores de usuario de la sesión de control remoto actual.

Paso 1. En la ventana Control remoto, haga clic en el icono **Preferencia** ().

Paso 2. Haga clic en la pestaña **Valores de usuario**.

Paso 3. Pulse **Importar** para importar los valores de un archivo exportado o bien pulse **Exportar** para guardar todos los valores de usuario actuales en un archivo de propiedades en el sistema local.

Definición de las preferencias del control remoto

Puede modificar los valores de preferencias de la sesión de control remoto actual.

Procedimiento

Lleve a cabo los pasos siguientes para modificar las preferencias del control de remoto.

Paso 1. Para modificar las preferencias de control remoto, haga clic en el icono **Preferencias** (). Todos los cambios se aplican con efecto inmediato.

- **KVM**
  - **Porcentaje de ancho de banda de video**. Cuando se aumenta el ancho de banda, mejora la calidad de la apariencia de la sesión de control remoto, pero el rendimiento de esta puede verse afectado.
  - **Porcentaje de fotogramas actualizados**. Cuando se aumenta el porcentaje de fotogramas actualizados, aumenta la frecuencia con la que se actualiza la sesión de control remoto, pero el rendimiento de esta puede verse afectado.
  - **Tipo de teclado**. Seleccione el tipo de teclado que va a utilizar para la sesión de control remoto. El tipo de teclado seleccionado debe coincidir con los valores de teclado del sistema local y del host remoto.

    Nota: Si selecciona un teclado internacional y necesita introducir combinaciones de teclas que requieren la tecla AltGr, asegúrese de que el sistema operativo de la estación de trabajo que utiliza para invocar la sesión de control remoto tenga el mismo tipo de sistema operativo que el servidor al que desea a acceder de forma remota. Por ejemplo, si el servidor ejecuta Linux, asegúrese de invocar la aplicación de control remoto desde una estación de trabajo que ejecute Linux.
  - **Escalar imagen a la ventana**. Seleccione esta opción para escalar la imagen de vídeo que se ha recibido desde el servidor al tamaño del área de sesiones de vídeo.
- **Seguridad**
  - **Preferir conexiones con modo de usuario único**. Especifique si el modo de usuario único debe ser la opción predeterminada para las conexiones con un servidor. Cuando se establece una conexión con el modo de usuario único, solo un usuario puede conectarse a un servidor cada vez. Si esta casilla no está seleccionada, la función predeterminada consiste en conectarse al servidor con el modo de multiusuario.
  - **Requerir conexiones de túnel (seguras)**. Seleccione esta opción para acceder a un servidor mediante el nodo de gestión. Puede utilizar esta opción para acceder a un servidor de un cliente que no esté en la misma red que el servidor.

    Nota: La aplicación de control remoto siempre intentará conectarse directamente al servidor desde el sistema local donde se inició la sesión de control remoto. Si selecciona esta opción, la aplicación de control remoto accederá al servidor mediante Lenovo XClarity Administrator cuando la estación de trabajo cliente no pueda acceder directamente al servidor.

- **Barra de herramientas**

  Nota: Haga clic en **Restaurar valores predeterminados** para restaurar todos los valores de esta página con los valores predeterminados.

  - **Fijar barra de herramientas en la ventana**. De forma predeterminada, la barra de herramientas está oculta encima de la ventana de la sesión de control remoto y solo se muestra cuando mueve el puntero del ratón por encima de ella. Si selecciona esta opción, la barra de herramientas se fija a la ventana y se muestra siempre entre el panel de las miniaturas y la ventana de la sesión de control remoto.
  - **Mostrar botones del teclado**. Especifique si los iconos de los botones del teclado (Bloq Mayús, Bloq Num y Bloq Despl) se deben mostrar en la barra de herramientas.
  - **Mostrar control de alimentación**. Especifique si las opciones de control de alimentación deben mostrarse en la barra de herramientas.
  - **Mostrar botones de teclas especiales**. Especifique si los iconos de los botones de las teclas especiales (Ctrl, Alt y Supr) deben mostrarse en la barra de herramientas.
  - **Ocultar puntero de ratón local**. Especifique si el puntero del ratón local debe mostrarse al situar el cursor en la sesión del servidor que se muestra en ese momento en el área de sesiones de vídeo.
  - **Habilitar modo de captura de ratón**. De forma predeterminada, el modo de captura de ratón está deshabilitado. Esto significa que puede mover libremente el cursor dentro y fuera del área de sesiones de vídeo. Si habilita el modo de captura de ratón, debe hacer clic en la tecla Alt izquierda para mover el cursor fuera del área de sesiones de video. Si el modo de captura de ratón está habilitado, puede especificar si se deben utilizar las teclas Ctrl+Alt para salir de este modo. La opción predeterminada consiste en utilizar la tecla Alt izquierda.
  - **Especificar opacidad de fondo de barra de herramientas**. Al reducir el porcentaje de opacidad, se muestra más área de sesiones de vídeo en el fondo de la barra de herramientas.

    Nota: Esta opción solo está disponible cuando la barra de herramientas no está fijada a la ventana.
- **Miniaturas**
  - **Mostrar miniaturas**. Seleccione esta opción para mostrar el área de miniaturas en la sesión de control remoto.
  - **Especificar intervalo de actualización de miniaturas**. Al reducir el intervalo de actualización de las miniaturas, aumenta la frecuencia con la que se actualizan las miniaturas del servidor.
- **General**
  - **Modo de depuración**. Especifique si se debe definir el modo de depuración para la aplicación de control remoto. Los valores determinan la granularidad de los sucesos que se registran en los archivos de registro. De forma predeterminada, solo se registran los sucesos graves. Para obtener más información acerca de las ubicaciones de los archivos de registro, consulte Visualización de los registros y rastreos del control remoto.
  - **Heredar valores de apariencia del sistema**. Este valor permite cambiar la apariencia para que coincida con los esquemas de color que están configurados para el servidor local (que ejecuta Windows). Debe reiniciar la aplicación de control remoto para que estos valores surtan efecto.
  - **Crear icono del escritorio**. Este valor crea un icono de escritorio en el sistema local para que pueda iniciar la aplicación de control remoto directamente desde su sistema. Debe seguir teniendo acceso al software de gestión desde su sistema.

– **Sincronizar con servidor de gestión**. Este valor garantiza que los datos del servidor que se muestran en la aplicación de control remoto coinciden con los datos del servidor que se muestran en el software de gestión.

Visualización de los registros y rastreos del control remoto

Cuando se inicia una sesión de control remoto, se crean archivos de registro. Los tipos de sucesos que se registran en estos archivos están basados en el modo de depuración, que se establece en la pestaña **General** del cuadro de diálogo Preferencias. Puede utilizar estos archivos de registro para resolver problemas.

Procedimiento

Los archivos de registro de control remoto se almacenan en las ubicaciones siguientes.

Sistema operativo	Directorio de registro
Windows 7 y Windows 8	`%USERPROFILE%\lenovo\remoteaccess` Por ejemplo:`C:\Users\win_user\lenovo\remoteaccess`

Para obtener más información sobre cómo recopilar y descargar archivos de diagnósticos y enviárselos a Lenovo Soporte, consulte Trabajo con servicio y soporte en la documentación en línea de Lenovo XClarity Administrator.

Gestión de acceso a los sistemas operativos en servidores gestionados

Puede gestionar acceso a los sistemas operativos en servidores gestionados.

Antes de empezar

Debe tener autoridad de **lxc-os-admin**, **lxc-supervisor**, **lxc-admin** o **lxc-hw-admin** para gestionar y desplegar controladores de dispositivos y realizar acciones avanzadas en servidores gestionados desde las páginas de Actualización del controlador Windows.

Acerca de esta tarea

Antes de que Lenovo XClarity Administrator pueda actualizar los controladores de dispositivos de SO en un sistema gestionado, debe proporcionar información para acceder al sistema operativo de host, incluida la dirección IP del sistema operativo y las credenciales de administrador almacenadas para acceder al sistema operativo host. Para obtener más información sobre cómo actualizar los controladores de dispositivos de SO, consulte Actualización de los controladores de dispositivos de Windows en servidores gestionados.

XClarity Administrator utiliza las credenciales almacenadas para la autenticación con el sistema operativo del host. Para obtener más información acerca de cómo crear credenciales almacenadas en XClarity Administrator, consulte Gestión de credenciales almacenadas.

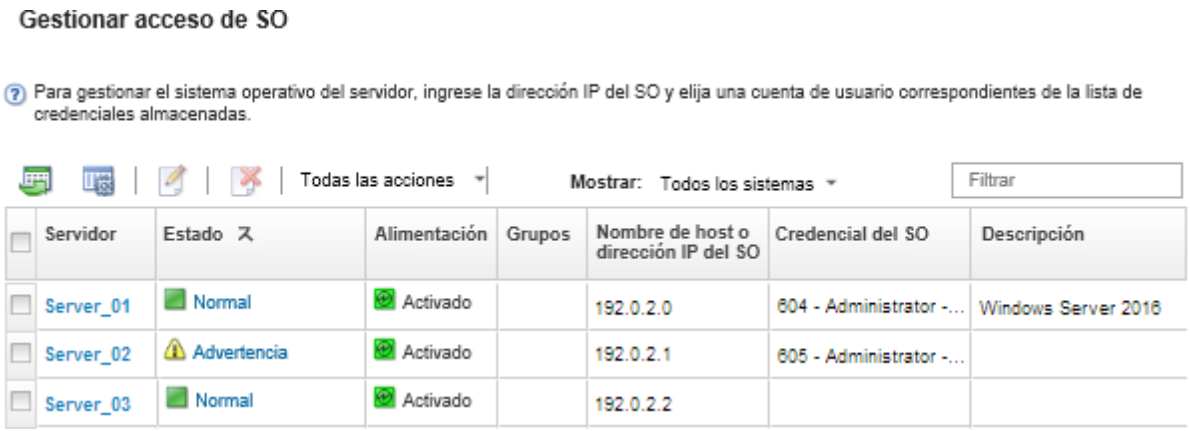
Consejo: XClarity Administrator no comprueba automáticamente la información que especifique en esta página.

Procedimiento

Lleve a cabo los pasos siguientes para modificar las propiedades del sistema operativo.

Paso 1. En la barra de menú de XClarity Administrator, haga clic en **Aprovisionamiento → Gestionar acceso de SO** para mostrar la página Gestionar acceso de SO.

Puede ordenar las columnas de la tabla para que sea más fácil encontrar los servidores específicos. Además, puede seleccionar un tipo de sistema en la lista desplegable **Todos los sistemas** e introducir texto (como un nombre de sistema o una dirección IP) en el campo **Filtro** para filtrar mejor los servidores que se muestran.



Paso 2. Seleccione los servidores que se van a actualizar.

Paso 3. Haga clic en el icono **Editar información de SO** ( ) para mostrar el cuadro de diálogo Editar información de SO.

Paso 4. Para cada servidor de destino, especifique la siguiente información:
- Nombre de host o dirección IP del sistema operativo del host
- (Opcional) Credenciales almacenadas para acceder al sistema operativo del host
- (Opcional) Descripción del sistema operativo del host

Paso 5. Haga clic en **Guardar**.

Después de finalizar

Puede realizar las siguientes acciones para gestionar el acceso al sistema operativo.

- Para borrar la información del sistema operativo (dirección IP, credenciales y descripción), seleccione el servidor y haga clic en el icono **Borrar información del SO** ( ).
- Para probar la autenticación de los servidores de Windows, haga clic en **Aprovisionamiento → Actualizaciones de controlador de Windows: Aplicar**, seleccione el servidor de destino y luego haga clic en **Comprobar autenticación**.
- Vea la información de despliegue del sistema operativo en un servidor específico; para ello, coloque el cursor sobre el nombre del servidor.

  Nota: La información de despliegue solo está disponible para los sistemas operativos que la instancia de XClarity Administrator estaba desplegando correctamente. La información de despliegue no está disponible para los despliegues con errores y para los despliegues realizados por otros medios, incluidas otras instancias de XClarity Administrator.

Ver claves de Características bajo demanda

Puede ver una lista de claves de Características bajo demanda que están instaladas en los servidores gestionados.

Acerca de esta tarea

No se pueden adquirir, instalar ni gestionar claves de Características bajo demanda desde la interfaz web de Lenovo XClarity Administrator. Para obtener más información sobre la adquisición e instalación de claves de Características bajo demanda, consulte Características bajo demanda en la documentación en línea de XClarity Administrator.

Procedimiento

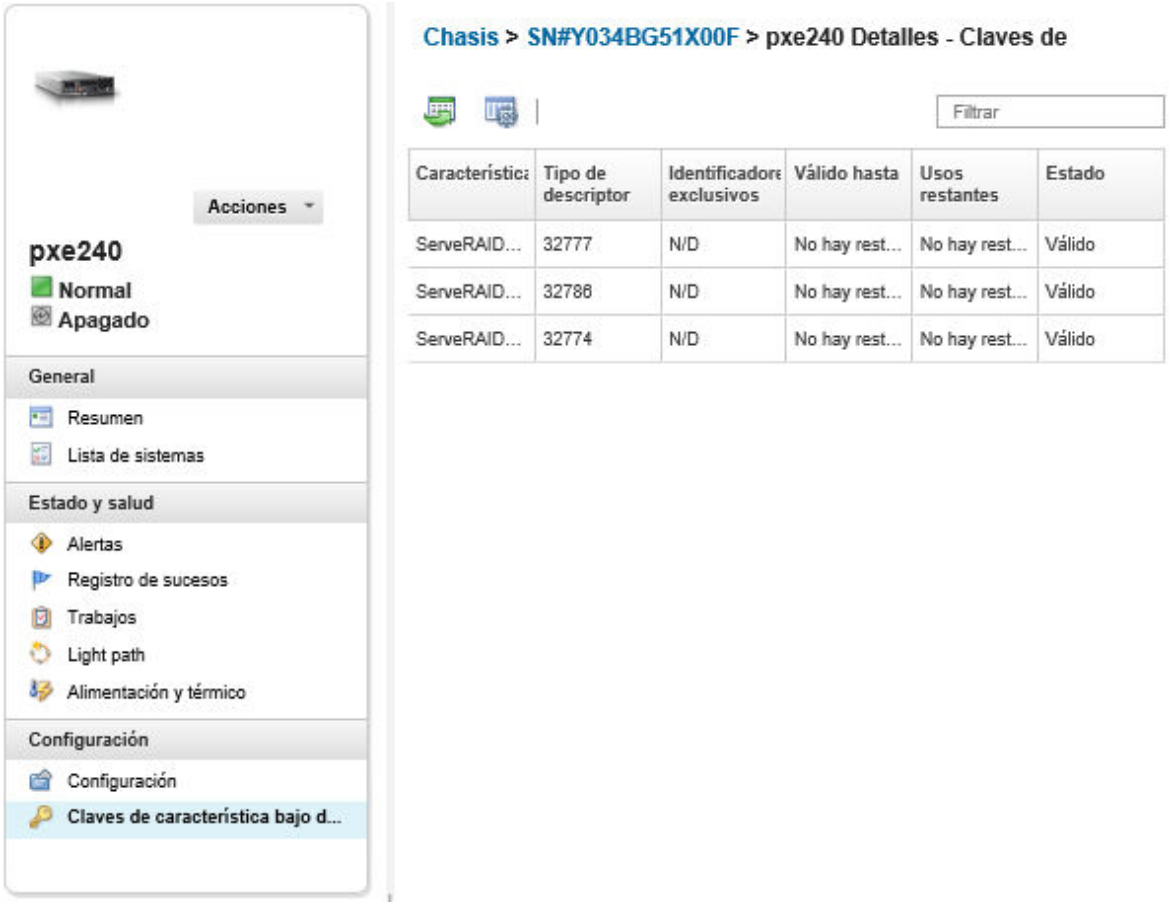
Lleve a cabo los pasos siguientes para mostrar una lista de claves de característica bajo demanda (FoD) de un servidor gestionado específico.

Paso 1. En el menú de XClarity Administrator, haga clic en **Hardware → Servidores**. Se muestra la página Servidores con una vista de tabla de todos los servidores gestionados (servidores de bastidor y de torre y nodos de cálculo).

Paso 2. Haga clic en el nombre del servidor en la columna **Servidor**. Aparece la página de resumen de estado de dicho servidor, donde se muestran las propiedades del servidor y una lista de los componentes que están instalados en él.

Paso 3. Haga clic en **Detalles del inventario** en el área General del panel de navegación izquierdo y, a continuación, expanda cada una de las secciones de componentes de hardware para ver los ID únicos de característica bajo demanda (FoD) relativos a dichos componentes.

Paso 4. Pulse **Claves de Características bajo demanda** en el área Configuración del panel de navegación izquierdo para ver información acerca de todas las claves de característica bajo demanda (FoD) que están instaladas en el servidor.



Gestión de la alimentación y la temperatura

Puede supervisar y gestionar el consumo de alimentación y la temperatura de servidores convergidos, NeXtScale, System x y ThinkServer y mejorar la eficiencia energética mediante Lenovo XClarity Energy Manager.

Más información: Lenovo XClarity Energy Manager

Acerca de esta tarea

XClarity Administrator es una interfaz de usuario independiente que puede usar para supervisar y gestionar el consumo de alimentación y la temperatura de los servidores admitidos, incluido:

- Supervisión del consumo de energía, al calcular la demanda de alimentación y la reasignación de energía a los servidores, según sea necesario.
- Supervisión de la temperatura y la capacidad de enfriamiento de los servidores.
- Enviar notificaciones cuando ocurran ciertos sucesos o cuando se superen los límites.
- Limitar la cantidad de energía que consume un dispositivo, mediante el uso de políticas.
- Optimizar la eficiencia energética al supervisar las temperaturas de entrada en tiempo real e identificar servidores de bajo uso a partir de datos de alimentación fuera de banda, al medir rangos de energía para diferentes modelos de servidores y al evaluar cómo los servidores organizan nuevas cargas de trabajo a partir de la disponibilidad de los recursos.
- Reducir el consumo de alimentación a un nivel mínimo para prolongar el tiempo de servicio durante un suceso de alimentación de emergencia (como una falla de alimentación de un centro de datos).

Para obtener más información acerca de cómo descargar, instalar y usar XClarity Administrator, consulte Sitio web de Lenovo XClarity Energy Manager.

Encendido y apagado de un servidor

Puede encender y apagar un servidor desde Lenovo XClarity Administrator.

Antes de empezar

- Para Red Hat® Enterprise Linux (RHEL) versión 7 y posterior, el reiniciar el sistema operativo desde un modo gráfico suspende el servidor de forma predeterminada. Antes de poder llevar a cabo las acciones **Reiniciar normalmente** o **Reiniciar inmediatamente** desde Lenovo XClarity Administrator, debe configurar manualmente el sistema operativo para cambiar el comportamiento del botón de encendido/apagado a apagado. Para obtener instrucciones, consulte Guía de migración de datos y de administración de Red Hat: cambiar el comportamiento al presionar el botón de encendido en modo de destino gráfico.
- En el sistema operativo SUSE Linux Enterprise Server (SLES), el apagado requiere que ingrese la contraseña de usuario root en la sesión de SLES. Antes de poder realizar las acciones **Apagar normalmente** y **Apagar inmediatamente** desde XClarity Administrator, debe apagar manualmente el servidor mediante la interfaz de SLES y seleccionar la opción **Recordar la autenticación** cuando ingrese la contraseña o revisar su política de seguridad para ver si se puede deshabilitar la autenticación obligatoria.
- Cuando está habilitada, la opción de arranque de Wake on LAN puede interferir con las operaciones de XClarity Administrator que apaga el servidor, incluyendo las actualizaciones de firmware si hay un cliente Wake on LAN en su red que emita comandos “Wake on Magic Packet”.
- La acción de alimentación **Reiniciar a configuración del sistema** reinicia el servidor y después inicia el programa de utilidad de inicio de BIOS/UEFI en una sesión a control remoto, en vez de un arranque normal del sistema operativo.
- Las acciones de alimentación **Apagar normalmente** y **Apagar inmediatamente** dependen de las configuraciones del sistema operativo instalado en el dispositivo y solo funcionan si el sistema operativo está configurado para admitirlas.
- Puede reiniciar el dispositivo con interrupción no enmascarable (NMI) al hacer clic en **Todas las acciones → Servicio → Activar NMI**.

Procedimiento

Lleve a cabo el procedimiento siguiente para encender o apagar un servidor.

Paso 1. En el menú de XClarity Administrator, haga clic en **Hardware → Servidores**. Se muestra la página Servidores con una vista de tabla de todos los servidores gestionados (servidores de bastidor y nodos de cálculo).

Paso 2. Seleccione el servidor.

Paso 3. Haga clic en **Todas las acciones → Acciones de alimentación** y, a continuación, haga clic en una de las siguientes acciones de alimentación:
- **Encender** enciente el dispositivo.
- **Apagar normalmente** apaga el sistema operativo y el dispositivo.
- **Apagar inmediatamente** apaga el dispositivo.
- **Reiniciar normalmente** apaga el sistema operativo y reinicia el dispositivo.
- **Reiniciar inmediatamente** reinicia el dispositivo
- **Reiniciar a la configuración del sistema** reinicia el dispositivo a la configuración BIOS/UEFI (F1). Esto se admite en servidores no ThinkServer compatibles sin limitaciones.
- **Reiniciar el controlador de gestión** reinicia el BMC.

- **Reiniciar inmediatamente e intentar un arranque de red PXE** reinicia el servidor inmediatamente e inicia el servidor a la red de Entorno de ejecución de prearranque (PXE). Esto se admite para Lenovo Flex System, System x y servidores ThinkSystem.

  Nota: Los valores UEFI relacionados con el arranque PXE se deben configurar en el servidor.

Reubicar virtualmente un servidor en un chasis de almacenamiento de Flex System

Puede simular la extracción y reinserción de un servidor en un chasis de Flex System reiniciando el servidor mediante una interrupción no enmascarable (NMI).

Acerca de esta tarea

Durante la reubicación virtual, se pierden todas las conexiones de red al servidor existentes y el estado de potencia de los cambios del servidor. Antes de realizar una reubicación virtual, asegúrese de que ha guardado todos los datos de los usuarios.

Atención:

- No lleve a cabo una reubicación virtual a menos que se lo indique Lenovo Soporte.
- Llevar a cabo una reubicación virtual puede dar como resultado la pérdida de los datos. Antes de reubicar el servidor, realice las operaciones necesarias para proteger los datos de los usuarios.
- En vez de llevar a cabo una reubicación virtual, considere la posibilidad de apagar el servidor. Para obtener información sobre las acciones de la alimentación, consulte Encendido y apagado de un servidor.

Procedimiento

Lleve a cabo los pasos siguientes para reubicar virtualmente un servidor en un chasis de Flex System.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Hardware → Servidores**. Se muestra la página Servidores con una vista de tabla de todos los servidores gestionados.

Puede ordenar las columnas de la tabla para que sea más fácil encontrar el servidor que desea reubicar. Además, puede seleccionar un tipo de dispositivo en la lista desplegable **Todos los dispositivos** e introducir texto (como un nombre o una dirección IP) en el campo **Filtro** para filtrar mejor los servidores que se muestran.

Paso 2. Seleccione el servidor en la tabla.

Paso 3. Pulse **Todas las acciones → Servicio → Reubicación virtual**.

Paso 4. Haga clic en **Reubicación virtual**.

Inicio de la interfaz del controlador de gestión para un servidor

Puede iniciar la interfaz web del controlador de gestión para un servidor específico desde Lenovo XClarity Administrator.

Antes de empezar

Para acceder a los servidores ThinkSystem SR635 SR655 a través de XClarity Administrator, un usuario debe tener autoridad de **lxc-supervisor**, **lxc-sysmgr**, **lxc-admin**, **lxc-fw-admin** o **lxc-os-admin** (consulte Gestión del servidor de autenticación).

Al usar el inicio de sesión único, puede iniciar la interfaz de gestión para servidores gestionados desde XClarity Administrator sin iniciar sesión. El inicio de sesión único es compatible con los servidores ThinkSystem y ThinkAgile (excepto SR635 y SR655). Los servidores ThinkSystem SR645 y SR665 requieren el firmware XCC 21A o posterior.

Para iniciar sesión directamente en el controlador de gestión mediante cuentas de usuario LDAP locales o externas sin iniciar sesión en el XClarity Administrator, utilice la URL `https://{XCC_IP_adderss}/#/login`.

Procedimiento

Lleve a cabo los pasos siguientes para iniciar la interfaz del controlador de gestión de un servidor.

Nota: No se admite el inicio de ninguna interfaz del controlador de gestión desde Lenovo XClarity Administrator mediante el navegador web Safari.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Hardware → Servidores** para mostrar la página Servidores.

Puede ordenar las columnas de la tabla para que sea más fácil encontrar servidores específicos. Además, puede seleccionar un tipo de sistema en la lista desplegable **Todos los sistemas** e introducir texto (como un nombre o una dirección IP) en el campo **Filtro** para filtrar mejor los servidores que se muestran.

Paso 2. Haga clic en el enlace relativo al servidor en la columna **Servidor**. Se muestra la página de resumen de estado de ese servidor.

Paso 3. Haga clic en **Todas las acciones → Iniciar → Interfaz web de gestión**. Se inicia la interfaz web del controlador de gestión del servidor.

Consejo: también puede hacer clic en la dirección IP en la columna **Direcciones IP** para iniciar la interfaz del controlador de gestión.

Paso 4. Inicie sesión en la interfaz del controlador de gestión utilizando sus credenciales de usuario de XClarity Administrator.

Después de finalizar

Para obtener más información acerca del uso de la interfaz del controlador de gestión para un servidor, consulte Documentación en línea de Integrated Management Module II y Documentación en línea de XClarity Controller.

Modificación de las propiedades del sistema de un servidor

Puede modificar las propiedades del sistema de un servidor específico.

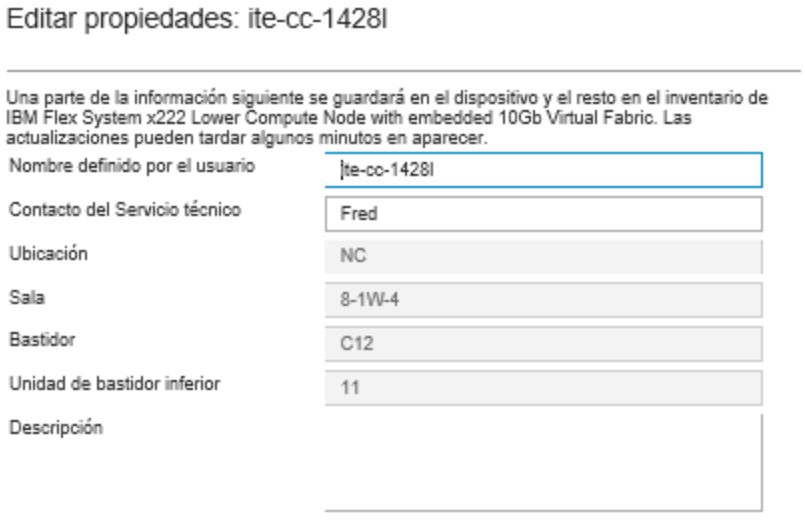
Procedimiento

Lleve a cabo los pasos siguientes para modificar las propiedades del sistema.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Hardware → Servidores** para mostrar la página Servidores.

Paso 2. Seleccione el servidor que se va a actualizar.

Paso 3. Haga clic en **Todas las acciones → Inventario → Editar propiedades**para mostrar el cuadro de diálogo Editar.



Paso 4. Cambie la siguiente información según sea necesario.
- Nombre definido por el usuario para el servidor
- Contacto de soporte
- Descripción

Nota: Las propiedades de ubicación, sala, bastidor y unidad de bastidor más baja se actualizan mediante XClarity Administrator cuando se agregan o quitan dispositivos de un bastidor en la interfaz web (consulte Gestión de bastidores).

Paso 5. Haga clic en **Guardar**.

Nota: Al cambiar estas propiedades, pueden transcurrir unos instantes antes de que los cambios aparezcan en la interfaz web de XClarity Administrator.

Resolución de credenciales almacenadas caducadas o no válidas para un servidor

Cuando una credencial almacenada caduca o deja de funcionar en un dispositivo, el estado de ese dispositivo pasa a ser “Fuera de línea.”

Procedimiento

Para resolver credenciales almacenadas caducadas o no válidas para un servidor.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Hardware → Servidores**. Se muestra la página Servidores con una vista de tabla de todos los servidores gestionados (servidores de bastidor y nodos de cálculo).

Paso 2. Haga clic en el encabezado de la columna **Alimentación** de la tabla para agrupar todos los servidores fuera de línea en la parte superior de la tabla.

Además, puede seleccionar un tipo de sistema en la lista desplegable Todos los sistemas e introducir texto (como un nombre de sistema o una dirección IP) en el campo **Filtro** para filtrar mejor los servidores que se muestran.

Paso 3. Seleccione el servidor que se va a resolver.

Paso 4. Haga clic en **Todas las acciones → Seguridad → Edtiar las credenciales almacenadas**.

Paso 5. Cambie la contraseña de la credencial almacenada o seleccione otra credencial almacenada a utilizar en el dispositivo gestionado.

Nota: Si gestionó más de un dispositivo utilizando las mismas credenciales almacenadas y cambiar la contraseña de las credenciales almacenadas, la cambiar la contraseña afecta a todos los dispositivos que estén utilizando las credenciales almacenadas.

Recuperación de un servidor con error tras el despliegue de un patrón de servidor

Si un servidor falla después de haber desplegado un patrón de servidor, puede recuperar el servidor eliminando la asignación de perfil del servidor con error y reasignando dicho perfil a un servidor en espera.

Procedimiento

Lleve a cabo los pasos siguientes para recuperar el servidor que presenta problemas que utiliza autenticación gestionada de Lenovo XClarity Administrator.

Paso 1. Identifique el servidor con error.

Paso 2. Elimine la asignación de perfil de servidor del servidor con error (consulte Desactivación de un perfil de servidor).

Atención: El servidor con error debe estar apagado para desactivar las direcciones virtuales asignadas *antes de* reasignar el perfil. Al eliminar la asignación de perfil de servidor, seleccione **Apagar servidor** en el cuadro de diálogo Eliminar asignación de perfil de servidor para apagar el servidor con error (consulte Encendido y apagado de un servidor).

Paso 3. Asigne el perfil de servidor a un servidor en espera (consulte Activación de un perfil de servidor).

Paso 4. Active el perfil encendiendo el servidor en espera si está actualmente apagado o reiniciándolo si está actualmente encendido (consulte Encendido y apagado de un servidor).

Paso 5. Migre los valores de la VLAN de los conmutadores conectados al servidor en espera.

Paso 6. Asegúrese de que el servidor con error esté apagado.

Paso 7. Sustituya o repare el servidor con error. Si repara el servidor, lleve a cabo los pasos siguientes para asegurarse de que el servidor recién reparado se ha restablecido a los valores predeterminados.

a. Restablezca el BMC a los valores de fábrica utilizando la interfaz web de gestión del servidor. Para obtener más información acerca del restablecimiento del BMC, consulte Recuperación de gestión de servidores ThinkSystem, Converged, NeXtScale o System x M5 o M6 tras un error de servidor de gestión mediante el restablecimiento del controlador de gestión.

b. Borre la información de Unified Extensible Firmware Interface (UEFI), incluida cualquier dirección virtual de adaptadores de E/S utilizando los menús de UEFI. Para obtener información, consulte la documentación de UEFI.

Recuperación de los valores de arranque tras el despliegue de patrones de servidor

Si uno o más servidores no se inician después de haber desplegado un nuevo patrón de servidor en ellos, el problema se puede deber a que los valores de arranque se hayan sobrescrito con los valores de arranque predeterminados que están en el patrón de servidor. Si se restauran los valores predeterminados en un sistema operativo instalado en modalidad UEFI, podrían requerirse pasos de configuración adicionales para restaurar la configuración de arranque.

Procedimiento

Lleve a cabo el siguiente procedimiento de recuperación manual para cada servidor afectado con el fin de restablecer los valores de arranque originales.

- Para un servidor con Red Hat Enterprise Linux instalado:
  1. Si accede remotamente al servidor, establezca una sesión de control remoto en el servidor (consulte Utilizar un control remoto para gestionar servidores convergidos, Flex System, NeXtScale y System x).
  2. Reinicie el servidor haciendo clic en **Herramientas → Alimentación → Activada**. Cuando se muestre la pantalla de inicio de UEFI para el servidor en la sesión de control remoto, presione F1 y se mostrará Setup Utility.
  3. Seleccione **Boot Manager**.
  4. Seleccione **Add Boot Option**.
  5. Seleccione **UEFI Full Path Option**.

6. En la lista que se muestra, seleccione la entrada que incluye SAS.
7. Seleccione **EFI**.
8. Seleccione **redhat**.
9. Seleccione **grub.efi**.
10. Seleccione el campo **Input the Description**.
11. Escriba Red Hat Enterprise Linux.
12. Seleccione **Commit Changes**.
13. Haga que Red Hat Enterprise Linux sea la primera opción del orden de arranque y quite el resto de las opciones.
14. Presione la tecla Escape; a continuación, seleccione **Save changes then exit this menu**.
15. Presione la tecla Escape; a continuación, seleccione **Exit the Configuration Utility and Reboot**. Se reinicia el nodo de cálculo.

- Para un servidor con Microsoft Windows Server 2008 instalado:
  1. Encienda el servidor y cuando se le pida, presione F1 para introducir la configuración.
  2. Seleccione **Boot Manager**.
  3. Seleccione **Boot from File**.
  4. Seleccione la partición del sistema Tabla de partición GUID (GPT) donde está instalado Microsoft Windows Server 2008.
  5. Seleccione **EFI**.
  6. Seleccione **Microsoft**.
  7. Seleccione **Boot**.
  8. Seleccione **bootmgfw.EFI**.

  Nota: Para obtener más información, consulte el apartado Sugerencia RETAIN 5079636.

Recuperación de la gestión de un servidor de bastidor o de torre tras un error de servidor de gestión

Si un servidor de bastidor o de torre se está gestionando mediante Lenovo XClarity Administrator y XClarity Administrator produce un error, puede restaurar las funciones de gestión hasta que XClarity Administrator se restaure o sustituya.

Acerca de esta tarea

Para recuperar la gestión de un servidor Flex System, consulte Recuperación de la gestión con un CMM tras un error de servidor de gestión.

Recuperación de la gestión de un servidor de bastidor o de torre tras un error de servidor de gestión mediante la opción Forzar gestión

Puede recuperar la gestión del servidor volviendo a gestionar el servidor utilizando la opción Forzar gestión.

Procedimiento

Si la instancia de sustitución de Lenovo XClarity Administrator utiliza la misma dirección IP que la instancia de XClarity Administrator que ha producido el error, vuelva a gestionar el dispositivo utilizando la cuenta y la contraseña de RECOVERY_ID y la opción **Forzar gestión** (consulte el Gestión de servidores).

Recuperación de un servidor System x o NeXtScale M4 en el que la gestión no se ha anulado correctamente utilizando el controlador de gestión

Puede recuperar la gestión de un servidor System x o NeXtScale M4 utilizando el controlador de gestión de la placa base (BMC).

Procedimiento

Lleve a cabo los pasos siguientes para recuperar la gestión del servidor para un servidor que utiliza autenticación gestionada de Lenovo XClarity Administrator.

Paso 1. Inicie sesión en la interfaz web del controlador de gestión mediante la cuenta y la contraseña del usuario que creó antes de gestionar el servidor de bastidor mediante XClarity Administrator.

Paso 2. Borrar los valores de la interrupción SNMP.

a. Haga clic en **Gestión de IMM → Red**.

b. Haga clic en la pestaña **SNMP**.

c. Haga clic en la pestaña **Comunidades**.

d. Ubique la entrada de la comunidad para el anterior XClarity Administrator, por ejemplo.
- **Dirección IP de LXCA:** 10.240.198.84
- **Host de LXCA:** LXCA_maqCBIt86d
- **Comunidad 2:**
- **Nombre de comunidad:** LXCA_maqCBIt86d
- **Tipo de acceso:** Interrupción
- **Permitir que hosts específicos reciban interrupciones en esta comunidad:** 10.240.198.84

e. Quite el valor en los campos para la entrada de la comunidad.

f. Haga clic en **Aplicar**.

Paso 3. Borre las cuentas de usuario.

a. Haga clic en **Gestión de IMM → Usuarios**.

b. Haga clic en la pestaña **Cuentas de usuario**.

c. Elimine todas las cuentas de usuario que sean XClarity Administrator, incluyendo las cuentas de usuario con los siguientes prefijos:
- DISABLE_*
- LXCA_*
- OBSOLETE_*
- SNMPCFGUSER

Después de finalizar

Una vez que XClarity Administrator se haya recuperado o sustituido, puede volver a gestionar el servidor System x o NeXtScale (consulte el Gestión de servidores). Se conserva toda la información sobre el servidor (como los valores de red, las políticas de servidor y las políticas de cumplimiento de firmware).

Recuperación de gestión de servidores ThinkSystem, Converged, NeXtScale o System x M5 o M6 tras un error de servidor de gestión mediante el restablecimiento del controlador de gestión

Puede recuperar la gestión de un servidor Converged, ThinkSystem, NeXtScale o System x M5 o M6, restableciendo el controlador de gestión de la placa base en el servidor a los valores predeterminados de fábrica.

Procedimiento

Lleve a cabo los pasos siguientes para recuperar la gestión del servidor para un servidor que utiliza autenticación gestionada de Lenovo XClarity Administrator.

Paso 1. Si la Encapsulación está habilitada en el dispositivo, conéctese al controlador de gestión de destino desde un sistema que esté configurado para utilizar la dirección IP del dispositivo virtual de XClarity Administrator que presenta el error.

Paso 2. Restablezca el controlador de gestión a los valores predeterminados de fábrica.

a. Inicie sesión en la interfaz web del controlador de gestión del servidor mediante la cuenta y contraseña del usuario de recuperación que creó antes de gestionar el servidor de bastidor mediante XClarity Administrator.

b. Haga clic en la pestaña **Gestión de IMM**.

c. Haga clic en **Restablecer IMM a los valores de fábrica**.

d. Haga clic en **Aceptar** para confirmar la acción de restablecimiento.

Importante: Una vez completada la configuración del BMC, este se reinicia. Si se trata de un servidor local, su conexión TCP/IP se interrumpe y debe volver a configurar la interfaz de red para restaurar la conectividad.

Paso 3. Se inicia nuevamente la sesión en la interfaz web del controlador de gestión del servidor.

- El BMC se configura inicialmente para intentar obtener una dirección IP desde un servidor DHCP. Si esto no es posible, utiliza la dirección IPv4 estática `192.168.70.125`.
- El IMMBMC se configura inicialmente con un nombre de usuario de `USERID` y una contraseña de `PASSWORD` (con un cero). Esta cuenta de usuario predeterminada tiene acceso de supervisor. Con el fin de obtener una seguridad ampliada, cambie este nombre de usuario y esta contraseña durante la configuración inicial.

Paso 4. Vuelva a configurar la interfaz de red para restaurar la conectividad. Para obtener más información, consulte el Documentación en línea de Integrated Management Module II

Después de finalizar

Una vez que XClarity Administrator se haya restaurado o sustituido, puede volver a gestionar el servidor (consulte el Gestión de servidores). Se conserva toda la información sobre el servidor (como los valores de red, las políticas de servidor y las políticas de cumplimiento de firmware).

Si el servidor se configuró utilizando Patrones de configuración, puede desactivar y, a continuación, volver a activar el perfil de servidor que se asignó al servidor para aplicar la configuración (consulte Trabajo con perfiles de servidor).

Recuperación de la gestión de servidores ThinkSystem, Converged, NeXtScale o System x M5 o M6 tras un error de servidor de gestión mediante el uso de cimcli

Puede recuperar la gestión de un servidor ThinkSystem, Converged, NeXtScale o System x M5 o M6, utilizando la herramienta `cimcli` para borrar las suscripciones CIM.

Antes de empezar

OpenPegasus con la herramienta cimcli debe instalarse en un sistema que tenga acceso de red al servidor de destino. Para obtener información acerca de cómo descargar, configurar y compilar OpenPegasus, consulte Sitio web de versiones de Openpegasus para Linux.

Nota: Para servidor 7 y posterior de Red Hat Enterprise Linux (RHEL), se incluyen RPM de origen y binarios de OpenPegasus como parte de la distribución de Red Hat. El paquete `top-pegasus-test.x86_64` incluye la herramienta cimcli.

Acerca de esta tarea

Una vez que el servidor se haya recuperado, puede volver a gestionar el servidor. Se conserva toda la información sobre el servidor (como los valores de red, las políticas de servidor y las políticas de cumplimiento de firmware).

Procedimiento

Lleve a cabo los pasos siguientes desde un servidor que use autenticación gestionada de Lenovo XClarity Administrator en el que se haya instalado OpenPegasus para recuperar la gestión del servidor.

Paso 1. Si la Encapsulación está habilitada en el dispositivo:

a. Conéctese al servidor de destino desde un sistema que esté configurado para usar la dirección IP del dispositivo virtual de XClarity Administrator que presenta el error.

b. Deshabilite la Encapsulación abriendo una sesión SSH en el dispositivo y ejecutando el siguiente comando:
```
encaps lite off
```

Paso 2. Ejecute los siguientes comandos para determinar las instancias CIM para CIM_ListenerDestinationCIMXML, CIM_Indicationfilter y CIM_IndicationSubscription.
```
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s ni CIM_ListenerDestinationCIMXML
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s ni CIM_Indicationfilter
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s ni CIM_IndicationSubscription
```

donde <*IP_address*>, <*user_ID*> y <*password*> son la dirección IP, el Id. de usuario y la contraseña del controlador de gestión. Por ejemplo:

```
$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop
-s ni CIM_ListenerDestinationCIMXML
CIM_ListenerDestinationCIMXML.creationclassname="CIM_ListenerDestinationCIMXML",
name="Lenovo:LXCA_10.243.5.191:Handler",
systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop s ni CIM_Indicationfilter
CIM_Indicationfilter.creationclassname="CIM_IndicationFilter",
name="Lenovo:LXCA_10.243.5.191:Filter",systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop
s ni CIM_IndicationSubscription
CIM_IndicationSubscription.filter="root/interop:cim_indicationfilter.creationclassname=
\"CIM_IndicationFilter\",name=\"Lenovo:LXCA_10.243.5.191:Filter\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\"",
handler="root/interop:cim_listenerdestinationcimxml.creationclassname=
\"CIM_ListenerDestinationCIMXML\",name=\"Lenovo:LXCA_10.243.5.191:Handler\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\""
```

Paso 3. Ejecute el siguiente comando para eliminar cada una de las instancias CIM para CIM_ListenerDestinationCIMXML, CIM_Indicationfilter y CIM_IndicationSubscription, una a una.

```
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s di '<cim_instance>'
```

donde <*IP_address*>, <*user_ID*> y <*password*> son la dirección IP, el Id. de usuario y la contraseña del controlador de gestión, mientras que <*cim_instance*> es la información devuelta para cada instancia CIM en el paso anterior, que se muestra entre comillas simples. Por ejemplo:

```
$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_ListenerDestinationCIMXML.creationclassname="CIM_ListenerDestinationCIMXML",
name="Lenovo:LXCA_10.243.5.191:Handler",systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"'

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_Indicationfilter.creationclassname="CIM_IndicationFilter",
name="Lenovo:LXCA_10.243.5.191:Filter",
systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"'

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_IndicationSubscription.filter="root/interop:cim_indicationfilter.creationclassname=
\"CIM_IndicationFilter\",name=\"Lenovo:LXCA_10.243.5.191:Filter\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\"",
handler="root/interop:cim_listenerdestinationcimxml.creationclassname=
\"CIM_ListenerDestinationCIMXML\",name=\"Lenovo:LXCA_10.243.5.191:Handler\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\""'
```

Después de finalizar

Una vez que Lenovo XClarity Administrator se haya recuperado o sustituido, puede volver a gestionar el servidor System x o NeXtScale (consulte el Gestión de servidores). Se conserva toda la información sobre el servidor (como los valores de red, las políticas de servidor y las políticas de cumplimiento de firmware).

Recuperación de la gestión de servidor del servidor de ThinkServer tras un error en el servidor de gestión mediante la interfaz del controlador de gestión

Puede recuperar la gestión de un servidor ThinkServer a partir de la interfaz del controlador de gestión.

Procedimiento

Lleve a cabo los pasos siguientes para recuperar la gestión del servidor.

Paso 1. Se inicia la sesión en la interfaz web del controlador de gestión del servidor como administrador (consulte Inicio de la interfaz del controlador de gestión para un servidor).

Paso 2. Elimine las cuentas de IPMI creadas por Lenovo XClarity Administrator al seleccionar Usuarios en el menú principal y luego eliminando todas las cuentas de usuarios con el prefijo “LXCA_”.

De manera alternativa, puede cambiar el nombre de usuario de la cuenta y eliminar el prefijo “LXCA_”.

Paso 3. Elimine los destinos de trampas SNMP al seleccionar **Gestión de PEF** en el menú principal, luego haga clic en la pestaña **Destino de LAN** y elimine la entrada que apunta hacia la dirección IP de la instancia XClarity Administrator.

Paso 4. Compruebe que tiene una configuración de NTP válida al seleccionar **Configuración de NTP** en el menú principal y luego configure la fecha y hora manualmente o proporcione una dirección de servidor NTP válida.

Anulación de la gestión de un servidor de bastidor o de torre

Puede quitar un servidor de bastidor o de torre de la gestión mediante Lenovo XClarity Administrator. Este proceso se denomina *anular la gestión* (no gestionar).

Antes de empezar

Puede habilitar XClarity Administrator para que se anule automáticamente la gestión de los dispositivos que están fuera de línea durante un período de tiempo específico. Esto está deshabilitado de forma predeterminada. Para habilitar la anulación automática de gestión de dispositivos fuera de línea, haga clic en **Hardware → Detectar y gestionar dispositivos nuevos** en el menú de XClarity Administrator y, a continuación, haga clic en **Editar**, ubicado junto a la opción **No gestionar los dispositivos fuera de línea está Deshabilitado**. A continuación, seleccione **Habilitar dispositivos no gestionados fuera de línea** y establezca el intervalo de tiempo. De manera predeterminada, se anula la gestión de los dispositivos después de estar fuera de línea durante 24 horas.

Antes de anular la gestión de un servidor de torre o bastidor, asegúrese de que no hay trabajos activos en ejecución en el servidor.

Si desea quitar el patrón de servidor y todas las direcciones virtuales del servidor de bastidor o de torre, desactive el perfil de servidor antes de anular la gestión del servidor (consulte Desactivación de un perfil de servidor).

Si la opción Llamar a casa está habilitada en XClarity Administrator, Llamar a casa se deshabilita en todos los chasis y servidores gestionados para evitar que se produzca una duplicación de los registros de problemas. Si tiene intención dejar de utilizar XClarity Administrator para gestionar sus dispositivos, puede volver a habilitar la función Llamar a casa en todos los dispositivos gestionados desde XClarity Administrator, en lugar de volver a habilitar Llamar a casa posteriormente para cada dispositivo individual (consulte Nueva habilitación de Llamar a casa en todos los dispositivos gestionados en la documentación en línea de XClarity Administrator).

Acerca de esta tarea

Cuando se elimina la gestión de un servidor de bastidor o de torre, Lenovo XClarity Administrator realiza las siguientes acciones:

- Borra la configuración que se utiliza para la gestión de usuarios centralizada.
- Quita el certificado de seguridad del controlador de gestión de la placa base desde el almacén de confianza de XClarity Administrator.
- Si la Encapsulación está habilitada en el dispositivo, configura las reglas de firewall de los dispositivos con los valores que tenía el dispositivo antes de que se gestionara.
- Elimina las suscripciones CIM a la configuración de XClarity Administrator, de modo que XClarity Administrator ya no recibe sucesos del servidor de bastidor o de torre.
- Deshabilita la opción Llamar a casa en el servidor de bastidor o de torre si Llamar a casa está habilitada en la actualidad en XClarity Administrator.
- Descarta sucesos que se han enviado desde el servidor de bastidor o de torre. Puede conservar dichos sucesos reenviándolos a un repositorio externo, como Syslog (consulte Reenvío de sucesos).

Cuando se anula la gestión de un servidor de bastidor o de torre, XClarity Administrator conserva determinada información sobre el servidor. Esta información se vuelve a aplicar cuando se gestiona de nuevo el mismo servidor de bastidor o de torre.

Importante: Si anula la gestión de un servidor ThinkServer y luego lo gestiona mediante otra instancia de XClarity Administrator, se pierde la información sobre el servidor.

Consejo: todos los dispositivos de demostración que se añaden opcionalmente durante la configuración inicial son nodos en un chasis. Para anular la gestión de los dispositivos de demostración, anule la gestión del chasis utilizando la opción **Forzar anulación de gestión incluso si no se puede acceder al dispositivo**.

Procedimiento

Lleve a cabo los pasos siguientes para anular la gestión de un servidor de bastidor o de torre.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Hardware → Servidores** para mostrar la página Servidores.

Paso 2. Seleccione uno o más servidores de bastidor o de torre para eliminar la gestión.

Paso 3. Haga clic en **No gestionar**. Se muestra el cuadro de diálogo No gestionar.

Paso 4. **Opcional:** seleccione **Forzar anulación de gestión aunque el dispositivo no esté accesible**.

Importante: Asegúrese de seleccionar esta opción si está anulando la gestión de un hardware de demostración.

Paso 5. Haga clic en **No gestionar**.El cuadro de diálogo No gestionar muestra el progreso de cada paso en el proceso de anulación de la gestión.

Paso 6. Cuando el proceso de anulación de la gestión esté completo, pulse **Aceptar**.

Recuperación de un servidor de bastidor o de torre en el que la gestión no se ha anulado correctamente

Si la gestión de un servidor convergido, NeXtScale, System x o ThinkServer no se ha anulado correctamente, debe recuperar el servidor antes de poder gestionarlo de nuevo.

Recuperación de un servidor de bastidor o de torre en el que la gestión no se ha anulado correctamente mediante la opción Forzar gestión

Puede recuperar la gestión del servidor volviendo a gestionar el servidor utilizando la opción Forzar gestión.

Procedimiento

Si la instancia de sustitución de Lenovo XClarity Administrator utiliza la misma dirección IP que la instancia de XClarity Administrator que ha producido el error, vuelva a gestionar el dispositivo utilizando la cuenta y la contraseña de `RECOVERY_ID` y la opción **Forzar gestión** (consulte el Gestión de servidores).

Recuperación de un servidor System x o NeXtScale M4 en el que la gestión no se ha anulado correctamente utilizando el controlador de gestión

Puede recuperar la gestión de un servidor System x o NeXtScale M4 utilizando el controlador de gestión.

Procedimiento

Lleve a cabo los pasos siguientes para recuperar la gestión del servidor.

Paso 1. Inicie sesión en la interfaz web del controlador de gestión mediante la cuenta y la contraseña del usuario que creó antes de gestionar el servidor de bastidor mediante XClarity Administrator.

Paso 2. Borrar los valores de la interrupción SNMP.

a. Haga clic en **Gestión de IMM → Red**.

b. Haga clic en la pestaña **SNMP**.

c. Haga clic en la pestaña **Comunidades**.

d. Ubique la entrada de la comunidad para el anterior XClarity Administrator, por ejemplo.
- **Dirección IP de LXCA:** 10.240.198.84
- **Host de LXCA:** LXCA_maqCBlt86d
- **Comunidad 2:**
- **Nombre de comunidad:** LXCA_maqCBlt86d
- **Tipo de acceso:** Interrupción
- **Permitir que hosts específicos reciban interrupciones en esta comunidad:** 10.240.198.84

e. Quite el valor en los campos para la entrada de la comunidad.

f. Haga clic en **Aplicar**.

Paso 3. Borre las cuentas de usuario.

a. Haga clic en **Gestión de IMM → Usuarios**.

b. Haga clic en la pestaña **Cuentas de usuario**.

c. Elimine todas las cuentas de usuario que sean XClarity Administrator, incluyendo las cuentas de usuario con los siguientes prefijos:
- DISABLE_*
- LXCA_*
- OBSOLETE_*
- SNMPCFGUSER

Paso 4. Gestione el servidor utilizando Lenovo XClarity Administrator.

a. En la barra de menús de XClarity Administrator, haga clic en **Hardware → Detectar y gestionar dispositivos nuevos**. Se muestra la página Detectar y gestionar.

b. Seleccione **Entrada manual**.

c. Haga clic en **Sistema único**, introduzca la dirección IP del servidor que desee gestionar y, a continuación, haga clic en **Aceptar**.

d. Especifique el Id. de usuario y la contraseña para su autenticación en el servidor.

e. Haga clic en **Gestionar**.

Se visualiza un cuadro de diálogo que muestra el progreso de este proceso de gestión. Supervise el progreso para asegurarse de que el proceso se completa satisfactoriamente.

f. Cuando el proceso esté completo, haga clic en **Aceptar**.

Recuperación de un servidor ThinkSystem, Converged, NeXtScale o System x M5 o M6 en el que no se ha anulado la gestión correctamente, restableciendo el controlador de gestión a los valores predeterminados de fábrica

Puede recuperar la gestión de un servidor ThinkSystem, Converged, NeXtScale o System x M5 o M6, restableciendo el controlador de gestión de la placa base (BMC) en el servidor a los valores predeterminados de fábrica.

Procedimiento

Lleve a cabo los pasos siguientes para recuperar la gestión del servidor.

Paso 1. Si la Encapsulación está habilitada en el dispositivo, conéctese al controlador de gestión de destino desde un sistema que esté configurado para utilizar la dirección IP del dispositivo virtual de XClarity Administrator que presenta el error.

Paso 2. Restablezca el controlador de gestión a los valores predeterminados de fábrica.

a. Inicie sesión en la interfaz web del controlador de gestión del servidor mediante la cuenta y contraseña del usuario de recuperación que creó antes de gestionar el servidor de bastidor mediante XClarity Administrator.

b. Haga clic en la pestaña **Gestión de IMM**.

c. Haga clic en **Restablecer IMM a los valores de fábrica**.

d. Haga clic en **Aceptar** para confirmar la acción de restablecimiento.

Importante: Una vez completada la configuración del BMC, este se reinicia. Si se trata de un servidor local, su conexión TCP/IP se interrumpe y debe volver a configurar la interfaz de red para restaurar la conectividad.

Paso 3. Se inicia nuevamente la sesión en la interfaz web del controlador de gestión del servidor.

- El BMC se configura inicialmente para intentar obtener una dirección IP desde un servidor DHCP. Si esto no es posible, utiliza la dirección IPv4 estática `192.168.70.125`.
- El IMMBMC se configura inicialmente con un nombre de usuario de `USERID` y una contraseña de `PASSWORD` (con un cero). Esta cuenta de usuario predeterminada tiene acceso de supervisor. Con el fin de obtener una seguridad ampliada, cambie este nombre de usuario y esta contraseña durante la configuración inicial.

Paso 4. Vuelva a configurar la interfaz de red para restaurar la conectividad. Para obtener más información, consulte el Documentación en línea de Integrated Management Module II

Paso 5. Gestione el servidor utilizando Lenovo XClarity Administrator.

a. En la barra de menús de XClarity Administrator, haga clic en **Hardware → Detectar y gestionar dispositivos nuevos**. Se muestra la página Detectar y gestionar.

b. Seleccione **Entrada manual**.

c. Haga clic en **Sistema único**, introduzca la dirección IP del servidor que desee gestionar y, a continuación, haga clic en **Aceptar**.

d. Especifique el Id. de usuario y la contraseña para su autenticación en el servidor.

e. Haga clic en **Gestionar**.

Se visualiza un cuadro de diálogo que muestra el progreso de este proceso de gestión. Supervise el progreso para asegurarse de que el proceso se completa satisfactoriamente.

f. Cuando el proceso esté completo, haga clic en **Aceptar**.

Paso 6. Si el servidor se ha configurado utilizando Patrones de configuración, vuelva a activar el perfil de servidor que se asignó al servidor.

a. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Perfiles de servidor**. Se muestra la página Patrones de configuración: Perfiles de servidor.

b. Seleccione el perfil de servidor y, a continuación, haga clic en el icono **Desactivar perfil de servidor** ().

c. Haga clic en **Apagar ITE** para apagar el servidor. Cuando el servidor se vuelve a encender, las asignaciones de direcciones virtuales vuelven a los valores predeterminados grabados.

d. Haga clic en **Desactivar**. El estado del perfil cambia a “Inactivo” en la columna Estado del perfil. Nota: los servidores mantienen su información de identificación (por ejemplo, el nombre de host, la dirección IP o la dirección MAC virtual) cuando se desactiva un perfil.

e. Vuelva a seleccionar el perfil de servidor y haga clic en el icono **Activar perfil de servidor** ().

f. Haga clic en **Activar** para activar los perfiles de servidor en el servidor. El estado del perfil cambia a “Activo” en la columna Estado del perfil.

Paso 7. Si se ha asignado una política de cumplimiento al servidor, vuelva a asignar la política de cumplimiento.

a. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Aplicar/Activar**. Se muestra la página Actualizaciones de firmware: Aplicar/Activar con una lista de los dispositivos gestionados.

b. Seleccione la política apropiada para el servidor en el menú desplegable de la columna **Política asignada**.

Recuperación de un servidor ThinkSystem, Converged, NeXtScale o System x M5 o M6, en el que la gestión no se ha anulado correctamente utilizando la herramienta cimcli

Puede recuperar la gestión de un servidor ThinkSystem, Converged, NeXtScale o System x, utilizando `cimcli` para borrar las suscripciones CIM.

Antes de empezar

OpenPegasus con la herramienta cimcli debe instalarse en un sistema que tenga acceso de red al servidor de destino. Para obtener información acerca de cómo descargar, configurar y compilar OpenPegasus, consulte Sitio web de versiones de Openpegasus para Linux.

Nota: Para servidor 7 y posterior de Red Hat Enterprise Linux (RHEL), se incluyen RPM de origen y binarios de OpenPegasus como parte de la distribución de Red Hat. El paquete `top-pegasus-test.x86_64` incluye la herramienta cimcli.

Acerca de esta tarea

Una vez que el servidor se haya recuperado, puede volver a gestionar el servidor. Se conserva toda la información sobre el servidor (como los valores de red, las políticas de servidor y las políticas de cumplimiento de firmware).

Procedimiento

Lleve a cabo los pasos siguientes desde un servidor que use autenticación gestionada de Lenovo XClarity Administrator en el que se haya instalado OpenPegasus para recuperar la gestión del servidor.

Paso 1. Si la Encapsulación está habilitada en el dispositivo:

a. Conéctese al servidor de destino desde un sistema que esté configurado para usar la dirección IP del dispositivo virtual de XClarity Administrator que presenta el error.

b. Deshabilite la Encapsulación abriendo una sesión SSH en el dispositivo y ejecutando el siguiente comando:

```
encaps lite off
```

Paso 2. Ejecute los siguientes comandos para determinar las instancias CIM para CIM_ListenerDestinationCIMXML, CIM_Indicationfilter y CIM_IndicationSubscription.

```
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s ni CIM_ListenerDestinationCIMXML
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s ni CIM_Indicationfilter
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s ni CIM_IndicationSubscription
```

donde <*IP_address*>, <*user_ID*> y <*password*> son la dirección IP, el Id. de usuario y la contraseña del controlador de gestión. Por ejemplo:

```
$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop
-s ni CIM_ListenerDestinationCIMXML
CIM_ListenerDestinationCIMXML.creationclassname="CIM_ListenerDestinationCIMXML",
name="Lenovo:LXCA_10.243.5.191:Handler",
systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop s ni CIM_Indicationfilter
CIM_Indicationfilter.creationclassname="CIM_IndicationFilter",
name="Lenovo:LXCA_10.243.5.191:Filter",systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop
s ni CIM_IndicationSubscription
CIM_IndicationSubscription.filter="root/interop:cim_indicationfilter.creationclassname=
\"CIM_IndicationFilter\",name=\"Lenovo:LXCA_10.243.5.191:Filter\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\"",
handler="root/interop:cim_listenerdestinationcimxml.creationclassname=
\"CIM_ListenerDestinationCIMXML\",name=\"Lenovo:LXCA_10.243.5.191:Handler\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\""
```

Paso 3. Ejecute el siguiente comando para eliminar cada una de las instancias CIM para CIM_ListenerDestinationCIMXML, CIM_Indicationfilter y CIM_IndicationSubscription, una a una.

```
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s di '<cim_instance>'
```

donde <*IP_address*>, <*user_ID*> y <*password*> son la dirección IP, el Id. de usuario y la contraseña del controlador de gestión, mientras que <*cim_instance*> es la información devuelta para cada instancia CIM en el paso anterior, que se muestra entre comillas simples. Por ejemplo:

```
$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_ListenerDestinationCIMXML.creationclassname="CIM_ListenerDestinationCIMXML",
name="Lenovo:LXCA_10.243.5.191:Handler",systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"'

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_Indicationfilter.creationclassname="CIM_IndicationFilter",
name="Lenovo:LXCA_10.243.5.191:Filter",
systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"'

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_IndicationSubscription.filter="root/interop:cim_indicationfilter.creationclassname=
\"CIM_IndicationFilter\",name=\"Lenovo:LXCA_10.243.5.191:Filter\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\"",
handler="root/interop:cim_listenerdestinationcimxml.creationclassname=
\"CIM_ListenerDestinationCIMXML\",name=\"Lenovo:LXCA_10.243.5.191:Handler\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\""'
```

Paso 4. Gestione el servidor utilizando Lenovo XClarity Administrator.

a. En la barra de menús de XClarity Administrator, haga clic en **Hardware → Detectar y gestionar dispositivos nuevos**. Se muestra la página Detectar y gestionar.

b. Seleccione **Entrada manual**.

c. Haga clic en **Sistema único**, introduzca la dirección IP del servidor que desee gestionar y, a continuación, haga clic en **Aceptar**.

d. Especifique el Id. de usuario y la contraseña para su autenticación en el servidor.

e. Haga clic en **Gestionar**.

   Se visualiza un cuadro de diálogo que muestra el progreso de este proceso de gestión. Supervise el progreso para asegurarse de que el proceso se completa satisfactoriamente.

f. Cuando el proceso esté completo, haga clic en **Aceptar**.

Recuperación de la gestión de un servidor de ThinkServer en el que la gestión no se ha anulado correctamente utilizando la interfaz del controlador de gestión

Puede recuperar la gestión de un servidor ThinkServer mediante el uso de la interfaz web del controlador de gestión.

Procedimiento

Lleve a cabo los pasos siguientes para recuperar la gestión del servidor.

Paso 1. Se inicia la sesión en la interfaz web del controlador de gestión del servidor como administrador (consulte Inicio de la interfaz del controlador de gestión para un servidor).

Paso 2. Elimine las cuentas de IPMI creadas por Lenovo XClarity Administrator al seleccionar Usuarios en el menú principal y luego eliminando todas las cuentas de usuarios con el prefijo “LXCA_”.

   De manera alternativa, puede cambiar el nombre de usuario de la cuenta y eliminar el prefijo “LXCA_”.

Paso 3. Elimine los destinos de trampas SNMP al seleccionar **Gestión de PEF** en el menú principal, luego haga clic en la pestaña **Destino de LAN** y elimine la entrada que apunta hacia la dirección IP de la instancia XClarity Administrator.

Paso 4. Compruebe que tiene una configuración de NTP válida al seleccionar **Configuración de NTP** en el menú principal y luego configure la fecha y hora manualmente o proporcione una dirección de servidor NTP válida.

Capítulo 9. Gestión de los dispositivos de almacenamiento

Lenovo XClarity Administrator puede gestionar varios tipos de dispositivos de almacenamiento, incluidos los sistemas de almacenamiento de Lenovo Storage, Flex System,y bibliotecas de cintas.

Más información:  XClarity Administrator: detección

Antes de empezar

Atención: Revise Consideraciones de gestión de almacenamiento antes de gestionar un dispositivo de almacenamiento.

Nota: Los dispositivos de almacenamiento de Flex System se detectan y gestionan automáticamente cuando gestiona el chasis que los contiene. No puede detectar ni gestionar dispositivos de almacenamiento de Flex System de forma independiente del chasis.

Algunos puertos deben estar disponibles para comunicarse con los dispositivos. Asegúrese de que todos los puertos requeridos estén disponibles antes de intentar gestionar dispositivos de almacenamiento. Para obtener más información sobre los puertos, consulte Disponibilidad de puertos en la documentación en línea de XClarity Administrator.

Asegúrese de que el firmware mínimo necesario esté instalado en cada dispositivo de almacenamiento 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: Asegúrese de que se cumplan los siguientes requisitos antes de detectar y gestionar dispositivos de almacenamiento de bastidor (que no sea ThinkSystem serie DE). Para obtener más información, consulte No se puede detectar un dispositivo y No puede gestionar un dispositivo en la documentación en línea de XClarity Administrator.

- La red de configuración debe permitir el tráfico SLP entre XClarity Administrator y el dispositivo de almacenamiento de bastidor.
- Se requiere SLP de difusión única.
- Se requiere SLP de multidifusión si desea que XClarity Administrator detecte automáticamente los dispositivos Lenovo Storage. Además, se debe habilitar SLP en el dispositivo de almacenamiento de bastidor.

Acerca de esta tarea

XClarity Administrator puede detectar automáticamente dispositivos de almacenamiento en su entorno, sondeando los dispositivos gestionables que se encuentran en la misma subred IP, como XClarity Administrator. Para detectar los dispositivos de almacenamiento que están en otras subredes, especifique una dirección IP o un rango de direcciones IP, o importe la información de una hoja de cálculo.

Una vez que XClarity Administrator gestiona los dispositivos de almacenamiento, XClarity Administrator sondea periódicamente todos los dispositivos de almacenamiento gestionados para recopilar información, como el inventario, los datos de producto fundamentales y el estado. Puede consultar y supervisar cada dispositivo de almacenamiento gestionado y realizar acciones de gestión (como configurar los valores del sistema, actualizar el firmware y encenderlo y apagarlo).

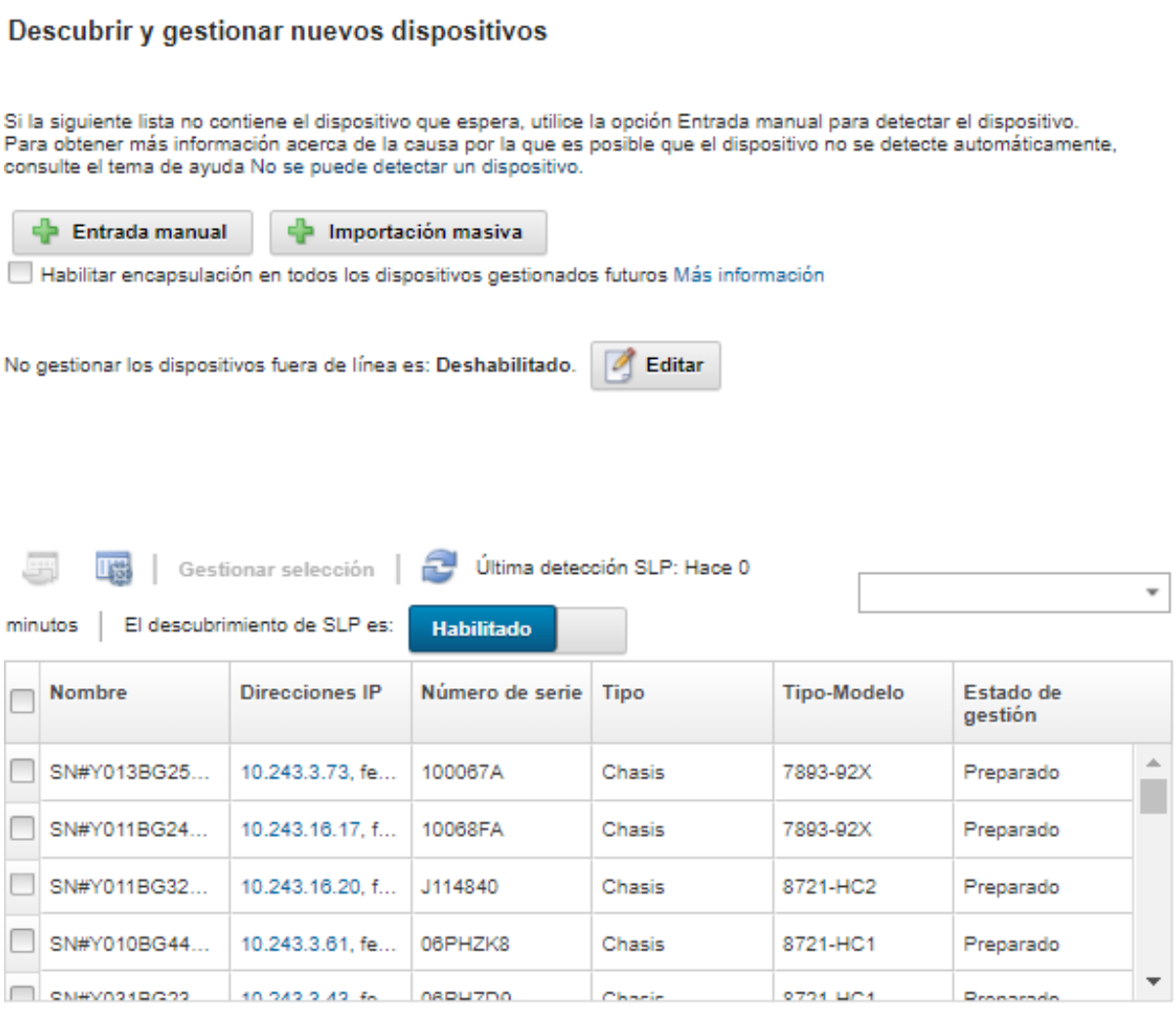
Un dispositivo solo puede estar gestionado al mismo tiempo por una instancia de XClarity Administrator. La gestión por parte de varias instancias de XClarity Administrator no es compatible. Si un dispositivo está gestionado por un XClarity Administrator y desea gestionarlo con otro XClarity Administrator, primero debe dejar de gestionar el dispositivo de almacenamiento en el XClarity Administrator inicial y luego gestionarlo con el nuevo XClarity Administrator. Si se produce un error durante el proceso de anulación de la gestión, puede seleccionar la opción **Forzar gestión** durante la gestión del nuevo XClarity Administrator.

Nota: Cuando explora la red en busca de dispositivos gestionables, XClarity Administrator no reconoce si un dispositivo ya está gestionado por otro gestionador hasta después de intentar gestionar el dispositivo.

Procedimiento

Complete uno de los siguientes procedimientos para gestionar sus dispositivos de almacenamiento mediante XClarity Administrator.

- Detecte y gestione un gran número de dispositivos de almacenamiento y otros tipos de dispositivos utilizando un archivo de importación masiva (consulte Gestión de sistemas en la documentación en línea de XClarity Administrator).
- Detecte y gestione dispositivos de almacenamiento que están en la misma subred IP que XClarity Administrator.
  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 dispositivos nuevos.



Puede ordenar las columnas de la tabla para que sea más fácil encontrar los dispositivos de almacenamiento que desea gestionar. Además, puede introducir el texto (como un nombre de sistema o una dirección IP) en el campo **Filtro** para aplicar filtros avanzados a los sistemas de almacenamiento que se visualizan. Puede cambiar las columnas que se muestran el orden predeterminado haciendo clic en el icono **Personalizar columnas** ().

2. Haga clic en el icono **Actualizar** () para descubrir todos los dispositivos gestionables en el dominio XClarity Administrator. La detección puede durar varios minutos.
3. Seleccione el sistema o los dispositivos de almacenamiento que desee gestionar.
4. Haga clic en **Gestionar selección**. Se muestra el cuadro de diálogo Gestionar.
5. Especifique el Id. de usuario y la contraseña para la autenticación del dispositivo de almacenamiento.

   Consejo: se recomienda usar una cuenta de supervisor o administrador para gestionar el dispositivo. Si se utiliza una cuenta con autoridad de nivel inferior, la gestión puede fallar, o la gestión puede finalizar correctamente, pero otras operaciones de XClarity Administrator futuras en el dispositivo pueden fallar (especialmente si el dispositivo se gestiona sin autenticación gestionada).
6. Haga clic en **Cambiar** para cambiar los grupos de roles que se pueden asignar a los dispositivos.

   Notas:

   – Puede seleccionar desde una lista de grupos de roles que están asignados al usuario actual.

   – Si no cambia los grupos de roles, se utilizan los grupos de roles predeterminados. Para obtener más información acerca de los grupos de roles predeterminados, consulte Cambiar los permisos predeterminados.
7. Haga clic en **Gestionar**.

   Se visualiza un cuadro de diálogo que muestra el progreso de este proceso de gestión. Para asegurarse de que el proceso se completa satisfactoriamente, supervise el progreso.
8. Cuando el proceso esté completo, haga clic en **Aceptar**.

   El dispositivo se gestiona ahora mediante XClarity Administrator, que automáticamente sondea los dispositivos gestionados de forma periódica para recopilar información actualizada, como el inventario.

   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.

- Para detectar y gestionar dispositivos de almacenamiento que no residen en la misma subred de IP que XClarity Administrator, especifique las direcciones IP manualmente.

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. Seleccione **Entrada manual**.
3. Especifique las direcciones de red de los dispositivos de almacenamiento que desee gestionar:
   - Haga clic en **Sistema único** y especifique una sola dirección IP, nombre de dominio o nombre de dominio totalmente cualificado (FQDN).

     Nota: Para especificar un FQDN, asegúrese de que se haya incluido un nombre de dominio válido en la página de Acceso de red (consulte Configuración del acceso de red).
   - Haga clic en **Varios sistemas** e introduzca un rango de direcciones IP. Para añadir otro rango, haga clic en el icono **Añadir** (). Para quitar un rango haga clic en el icono **Quitar** ().
4. Haga clic en **Aceptar**.
5. Especifique el Id. de usuario y la contraseña para la autenticación del dispositivo de almacenamiento.

   Consejo: se recomienda usar una cuenta de supervisor o administrador para gestionar el dispositivo. Si se utiliza una cuenta con autoridad de nivel inferior, la gestión puede fallar, o la gestión puede finalizar correctamente, pero otras operaciones de XClarity Administrator futuras en el dispositivo pueden fallar (especialmente si el dispositivo se gestiona sin autenticación gestionada).
6. Haga clic en **Cambiar** para cambiar los grupos de roles que se pueden asignar a los dispositivos.

   Notas:
   - Puede seleccionar desde una lista de grupos de roles que están asignados al usuario actual.
   - Si no cambia los grupos de roles, se utilizan los grupos de roles predeterminados. Para obtener más información acerca de los grupos de roles predeterminados, consulte Cambiar los permisos predeterminados.
7. Haga clic en **Gestionar**.

   Se visualiza un cuadro de diálogo que muestra el progreso de este proceso de gestión. Para asegurarse de que el proceso se completa satisfactoriamente, supervise el progreso.
8. Cuando el proceso esté completo, haga clic en **Aceptar**.

   El dispositivo se gestiona ahora mediante XClarity Administrator, que automáticamente sondea los dispositivos gestionados de forma periódica para recopilar información actualizada, como el inventario.

   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.

Después de finalizar

- Detecte y gestione dispositivos adicionales.
- Actualice el firmware de los dispositivos que no cumplen las políticas actuales (consulte Actualización de firmware en dispositivos gestionados).
- Agregue los nuevos dispositivos al bastidor adecuado para reflejar el entorno físico (consulte Gestión de bastidores).
- Supervise el estado y los detalles del hardware (consulte Visualización del estado de los dispositivos de almacenamiento).
- Descubra sucesos y alertas (consulte Trabajo con sucesos y Trabajo con alertas).

Consideraciones de gestión de almacenamiento

Antes de gestionar un dispositivo de almacenamiento, revise las siguientes consideraciones de importancia.

Para obtener más información acerca de los requisitos de los puertos, consulte Disponibilidad de puertos en la documentación en línea de Lenovo XClarity Administrator.

Importante: Asegúrese de que se cumplan los siguientes requisitos antes de detectar y gestionar dispositivos de almacenamiento de bastidor (que no sea ThinkSystem serie DE). Para obtener más información, consulte No se puede detectar un dispositivo y No puede gestionar un dispositivo en la documentación en línea de XClarity Administrator.

- La red de configuración debe permitir el tráfico SLP entre XClarity Administrator y el dispositivo de almacenamiento de bastidor.
- Se requiere SLP de difusión única.
- Se requiere SLP de multidifusión si desea que XClarity Administrator detecte automáticamente los dispositivos Lenovo Storage. Además, se debe habilitar SLP en el dispositivo de almacenamiento de bastidor.

Para los dispositivos Lenovo Storage, el sensor de temperatura más cercano a la placa media del sistema mide la temperatura de aire en el nivel del sistema y refleja la temperatura ambiente después de que el flujo de aire pasa a través de los controladores. Tenga en cuenta que la temperatura del aire notificada por XClarity Administrator y el controlador de gestión puede variar si dicha temperatura se captura en diferentes momentos.

Para dispositivos de almacenamiento Lenovo de la serie DE, es necesario que se pueda acceder a ambos controladores de gestión en la red durante la gestión inicial.

Para algunos dispositivos de almacenamiento, las capturas de SNMP solo están disponibles en inglés.

Visualización del estado de los dispositivos de almacenamiento

Puede ver un resumen y el estado detallado de los dispositivos de almacenamiento gestionados desde Lenovo XClarity Administrator.

Más información:

- XClarity Administrator: inventario
- XClarity Administrator: supervisión

Acerca de esta tarea

Los siguientes iconos de estado se usan para indicar el estado general del dispositivo. Si los certificados no coinciden, se agrega “(no es de confianza)” se agrega al estado de cada dispositivo aplicable, por ejemplo Advertencia (no es de confianza). Si existe un problema de conectividad o si la conexión del dispositivo no tiene confianza, “(Conectividad)” se agrega al estado del dispositivo aplicable, por ejemplo, Advertencia (Conectividad).

- ( ) Crítico
- ( ) Advertencia
- ( ) Pendiente
- ( ) Informativo
- ( ) Normal
- ( ) Fuera de línea
- ( ) Desconocido

Procedimiento

Para ver el estado de un dispositivo de almacenamiento gestionado, realice una o varias de las acciones siguientes.

- En la barra de menús de Lenovo XClarity Administrator, haga clic en **Panel**. Se muestra la página del panel con una descripción general y el estado de todos los dispositivos de almacenamiento gestionados y otros recursos.

- En la barra de menús de Lenovo XClarity Administrator, haga clic en **Hardware → Almacenamiento**. Se muestra la página Almacenamiento con una vista de tabla de todos los dispositivos de almacenamiento que están instalados en el chasis gestionado.

  Puede ordenar las columnas de la tabla para que sea más fácil encontrar los dispositivos de almacenamiento que desea gestionar. Además, puede introducir texto (como un nombre de sistema o

dirección IP) en el campo **Filtro** y hacer clic en los iconos de estado para ver una lista que se limita a mostrar los dispositivos de almacenamiento que cumplen los criterios seleccionados.

Desde esta página puede llevar a cabo las siguientes acciones:

- Ver información detallada acerca del dispositivo de almacenamiento y sus componentes (consulte Visualización de los detalles de un dispositivo de almacenamiento).
- Ver un dispositivo de almacenamiento en una vista gráfica de bastidores o de chasis al hacer clic en **Todas las acciones → Vistas → Mostrar en vista de bastidores** o **Todas las acciones → Vistas → Mostrar en vista de chasis**.
- Iniciar la interfaz web del controlador de gestión del dispositivo de almacenamiento al hacer clic en el vínculo **Dirección IP** (consulte Inicio de la interfaz del controlador de gestión para un dispositivo de almacenamiento).
- Encender y apagar el controlador de almacenamiento en el dispositivo de almacenamiento (consulte Encendido y apagado de un dispositivo de almacenamiento).
- Modifique la información del sistema al seleccionar un dispositivo de almacenamiento y hacer clic en **Todas las acciones → Inventario → Editar propiedades**.
- Actualizar el inventario al seleccionar un dispositivo de almacenamiento y pulsando **Todas las acciones → Inventario → Actualizar inventario**.
- Exportar información detallada acerca de uno o varios dispositivos de almacenamiento a un archivo CSV único al seleccionar los dispositivos de almacenamiento y pulsando **Todas las acciones → Inventario → Exportar inventario**.

  Nota: Puede exportar datos de inventario para un máximo de 60 dispositivos por vez.

  Consejo: Al importar un archivo CSV en Microsoft Excel, Excel trata los valores de texto que contienen solo números como valores numéricos (por ejemplo, para UUID). Formatee cada celda como texto para corregir este error.
- Se anuló la gestión del dispositivo de almacenamiento (consulte Anular la gestión de un dispositivo de almacenamiento).
- (Únicamente dispositivos de almacenamiento de Flex System) Reubicar virtualmente el controlador de almacenamiento en el dispositivo de almacenamiento (consulte Reubicar virtualmente los controladores de almacenamiento en un dispositivo de almacenamiento de Flex System).
- Excluir sucesos que no sean de su interés de todas las páginas en las que se muestran sucesos haciendo clic en el icono **Excluir sucesos** ( ). (consulte Exclusión de sucesos).
- Solucione los problemas que puedan surgir entre el certificado de seguridad de Lenovo XClarity Administrator y el certificado de seguridad del CMM del chasis en el que está instalado el dispositivo de almacenamiento seleccionando un dispositivo de almacenamiento y pulsando **Todas las acciones → Seguridad → Resolver certificados no fiables** (consulte Resolución de un certificado de servidor no fiable).

– Agregue o quite un dispositivo de almacenamiento de un grupo de recursos estático haciendo clic en **Todas las acciones → Grupos → Agregar al grupo** o **Todas las acciones → Grupos → Quitar del grupo**.

Visualización de los detalles de un dispositivo de almacenamiento

Puede ver información detallada acerca de los dispositivos de almacenamiento gestionados desde Lenovo XClarity Administrator, incluidos las direcciones IP, el nombre del producto, el número de serie y los detalles de cada bote.

Acerca de esta tarea

Más información:

- XClarity Administrator: inventario
- XClarity Administrator: supervisión

Para los dispositivos Lenovo Storage, el sensor de temperatura más cercano a la placa media del sistema mide la temperatura de aire en el nivel del sistema y refleja la temperatura ambiente después de que el flujo de aire pasa a través de los controladores. Tenga en cuenta que la temperatura del aire notificada por XClarity Administrator y el controlador de gestión puede variar si dicha temperatura se captura en diferentes momentos.

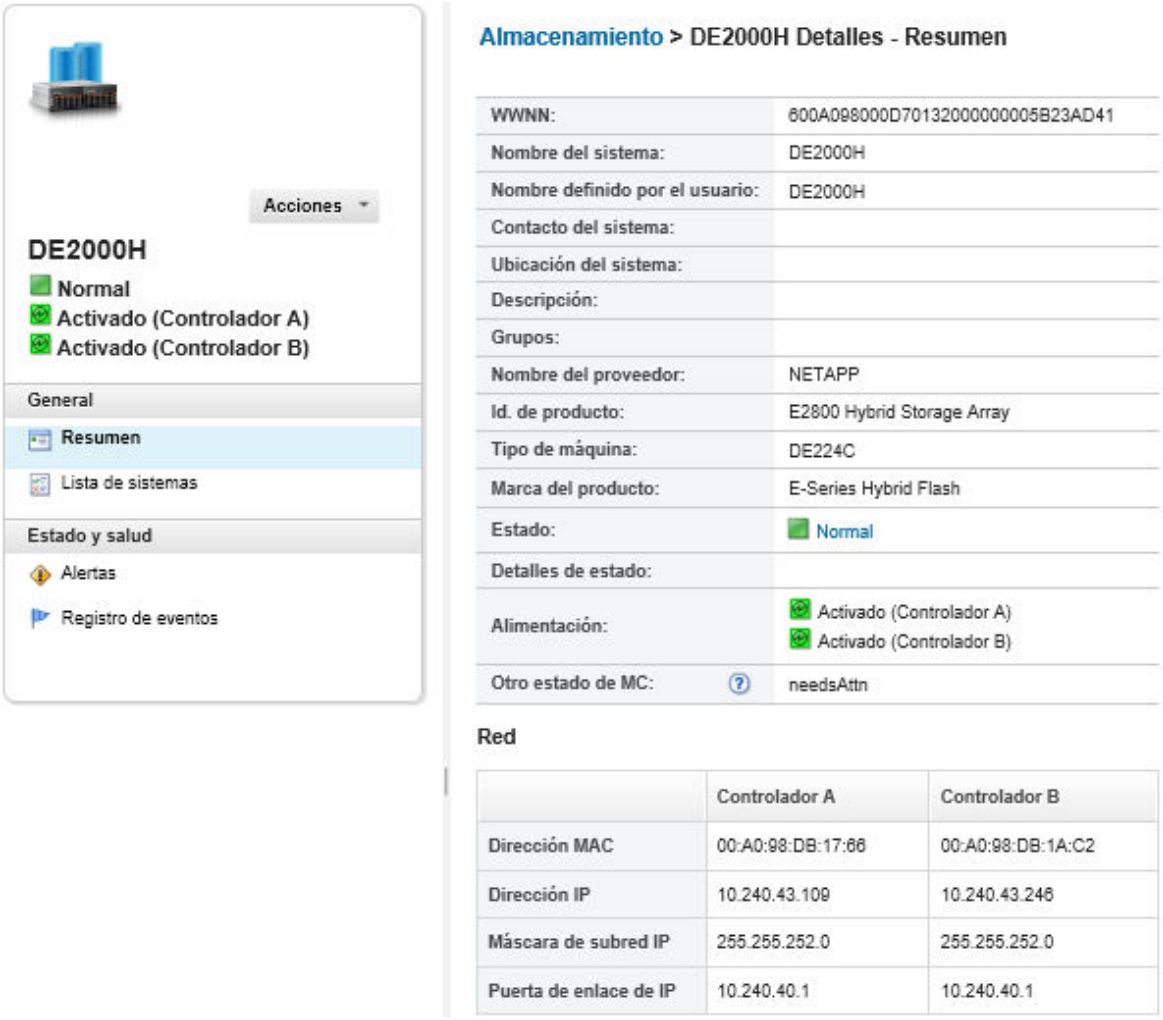
Procedimiento

Para ver los detalles de un dispositivo de almacenamiento gestionado específico, lleve a cabo los pasos siguientes.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Hardware → Almacenamiento**. Se muestra la página Almacenamiento con una vista de tabla de todos los dispositivos de almacenamiento que están instalados en el chasis gestionado.

Puede ordenar las columnas de la tabla para que sea más fácil encontrar los dispositivos de almacenamiento. Además, puede introducir el texto (como un nombre de sistema o una dirección IP) en el campo **Filtro** para aplicar filtros avanzados a los dispositivos de almacenamiento que se visualizan.

Paso 2. Haga clic en el nombre del dispositivo de almacenamiento en la columna **Almacenamiento**. Se muestra la página Resumen con las propiedades y una lista de los componentes que están instalados en ese dispositivo de almacenamiento.



Paso 3. Lleve a cabo uno o más de las siguientes acciones para ver los detalles de almacenamiento. Los datos que se muestran pueden variar según el tipo de dispositivo de almacenamiento.

- Haga clic en **Resumen** para ver un resumen del servidor y los componentes instalados que tiene instalados, incluidos la información del sistema y los dispositivos instalados (consulte Visualización del estado de los dispositivos de almacenamiento).
- Haga clic en **Detalles del inventario** para ver detalles acerca de los componentes del dispositivo de almacenamiento, incluidos:
  - Niveles de firmware para el dispositivo de almacenamiento.
  - Detalles de la red del controlador de gestión, como nombre de host, dirección IPv4, dirección IPv6 y direcciones MAC.
  - Detalles de los activos del dispositivo de almacenamiento.
  - Detalles acerca de cada bote del dispositivo de almacenamiento.

  Consejo: si hay un nodo de expansión, como el nodo de expansión de almacenamiento de Flex System o el PCIe Expansion Node de Flex System, instalado en el chasis y conectado a un dispositivo de almacenamiento, también se muestran los detalles del inventario relativos al nodo de expansión.
- Haga clic en **Alertas** para mostrar las alertas en la lista de alertas relacionadas con el dispositivo de almacenamiento (consulte Trabajo con alertas).

- Haga clic en **Registro de sucesos** para mostrar los sucesos del registro de sucesos que están relacionados con el dispositivo de almacenamientodispositivo de almacenamiento (consulte Trabajo con sucesos).
- Haga clic en **Trabajos** para mostrar una lista de trabajos asociados con el dispositivo de almacenamiento (consulte Supervisión de trabajos).
- Haga clic en **Light path** para mostrar el estado actual de cada uno de los LED del dispositivo de almacenamiento.
- Haga clic en **Alimentación y térmico** para mostrar las características de alimentación y térmicas del dispositivo de almacenamiento.

  Consejo: utilice el botón Actualizar de su navegador web para recopilar los datos de alimentación y térmicos más recientes. La recopilación de datos puede durar varios minutos.

Después de finalizar

Además de mostrar un resumen e información detallada acerca de un dispositivo de almacenamiento, también puede realizar las siguientes acciones:

- Ver un dispositivo de almacenamiento en un bastidor gráfico o una vista de chasis haciendo clic en **Acciones → Vistas → Mostrar en vista de bastidores** o **Acciones → Vistas → Mostrar en vista de chasis**.
- Exportar información detallada acerca del dispositivo de almacenamiento a un archivo CSV pulsando **Acciones → Inventario → Exportar inventario**.

  Notas:

  – Para obtener más información sobre datos de inventario en el archivo CSV, consulte GET /storage/*<UUID_list>* REST API en la documentación en línea de Lenovo XClarity Administrator.

  – Al importar un archivo CSV en Microsoft Excel, Excel trata los valores de texto que contienen solo números como valores numéricos (por ejemplo, para UUID). Formatee cada celda como texto para corregir este error.
- Iniciar la interfaz web del controlador de gestión del dispositivo de almacenamiento al hacer clic en el vínculo **Dirección IP** (consulte Inicio de la interfaz del controlador de gestión para un dispositivo de almacenamiento).
- Encender y apagar un controlador de almacenamiento en el dispositivo de almacenamiento (consulte Encendido y apagado de un dispositivo de almacenamiento).
- Reubicar virtualmente el controlador de almacenamiento en el dispositivo de almacenamiento (consulte Reubicar virtualmente un servidor en un chasis de almacenamiento de Flex System).
- Modifique la información del sistema al seleccionar un dispositivo de almacenamiento y hacer clic en **Editar propiedades**.
- Actualizar el inventario al seleccionar un dispositivo de almacenamiento y pulsando **Acciones → Inventario → Actualizar inventario**.
- Excluya los sucesos que no sean de su interés de todas las páginas en las que se muestran sucesos al hacer clic en el icono **Acciones → Restablecer servicio → Excluir sucesos** (consulte Exclusión de sucesos).
- Solucionar los problemas que puedan surgir entre el certificado de seguridad de XClarity Administrator y el certificado de seguridad del CMM del chasis en el que está instalado el dispositivo de almacenamiento seleccionando un dispositivo de almacenamiento y hacer clic en **Acciones → Servicio → Resolver certificados no fiables** (consulte Resolución de un certificado de servidor no fiable).

Creación de copia de seguridad y restauración de datos de configuración de almacenamiento

Lenovo XClarity Administrator no incluye funciones integradas de copia de seguridad de datos para la configuración de almacenamiento. En su lugar, utilice las funciones de copia de seguridad disponibles para los dispositivos de almacenamiento gestionados.

Consulte la documentación del producto que se proporciona con el dispositivo de almacenamiento para obtener información acerca de cómo recuperar el dispositivo.

- Para dispositivos Lenovo Storage, consulte el Documentación de producto de Lenovo Storage S2200/S3200.
- Para dispositivos de almacenamiento Lenovo ThinkSystem, consulte el Documentación de producto de ThinkSystem Storage.

Encendido y apagado de un dispositivo de almacenamiento

Puede encender y apagar un dispositivo de almacenamiento desde Lenovo XClarity Administrator.

Acerca de esta tarea

Para los dispositivos de almacenamiento de Flex System, cuando se apaga un controlador de almacenamiento, los datos se almacenan primero en la unidad interna y el dispositivo de almacenamiento entra en estado en espera. En estado en espera, ya no se puede acceder a los volúmenes proporcionados por el dispositivo de almacenamiento.

Para encender un dispositivo de almacenamiento de la serie DM ThinkSystem, asegúrese de que el controlador de almacenamiento que se utiliza para la gestión esté en línea y que su dirección IP sea capaz de comunicarse directamente con el procesador de servicio del controlador de almacenamiento apagado mediante la red externa.

Procedimiento

Lleve a cabo los pasos siguientes para encender y apagar un dispositivo de almacenamiento gestionado.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Hardware → Almacenamiento**. Se muestra la página Almacenamiento con una vista de tabla de todos los dispositivos de almacenamiento que están instalados en el chasis gestionado.

Puede ordenar las columnas de la tabla para que sea más fácil encontrar los dispositivos de almacenamiento. Además, puede introducir texto (como un nombre de sistema o una dirección IP) en el campo **Filtro** para filtrar mejor los dispositivos de almacenamiento que se muestran.

Paso 2. Seleccione el dispositivo de almacenamiento que se va a encender o apagar.

Paso 3. Haga clic en **Todas las acciones** y, a continuación, haga clic en una de las siguientes acciones de alimentación:
- **Encender el controlador A**
- **Encender el controlador B**
- **Apagar el controlador A**
- **Apagar el controlador B**
- **Reiniciar el controlador A**
- **Reiniciar el controlador B**

Reubicar virtualmente los controladores de almacenamiento en un dispositivo de almacenamiento de Flex System

Puede realizar una reubicación virtual que simule la retirada y la reinserción de un controlador de almacenamiento (bote) en la bahía del dispositivo de almacenamiento

Acerca de esta tarea

Durante la reubicación virtual, se pierden todas las conexiones de red existentes con el dispositivo de almacenamiento y el estado de alimentación de dicho dispositivo cambia. Antes de realizar una reubicación virtual, asegúrese de que ha guardado todos los datos de los usuarios.

Procedimiento

Lleve a cabo los pasos siguientes para reubicar virtualmente un controlador de almacenamiento.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Hardware → Almacenamiento**. Se muestra la página Almacenamiento con una vista de tabla de todos los dispositivos de almacenamiento.

Puede ordenar las columnas de la tabla para que sea más fácil encontrar los dispositivos de almacenamiento. Además, puede introducir el texto (como un nombre de sistema o una dirección IP) en el campo **Filtro** para aplicar filtros avanzados a los dispositivos de almacenamiento que se visualizan.

Paso 2. Seleccione el dispositivo de almacenamiento de Flex System.

Paso 3. Pulse **Todas las acciones → Servicio** y, a continuación, pulse **Reubicación virtual del controlador A** o **Reubicación virtual del controlador B**.

Paso 4. Haga clic en **Reubicación virtual**.

Inicio de la interfaz del controlador de gestión para un dispositivo de almacenamiento

Puede iniciar la interfaz web del controlador de gestión para el chasis en el que el dispositivo de almacenamiento se instala desde Lenovo XClarity Administrator.

Procedimiento

Lleve a cabo los pasos siguientes para iniciar una interfaz web del controlador de gestión.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Hardware → Almacenamiento**. Se muestra la página Almacenamiento con una vista de tabla de todos los dispositivos de almacenamiento.

Puede ordenar las columnas de la tabla para que sea más fácil encontrar los dispositivos de almacenamiento. Además, puede introducir el texto (como un nombre de dispositivo o una dirección IP) en el campo **Filtro** para aplicar filtros avanzados a los dispositivos de almacenamiento que se visualizan.

Paso 2. Seleccione el dispositivo de almacenamiento.

Paso 3. Haga clic en **Acciones → Iniciar → Interfaz web de gestión**. Se inicia la interfaz web del controlador de gestión.

Paso 4. Inicie sesión en la interfaz del controlador de gestión.

Nota: Para los dispositivos de almacenamiento de Flex System, utilice las credenciales de usuario de XClarity Administrator.

Modificación de las propiedades del sistema de un dispositivo de almacenamiento

Puede modificar las propiedades del sistema de un dispositivo de almacenamiento específico.

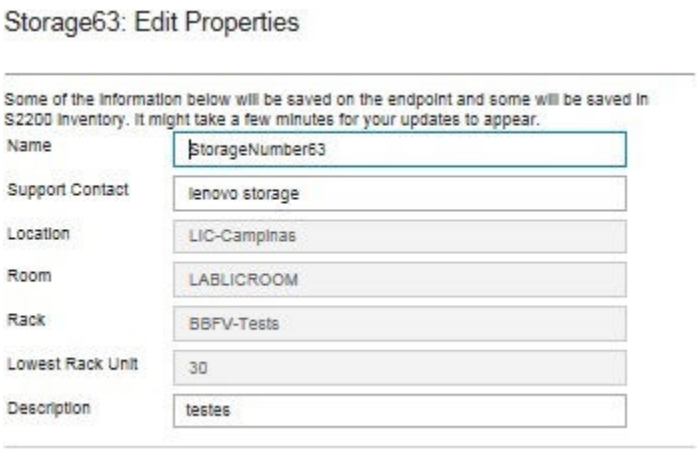
Procedimiento

Para modificar las propiedades del sistema, lleve a cabo los pasos siguientes.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Hardware → Almacenamiento** para mostrar la página Almacenamiento.

Paso 2. Seleccione el dispositivo de almacenamiento que va a actualizar.

Paso 3. Haga clic en **Todas las acciones → Inventario → Editar propiedades**para mostrar el cuadro de diálogo Editar.



Paso 4. Cambie la siguiente información según sea necesario.
- Nombre
- Contacto de soporte
- Descripción

Nota: XClarity Administrator actualiza las propiedades de ubicación, sala, bastidor y unidad de bastidor más baja cuando se agregan o quitan dispositivos de un bastidor en la interfaz web (consulte Gestión de bastidores).

Paso 5. Haga clic en **Guardar**.

Nota: Al cambiar estas propiedades, pueden transcurrir unos instantes antes de que los cambios aparezcan en la interfaz web de XClarity Administrator.

Recuperación de la gestión de un dispositivo de almacenamiento de bastidor tras un error de servidor de gestión

Si la gestión de un dispositivo de almacenamiento de bastidor no se ha anulado correctamente, debe recuperar el dispositivo de almacenamiento antes de poder gestionarlo de nuevo. Puede recuperar la gestión al borrar las partes específicas de la configuración del dispositivo de almacenamiento establecida previamente por Lenovo XClarity Administrator.

Procedimiento

Lleve a cabo uno de los siguientes pasos para la recuperación un dispositivo de almacenamiento de servidor.

- 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 opción **Forzar gestión** (consulte Gestión de los dispositivos de almacenamiento).
- Quite todas las cuentas de usuario con el prefijo “LXCA_” y opcionalmente quite las cuentas de usuario con el prefijo “SYSMGR_” y escriba “SNMPv3” del dispositivo de almacenamiento.

Después de finalizar

Una vez que XClarity Administrator se haya restaurado o sustituido, puede volver a gestionar el dispositivo de almacenamiento (consulte el Gestión de los dispositivos de almacenamiento). Se conserva toda la información acerca del dispositivo de almacenamiento (como las propiedades del sistema).

Recuperación de la gestión de un dispositivo de almacenamiento Lenovo ThinkSystem DE Series tras un error de servidor de gestión

Si la gestión de un dispositivo de almacenamiento Lenovo ThinkSystem DE series no se anuló correctamente, debe recuperar el dispositivo de almacenamiento antes de poder gestionarlo de nuevo. Puede recuperar la gestión al borrar las partes específicas de la configuración del dispositivo de almacenamiento establecida previamente por Lenovo XClarity Administrator.

Procedimiento

Complete uno de los siguientes pasos para la recuperación un dispositivo de almacenamiento Lenovo ThinkSystem DE Series.

- 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 opción **Forzar gestión** (consulte Gestión de los dispositivos de almacenamiento).
- Elimine el registro de par de claves “LXCA_REMOTE_MANAGMENT_VERIFICATION” de la API de par de claves del dispositivo de almacenamiento.

Después de finalizar

Una vez que XClarity Administrator se haya restaurado o sustituido, puede volver a gestionar el dispositivo de almacenamiento (consulte el Gestión de los dispositivos de almacenamiento). Se conserva toda la información acerca del dispositivo de almacenamiento (como las propiedades del sistema).

Anular la gestión de un dispositivo de almacenamiento

Puede quitar un dispositivo de almacenamiento de la gestión mediante Lenovo XClarity Administrator. Este proceso se denomina *anular la gestión* (no gestionar).

Antes de empezar

Antes de eliminar la gestión de un dispositivo de almacenamiento, asegúrese de que no hay trabajos activos en ejecución en el conmutador.

Acerca de esta tarea

Cuando se anula la gestión de un dispositivo de almacenamiento, XClarity Administrator conserva determinada información acerca del dispositivo de almacenamiento. Esta información se vuelve a aplicar cuando se gestiona de nuevo el mismo dispositivo de almacenamiento.

Consejo: todos los dispositivos de demostración que se añaden opcionalmente durante la configuración inicial son nodos en un chasis. Para anular la gestión de los dispositivos de demostración, anule la gestión del chasis utilizando la opción **Forzar anulación de gestión incluso si no se puede acceder al dispositivo**.

Procedimiento

Para dejar de gestionar un dispositivo de almacenamiento, lleve a cabo los pasos siguientes.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Hardware → Almacenamiento** para mostrar la página Almacenamiento.

Paso 2. Seleccione uno o más dispositivos de almacenamiento de las listas de conmutadores gestionados.

Paso 3. Haga clic en **No gestionar**. Se muestra el cuadro de diálogo No gestionar.

Paso 4. **Opcional:** seleccione **Forzar anulación de gestión aunque el dispositivo no esté accesible**.

Importante: Asegúrese de seleccionar esta opción si está anulando la gestión de un hardware de demostración.

Paso 5. Haga clic en **No gestionar**.El cuadro de diálogo No gestionar muestra el progreso de cada paso en el proceso de anulación de la gestión.

Paso 6. Cuando el proceso de anulación de la gestión esté completo, pulse **Aceptar**.

Recuperación de un dispositivo de almacenamiento de bastidor en el que la gestión no se ha anulado correctamente

Si un dispositivo de almacenamiento de bastidor se está gestionando mediante Lenovo XClarity Administrator y XClarity Administrator produce un error, puede recuperar las funciones de gestión hasta que el servidor de gestión se restaure o se sustituya. Puede recuperar la gestión del sistema al borrar las partes específicas de la configuración del dispositivo de almacenamiento establecida previamente por XClarity Administrator.

Procedimiento

Lleve a cabo uno de los siguientes pasos para la recuperación un dispositivo de almacenamiento de servidor.

- 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 opción **Forzar gestión** (consulte Gestión de los dispositivos de almacenamiento).
- Quite todas las cuentas de usuario con el prefijo “LXCA_” y opcionalmente quite las cuentas de usuario con el prefijo “SYSMGR_” y escriba “SNMPv3” del dispositivo de almacenamiento.

Después de finalizar

Una vez que XClarity Administrator se haya restaurado o sustituido, puede volver a gestionar el dispositivo de almacenamiento (consulte el Gestión de los dispositivos de almacenamiento). Se conserva toda la información acerca del dispositivo de almacenamiento (como las propiedades del sistema).

Capítulo 10. Gestión de conmutadores

Lenovo XClarity Administrator puede gestionar conmutadores de red.

Más información:

- XClarity Administrator: detección
- XClarity Administrator: Administrar conmutadores

Antes de empezar

Atención: Revise las consideraciones de gestión de conmutadores antes de gestionar un conmutador. Para obtener más información, consulte Consideraciones de gestión de conmutadores.

Nota: Los conmutadores Flex se detectan y gestionan automáticamente cuando gestiona el chasis que los contiene. No puede detectar ni gestionar conmutadores Flex de forma independiente del chasis.

Algunos puertos deben estar disponibles para comunicarse con los conmutadores. Asegúrese de que todos los puertos requeridos estén disponibles antes de intentar gestionar un conmutador. Para obtener más información sobre los puertos, consulte Disponibilidad de puertos en la documentación en línea de XClarity Administrator.

Asegúrese de que el firmware mínimo necesario esté instalado en cada conmutador 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 crear credenciales almacenadas en XClarity Administrator antes de gestionar conmutadores de bastidor. XClarity Administrator solo utiliza credenciales almacenadas para autenticar los conmutadores de bastidor. Las credenciales almacenadas deben coincidir con una cuenta de usuario activa en el dispositivo. Puede crear credenciales almacenadas en los cuadros de diálogo de gestión o desde la página Credenciales almacenadas. Para obtener más información, consulte el apartado Gestión de credenciales almacenadas.

Se admite la gestión utilizando interfaces de bucle invertido para todos los dispositivos de RackSwitch. Asegúrese de que XClarity Administrator tenga conectividad a la interfaz de bucle invertido, agregando una ruta estática o anunciando la dirección a través de un protocolo de enrutamiento. Tenga en cuenta que no se puede realizar la disposición entre el puerto de gestión y *cualquier* puerto de datos (incluidos de bucle invertido).

Para conmutadores de la serie Lenovo ThinkSystem DB:

- Se necesita FOS 8.2.3 o posterior
- Asegúrese de configurar el usuario SNMPv3 en el índice 1 del conmutador *antes* de gestionar el conmutador ejecutando el siguiente comando en el conmutador: `snmpconfig --add snmpv3 -index 1 -user snmpadmin1 -groupname rw`
- Asegúrese de que REST esté habilitado en el conmutador. Para habilitar REST, ejecute el siguiente comando: `mgmtapp --enable rest`
- Asegúrese de que el número de sesiones REST permitidas sea 10. Para establecer el recuento de la sesión REST, ejecute el siguiente comando: `mgmtapp --config -maxrestsession 10`

- Los conmutadores de la serie Lenovo ThinkSystem DB no se pueden detectar mediante protocolos de detección de servicio. Para gestionar estos conmutadores, utilice la opción **Entrada manual**, borre los **Protocolos de detección de servicios de usuario para identificar el tipo de dispositivo** y, a continuación, seleccione “Lenovo ThinkSystem DB Series Switch” en la lista **Tipo de dispositivo**. Para obtener más detalles, consulte el procedimiento que se indica a continuación para detectar y gestionar conmutadores que no están en la misma subred IP que XClarity Administrator.

Para los conmutadores NVIDIA:

- Se necesita Cumulus 4.3 o posterior
- Los conmutadores NVIDIA no se pueden detectar mediante protocolos de detección de servicio. Para gestionar estos conmutadores, utilice la opción **Entrada manual**, borre los Protocolos de detección de servicios de usuario para identificar el tipo de dispositivo y, a continuación, seleccione “Conmutador NVIDIA” desde la lista **Tipo de dispositivo**. Para obtener más detalles, consulte el procedimiento que se indica a continuación para detectar y gestionar conmutadores que no están en la misma subred IP que XClarity Administrator.

Acerca de esta tarea

XClarity Administrator puede detectar automáticamente conmutadores RackSwitch en su entorno, sondeando los dispositivos gestionables que se encuentran en la misma subred IP, como XClarity Administrator. Para detectar los conmutadores que están en otras subredes, especifique una dirección IP o un rango de direcciones IP, o importe la información de una hoja de cálculo.

Nota: Las credenciales manuales no son compatibles con los conmutadores de bastidor en XClarity Administrator.

Una vez que XClarity Administrator gestiona los conmutadores, XClarity Administrator sondea periódicamente todos los conmutadores gestionados para recopilar información, como el inventario, los datos de producto fundamentales y el estado. Puede consultar y supervisar cada conmutador gestionado y realizar tareas de gestión, como iniciar la consola de gestión y realizar operaciones de encendido y apagado.

Si el XClarity Administrator pierde la comunicación con el conmutador (por ejemplo, debido a la falla de red o una pérdida de alimentación o si el conmutador está fuera de línea) al recopilar el inventario durante el proceso de gestión, realiza la gestión correctamente; sin embargo, es posible que alguna información de inventario esté incompleta. Espere a que el conmutador entre en línea y que XClarity Administrator sondee el conmutador para el inventario o recopile manualmente el inventario en el conmutador de la página Conmutadores seleccionando el conmutador y haciendo clic en **Todas las acciones → Inventario → Actualizar inventario**.

Nota: Los conmutadores se pueden apilar. Un *conmutador apilado* es un grupo de conmutadores que pueden funcionar como un solo conmutador de red. La pila incluye un *conmutador principal* y uno o varios *conmutadores miembro*. Para los conmutadores Flex, puede ver y supervisar cada uno de los conmutadores de la pila y recopilar datos de diagnóstico; no obstante, no puede realizar tareas de gestión (como las actualizaciones de firmware y la configuración del servidor) en ningún conmutador apilado. Estas tareas de gestión de XClarity Administrator están deshabilitadas para todos los conmutadores apilados, incluido el conmutador maestro. Puede actualizar el firmware del conmutador apilado directamente desde el CLI del conmutador principal. Para conmutadores RackSwitch, puede ver y supervisar únicamente la información del conmutador maestro. XClarity Administrator no detecta los conmutadores miembros.

Las tareas de gestión también están deshabilitadas para los Conmutadores Flex que están en modo protegido.

Un dispositivo solo puede estar gestionado 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. Si se produce un error durante el proceso de anulación de la gestión, puede seleccionar la opción **Forzar gestión** durante la gestión del nuevo XClarity Administrator.

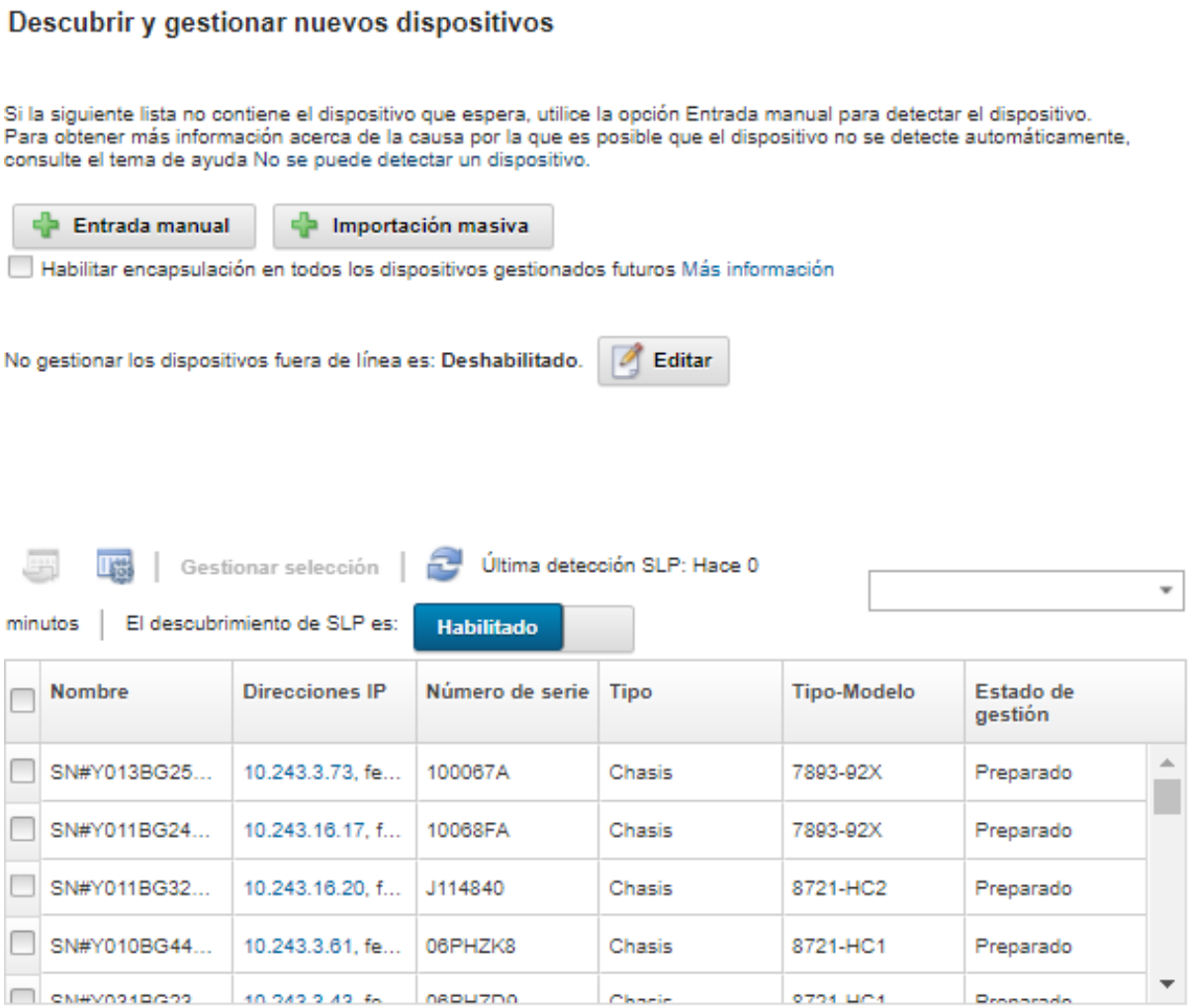
Nota: Cuando explora la red en busca de dispositivos gestionables, XClarity Administrator no reconoce si un dispositivo ya está gestionado por otro gestionador hasta después de intentar gestionar el dispositivo.

Cuando un conmutador está gestionado directamente usando SSH o de forma indirecta mediante un CMM, el conmutador se identifica como gestionado por XClarity Administrator, se realiza la configuración necesaria para la interacción y se recopila el inventario.

Procedimiento

Complete uno de los procedimientos siguientes para gestionar los conmutadores RackSwitch mediante XClarity Administrator.

- Detecte y gestione un gran número de conmutadores y otros dispositivos utilizando un archivo de importación masiva (consulte Gestión de sistemas en la documentación en línea de Lenovo XClarity Administrator).
- Descubra y gestione conmutadores RackSwitch que están en la misma subred IP que XClarity Administrator.
  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 dispositivos nuevos.



Puede ordenar las columnas de la tabla para que sea más fácil encontrar los conmutadores que desea gestionar. Además, puede introducir texto (como un nombre o una dirección IP) en el campo **Filtro** para aplicar filtros avanzados a los conmutadores que se muestran. Puede cambiar las columnas que se muestran el orden predeterminado haciendo clic en el icono **Personalizar columnas** ( ).

2. Haga clic en el icono **Actualizar** ( ) para descubrir todos los dispositivos gestionables en el dominio XClarity Administrator. La detección puede durar varios minutos.
3. Seleccione uno o varios conmutadores que desee gestionar.
4. Haga clic en **Gestionar selección**.
5. Especifique las credenciales almacenadas para la autenticación de los conmutadores.

   Consejo:

   – Haga clic en **Gestionar credenciales almacenadas** para crear y gestionar las credenciales almacenadas en XClarity Administrator (consulte Gestión de credenciales almacenadas).

   – Se recomienda usar una cuenta de supervisor o administrador para gestionar el dispositivo. Si se utiliza una cuenta con autoridad de nivel inferior, la gestión puede fallar, o la gestión puede finalizar correctamente, pero otras operaciones de XClarity Administrator futuras en el dispositivo pueden fallar (especialmente si el dispositivo se gestiona sin autenticación gestionada).

6. (Solo conmutadores que ejecutan ENOS) Si está configurado, especifique la contraseña para “habilitar” el ingreso a Privileged Exec Mode en el conmutador.

   Al gestionar un conmutador RackSwitch que ejecutan ENOS, es obligatorio el acceso a Privileged Exec Mode en el conmutador. Esto lo usa XClarity Administrator al emitir del mandato “enable” al conmutador. De forma predeterminada, no hay una contraseña establecida para este mandato en el conmutador. Sin embargo, si el administrador del conmutador configuró una contraseña para este mandato para mayor seguridad, se debe especificar para que XClarity Administrator gestione el conmutador correctamente.

7. Opcional: (Solo conmutadores que ejecutan ENOS) Para elegir si desea habilitar HTTPS en el conmutador, haga clic en **Avanzado** y luego seleccione **Habilitar HTTPS**. Esto está habilitado de forma predeterminada.

   Notas:

   – Para conmutadores que ejecutan CNOS, HTTPS debe estar habilitado en el conmutador antes de la gestión (consulte Consideraciones de gestión de conmutadores).
   – Si elige no habilitar HTTPS, se usa la configuración actual del conmutador.
   – Cuando el conmutador está gestionado, XClarity Administrator restaura HTTPS a su configuración original.

8. Opcional: Elija si va a sustituir la configuración de NTP en el conmutador con los valores de zona horaria y los valores NTP que se definen para Lenovo XClarity Administrator haciendo clic en **Avanzado** y luego seleccionando **Configurar clientes NTP para utilizar la configuración de NTP desde el servidor de gestión**. Esto está habilitado de forma predeterminada.

   Notas:

   – Si elige *no* reemplazar los valores NTP y la zona horaria, la marca de tiempo de entradas de registro y sucesos podrían estar fuera de sincronización entre los conmutadores gestionados y el servidor de gestión.
   – Cuando el conmutador está gestionado, XClarity Administrator restaura los valores NTP y la zona horaria en la configuración original.

9. Haga clic en **Cambiar** para cambiar los grupos de roles que se pueden asignar a los dispositivos.

   Notas:

   – Puede seleccionar desde una lista de grupos de roles que están asignados al usuario actual.
   – Si no cambia los grupos de roles, se utilizan los grupos de roles predeterminados. Para obtener más información acerca de los grupos de roles predeterminados, consulte Cambiar los permisos predeterminados.

10. Haga clic en **Gestionar**.

    Se visualiza un cuadro de diálogo que muestra el progreso de este proceso de gestión. Para asegurarse de que el proceso se completa satisfactoriamente, supervise el progreso.

11. Cuando el proceso esté completo, haga clic en **Aceptar**.

    El dispositivo se gestiona ahora mediante XClarity Administrator, que automáticamente sondea los dispositivos gestionados de forma periódica para recopilar información actualizada, como el inventario.

    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.

- Descubra y gestione conmutadores RackSwitch que no están en la misma subred IP que XClarity Administrator especificando manualmente direcciones IP:
  1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Hardware → Detectar y gestionar dispositivos nuevos**. Se muestra la página Detectar y gestionar.
  2. Seleccione **Entrada manual**.
  3. Especifique las direcciones de red de los conmutadores que desee gestionar:
     - Haga clic en **Sistema único** y especifique una sola dirección IP, nombre de dominio o nombre de dominio totalmente cualificado (FQDN).

       Nota: Para especificar un FQDN, asegúrese de que se haya incluido un nombre de dominio válido en la página de Acceso de red (consulte Configuración del acceso de red).
     - Haga clic en **Varios sistemas** e introduzca un rango de direcciones IP. Para añadir otro rango, haga clic en el icono **Añadir** (). Para quitar un rango haga clic en el icono **Quitar** ().
  4. Si el tipo de dispositivo no se puede detectar con los protocolos de detección del servicio, borre los protocolos de detección del servicio del usuario para identificar el tipo de dispositivo y luego seleccione en la lista desplegable el tipo de dispositivo que se gestionará.

     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
  5. Haga clic en **Aceptar**.
  6. Especifique las credenciales almacenadas para la autenticación de los conmutadores.

     Consejo:
     - Haga clic en **Gestionar credenciales almacenadas** para crear y gestionar las credenciales almacenadas en XClarity Administrator (consulte Gestión de credenciales almacenadas).
     - Se recomienda usar una cuenta de supervisor o administrador para gestionar el dispositivo. Si se utiliza una cuenta con autoridad de nivel inferior, la gestión puede fallar, o la gestión puede finalizar correctamente, pero otras operaciones de XClarity Administrator futuras en el dispositivo pueden fallar (especialmente si el dispositivo se gestiona sin autenticación gestionada).

7. (Solo conmutadores que ejecutan ENOS) Si está configurado, especifique la contraseña para “habilitar” el ingreso a Privileged Exec Mode en el conmutador.

   Al gestionar un conmutador RackSwitch que ejecutan ENOS, es obligatorio el acceso a Privileged Exec Mode en el conmutador. Esto lo usa XClarity Administrator al emitir del mandato “enable” al conmutador. De forma predeterminada, no hay una contraseña establecida para este mandato en el conmutador. Sin embargo, si el administrador del conmutador configuró una contraseña para este mandato para mayor seguridad, se debe especificar para que XClarity Administrator gestione el conmutador correctamente.

8. Opcional: (Solo conmutadores que ejecutan ENOS) Para elegir si desea habilitar HTTPS en el conmutador, haga clic en **Avanzado** y luego seleccione **Habilitar HTTPS**. Esto está habilitado de forma predeterminada.

   Notas:

   – Para conmutadores que ejecutan CNOS, HTTPS debe estar habilitado en el conmutador antes de la gestión (consulte Consideraciones de gestión de conmutadores).
   – Si elige no habilitar HTTPS, se usa la configuración actual del conmutador.
   – Cuando el conmutador está gestionado, XClarity Administrator restaura HTTPS a su configuración original.

9. Opcional: Elija si va a sustituir la configuración de NTP en el conmutador con los valores de zona horaria y los valores NTP que se definen para Lenovo XClarity Administrator haciendo clic en **Avanzado** y luego seleccionando **Configurar clientes NTP para utilizar la configuración de NTP desde el servidor de gestión**. Esto está habilitado de forma predeterminada.

   Notas:

   – Si elige *no* reemplazar los valores NTP y la zona horaria, la marca de tiempo de entradas de registro y sucesos podrían estar fuera de sincronización entre los conmutadores gestionados y el servidor de gestión.
   – Cuando el conmutador está gestionado, XClarity Administrator restaura los valores NTP y la zona horaria en la configuración original.

10. Haga clic en **Cambiar** para cambiar los grupos de roles que se pueden asignar a los dispositivos.

    Notas:

    – Puede seleccionar desde una lista de grupos de roles que están asignados al usuario actual.
    – Si no cambia los grupos de roles, se utilizan los grupos de roles predeterminados. Para obtener más información acerca de los grupos de roles predeterminados, consulte Cambiar los permisos predeterminados.

11. Haga clic en **Gestionar**.

    Se visualiza un cuadro de diálogo que muestra el progreso de este proceso de gestión. Para asegurarse de que el proceso se completa satisfactoriamente, supervise el progreso.

12. Cuando el proceso esté completo, haga clic en **Aceptar**.

    El dispositivo se gestiona ahora mediante XClarity Administrator, que automáticamente sondea los dispositivos gestionados de forma periódica para recopilar información actualizada, como el inventario.

    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.

Después de finalizar

- Detecte y gestione dispositivos adicionales.
- Agregue los dispositivos recién gestionados al bastidor adecuado para reflejar el entorno físico (consulte Gestión de bastidores).
- Supervise el estado y los detalles del hardware (consulte Visualización del estado de los conmutadores).
- Supervise sucesos (consulte Trabajo con sucesos).

Consideraciones de gestión de conmutadores

Antes de gestionar un conmutador, revise las siguientes consideraciones de importancia.

Para obtener más información acerca de los requisitos de los puertos, consulte Disponibilidad de puertos en la documentación en línea de Lenovo XClarity Administrator.

Los dispositivos RackSwitch se pueden gestionar mediante el puerto de gestión o uno de los puertos de datos. Se pueden gestionar dispositivos de Rackswitch CNOS en ejecución en interfaces que pertenecen a “gestión” o VRF “predeterminado”.

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

Sucesos de XClarity y configuración de interrupciones SNMP

Cuando se gestiona un dispositivo RackSwitch ejecutando ENOS (cualquier versión), la fuente de interrupciones SNMP se establece en la interfaz que tiene la dirección IP que se utiliza para la gestión.

Cuando se gestiona un dispositivo de RackSwitch que ejecuta CNOS v10.8.1 o posterior, el VFR de origen de la interrupción SNMP se comprueba y se cambia para que coincida con el puerto que se utiliza para la gestión.

Para los dispositivos de RackSwitch que ejecutan CNOS anterior a v10.8.1, XClarity Administrator requiere que el origen de interrupciones SNMP sea el VRF que está conectado al puerto que se utiliza para la gestión. El valor predeterminado “todos” permite que los puertos de gestión o de datos se utilicen. Si la configuración del conmutador no utiliza el valor predeterminado, debe cambiarse para que coincida con el puerto que se utiliza para la gestión.

- Si se utiliza el puerto de gestión para la gestión, configure el VRF de origen de interrupción de SNMP en “todos” o “gestión.”

- Si se utiliza uno de los puertos de datos para la gestión, configure el VRF de origen de interrupción de SNMP en “todos” o “predeterminado.”

Conmutadores RackSwitch que ejecutan CNOS

HTTPS debe estar habilitado para la gestión y SLP debe estar habilitado para el descubrimiento.

Nota: HTTPS está habilitado de forma predeterminada en CNOS. Si cambió la configuración predeterminada del restApi (utilizando el comando `feature restApi http`), puede volver a cambiarlo a HTTPS utilizando el comando `feature restApi`. Para comprobar el estado actual, utilice el comando `display restApi server`. El resultado refleja el estado actual. Si el número de puerto se seguido por “(HTTP)”, esto significa que HTTPS está *deshabilitado*. De lo contrario, el puerto debe ser 443.

Cuando un dispositivo de RackSwitch no está gestionado, XClarity Administrator puede no ser capaz de restablecer la opción “preferir” con el valor en que se encontraba antes de que el dispositivo se gestionara según la versión de firmware CNOS.

Conmutadores RackSwitch que ejecutan ENOS

- Si los conmutadores RackSwitch están en una red distinta de XClarity Administrator, la red se debe configurar para permitir UDP entrante mediante los puertos 161 y 162 para que XClarity Administrator pueda recibir y gestionar sucesos para esos dispositivos.
- Se debe habilitar SSH para la gestión y se debe habilitar SLP para la detección. HTTPS es opcional; sin embargo, debe estar habilitado para iniciar la interfaz web del conmutador
- 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.
  - `ip slp enable`
  - `ssh enable`
- Cuando se gestiona un conmutador RackSwitch, XClarity Administrator modifica los siguientes valores de configuración. Cambiar estos valores en un conmutador gestionado puede interrumpir la conectividad y evitar que se realicen correctamente las acciones de gestión. Cuando un conmutador RackSwitch no está gestionado, los valores de configuración se restablecen a los valores originales (antes de la gestión).
  - snmp-server access 32
  - snmp-server group 16
  - snmp-server notify 16
  - snmp-server target-parameters 16
  - snmp-server target-address 16
  - snmp-server trap-source <*IP interface*>
  - snmp-server user 16
  - versión de servidor snmp <*v3only or v1v2v3*>
  - ntp enable
  - ntp primary-server <*hostname or IP address*> MGT
  - ntp secondary-server <*hostname or IP address*> MGT
  - ntp interval 1500
  - ntp offset 500
  - access https enable

  Puede usar XClarity Administrator para modificar los siguientes valores de configuración al modificar las propiedades de información de contacto de soporte, nombre o ubicación para el conmutador. La ubicación se modifica al agregar el conmutador al bastidor.
  - hostname “<*device_name*>”
  - snmp-server location “Location:<*location*>,Room:<*room*>,Rack:<*rack*>,LRU:<*lru*>”
  - snmp-server contact “<*contact_name*>”

Visualización del estado de los conmutadores

Puede ver el estado de todos los conmutadores que se están gestionando mediante Lenovo XClarity Administrator.

Más información:

- XClarity Administrator: inventario
- XClarity Administrator: supervisión

Acerca de esta tarea

Los siguientes iconos de estado se usan para indicar el estado general del dispositivo. Si los certificados no coinciden, se agrega “(no es de confianza)” se agrega al estado de cada dispositivo aplicable, por ejemplo Advertencia (no es de confianza). Si existe un problema de conectividad o si la conexión del dispositivo no tiene confianza, “(Conectividad)” se agrega al estado del dispositivo aplicable, por ejemplo, Advertencia (Conectividad).

- ( ) Crítico
  - Uno o más sensores de temperatura están en el rango de falla.
  - Los módulos de ventilador o los ventiladores no funcionan correctamente, según lo siguiente:
    - RackSwitch G8124-E: uno o más ventiladores están funcionando a 100 RPM o menos.
    - RackSwitch G8052: menos de tres módulos de ventilador están en buen estado. Si los ventiladores en ese módulo están funcionando a más de 500 RPM, un módulo de ventilador se considera en buen estado.
    - RackSwitch G8264, G8264CS, G8332, G8272: menos de cuatro módulos de ventilador están en buen estado. Si los ventiladores en ese módulo están funcionando a más de 500 RPM, un módulo de ventilador se considera en buen estado.
    - RackSwitch G8296: menos de tres ventiladores están en buen estado. Si los ventiladores en ese módulo están funcionando a más de 480 RPM, un módulo de ventilador se considera en buen estado.
    - RackSwitch G7028, G7052: menos de tres módulos de ventilador están en buen estado. Si los ventiladores en ese módulo están funcionando a más de 500 RPM, un módulo de ventilador se considera en buen estado.
  - Una fuente de alimentación está apagada.
- ( ) Advertencia
  - Uno o más sensores de temperatura están en el rango de advertencia.
  - En flash existe un volcado de pánico.
- ( ) Pendiente
- ( ) Informativo
- ( ) Normal
  - Todos los sensores de temperatura están en el rango normal.
  - Todos los módulos de ventilador o los ventiladores funcionan correctamente.
  - Ambas fuentes de alimentación están encendidas.
  - En flash no existe ningún volcado de pánico.
- ( ) Fuera de línea
- ( ) Desconocido

Un dispositivo puede estar en uno de los siguientes estados de alimentación:

- Activado
- Apagado
- Apagar

- En espera
- Hibernar
- Desconocido

Procedimiento

Para ver el estado de un conmutador gestionado, realice una o más de las acciones siguientes.

- En la barra de menús de XClarity Administrator, haga clic en **Panel**. Se muestra la página del panel con una descripción general y el estado de todos los conmutadores gestionados y otros recursos.

- En la barra de menús de XClarity Administrator, haga clic en **Hardware → Conmutadores**. Se muestra la página Conmutadores con una vista de tabla de todos los conmutadores gestionados.

  Puede ordenar las columnas de la tabla para que sea más fácil encontrar los conmutadores que desea gestionar. Además, puede introducir texto (como un nombre o dirección IP) en el campo **Filtro** y hacer clic en los iconos de estado para ver una lista que se limita a mostrar los conmutadores que cumplen los criterios seleccionados.

Desde esta página puede llevar a cabo las siguientes acciones:

- Ver información detallada sobre el conmutador (consulte Visualización de los detalles de un conmutador).
- Vea un conmutador Flex en la vista gráfica de bastidores o de chasis haciendo clic en **Todas las acciones → Vistas → Mostrar en vista de bastidores** o **Todas las acciones → Vistas → Mostrar en vista de chasis**.
- Vea un conmutador RackSwitch en la vista gráfica al hacer clic en **Todas las acciones → Vistas → Mostrar en vista de bastidores**.
- Iniciar la interfaz web del controlador de gestión del conmutador al hacer clic en el vínculo **Dirección IP** (consulte Inicio de la interfaz del controlador de gestión para un conmutador).
- Inicie la consola SSH del conmutador (consulte Inicia una sesión SSH remota para un conmutador).
- Encender y apagar el conmutador (consulte Encendido y apagado de un conmutador).
- (Solo conmutadores RackSwitch) Modifique la información del sistema al seleccionar un conmutador y haga clic en **Todas las acciones → Inventario → Editar propiedades**.
- Actualizar el inventario al seleccionar un servidor y hacer clic en **Todas las acciones → Inventario → Actualizar inventario**.
- Exporte información detallada acerca de uno o varios conmutadores a un archivo CSV único al seleccionar los conmutadores y al hacer clic en **Todas las acciones → Inventario → Exportar inventario** (consulte Exclusión de sucesos).

  Nota: Puede exportar datos de inventario para un máximo de 60 dispositivos por vez.

  Consejo: Al importar un archivo CSV en Microsoft Excel, Excel trata los valores de texto que contienen solo números como valores numéricos (por ejemplo, para UUID). Formatee cada celda como texto para corregir este error.
- Excluir los sucesos que no sean de su interés de todas las páginas en las que se muestran sucesos haciendo clic en el icono **Excluir sucesos** ( ) (consulte Exclusión de sucesos).
- (Únicamente conmutadores Flex) Solucionar los problemas que puedan surgir entre el certificado de seguridad de XClarity Administrator y el certificado de seguridad del CMM del chasis en el que está instalado el conmutador seleccionando un conmutador y pulsando **Todas las acciones → Seguridad → Resolver certificados no fiables** (consulte Resolución de un certificado de servidor no fiable).
- Agregue o quite un conmutador de un grupo de recursos estático haciendo clic en **Todas las acciones → Grupos → Agregar a grupo** o **Todas las acciones → Grupos → Quitar del grupo**.

Visualización de los detalles de un conmutador

Puede ver información detallada sobre un conmutador gestionado desde Lenovo XClarity Administrator, incluidos los niveles de firmware y las direcciones IP.

Más información:

- XClarity Administrator: inventario
- XClarity Administrator: supervisión

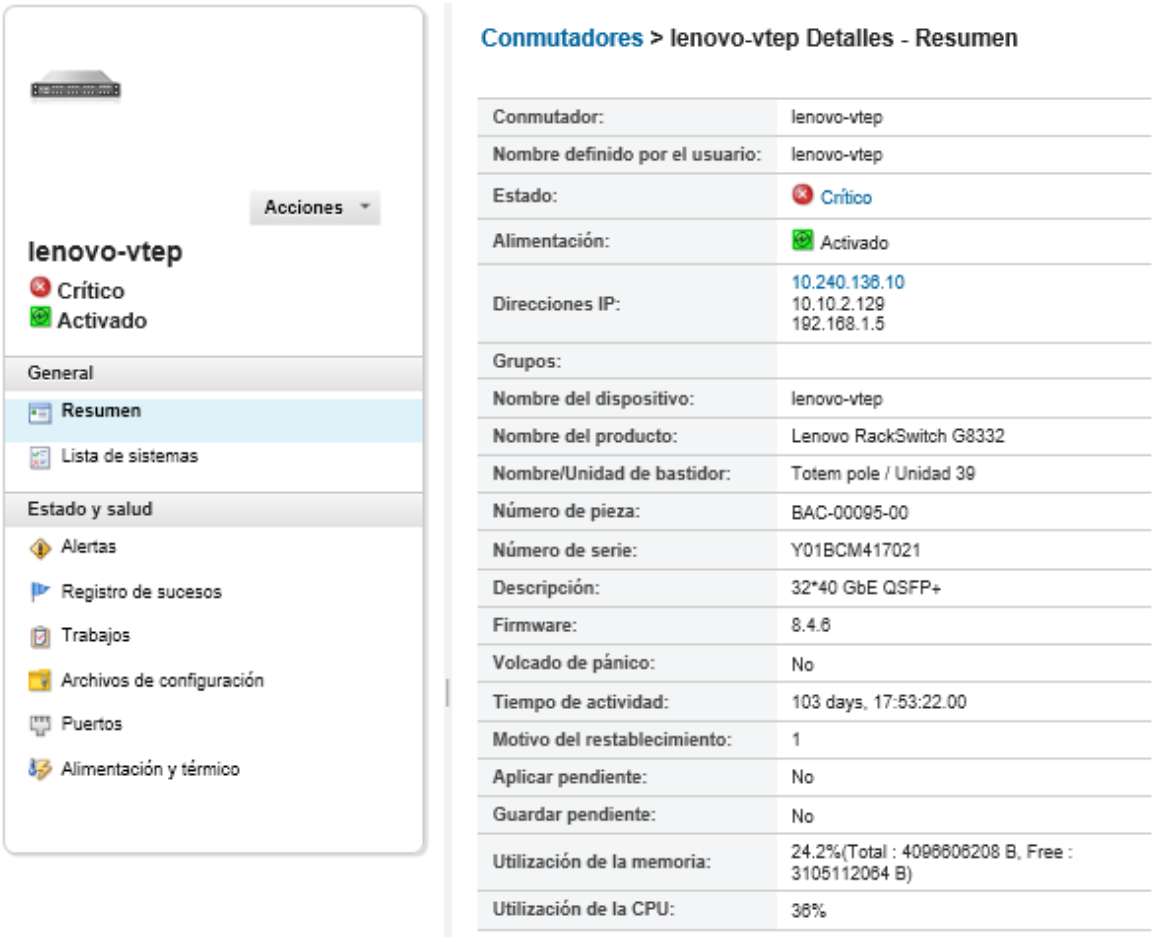
Procedimiento

Para ver los detalles de un conmutador específico gestionado mediante XClarity Administrator, lleve a cabo los pasos siguientes.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Hardware → Conmutadores**. Se muestra la página Conmutadores con una vista de tabla de todos los conmutadores que están instalados en el chasis gestionado.

Puede ordenar las columnas de la tabla para que sea más fácil encontrar los conmutadores que desea gestionar. Además, puede introducir texto (como un nombre o una dirección IP) en el campo **Filtro** para filtrar mejor los conmutadores que se muestran.

Paso 2. Haga clic en el conmutador en la columna **Conmutadores**. Se muestra la página Resumen con las propiedades y una lista de los componentes que están instalados en ese conmutador.



Paso 3. Complete uno o más de los siguientes pasos para ver la información detallada de inventario:

Nota: Algunos detalles puede que no estén disponible en todos los conmutadores.

- Haga clic en **Resumen** para ver un resumen del conmutador, incluidos la información del sistema y el firmware (consulte Visualización del estado de los dispositivos de almacenamiento).
- Haga clic en **Detalles del inventario** para ver detalles sobre los componentes del conmutador, incluidos:
  - Niveles de firmware para el conmutador
  - Detalles de la red del controlador de gestión, como nombre de host, dirección IPv4, dirección IPv6 y direcciones MAC
  - Detalles de activos del conmutador
- Haga clic en **Conectividad de E/S** para mostrar los detalles de la conectividad del conmutador seleccionado y los adaptadores de red asociados que están instalado en el conmutador.
- Pulse **Alertas** para mostrar las alertas en la lista de alertas que están relacionadas con el conmutador (consulte Trabajo con alertas).
- Pulse **Registro de sucesos** para mostrar los sucesos del registro de sucesos que están relacionados con el conmutador (consulte Trabajo con sucesos).
- Haga clic en **Archivos de configuración** para crear una copia de seguridad y restaurar la configuración del conmutador (consulte Creación de copia de seguridad y restauración de datos de configuración de conmutador).
- Haga clic en **Historial de implementación** para ver información acerca de las plantillas de configuración del conmutador que se desplegaron en el conmutador (consulte Visualización del historial de despliegue de la configuración del conmutador).
- Haga clic en **Trabajos** para mostrar los archivos de datos de configuración del conmutador (consulte Supervisión de trabajos).
- Haga clic en **Puertos** para mostrar el estado y la configuración de todos los puertos en un conmutador gestionado y para habilitar o deshabilitar puertos de conmutador.

  Nota: Para los conmutadores Flex, haga clic en el icono **Actualizar** ( ) para recopilar los datos de puerto actuales. La recopilación de datos puede durar varios minutos.
- Haga clic en **Light Path** para mostrar el estado actual de cada uno de los LED del conmutador.
- Haga clic en **Alimentación y térmico** para mostrar información acerca de la temperatura, el suministro de alimentación y los ventiladores.

  Consejo: para recopilar los datos de alimentación y térmicos más recientes, utilice el botón Actualizar de su navegador web. La recopilación de datos puede durar varios minutos.

Después de finalizar

Además de mostrar un resumen e información detallada sobre un conmutador, también puede realizar las siguientes acciones:

- Ver un conmutador Flex en una vista gráfica de bastidores o de chasis haciendo clic en **Acciones → Vistas → Mostrar en vista de bastidores** o **Acciones → Vistas → Mostrar en vista de chasis**.
- Ver un conmutador RackSwitch en una vista gráfica al hacer clic en **Acciones → Vistas → Mostrar en vista de bastidores**.
- Iniciar la interfaz web del controlador de gestión del conmutador al hacer clic en el vínculo **Dirección IP** (consulte Inicio de la interfaz del controlador de gestión para un conmutador).
- Inicie la consola SSH del conmutador (consulte Inicia una sesión SSH remota para un conmutador).
- Encender y apagar el conmutador (consulte Encendido y apagado de un conmutador).

- (Solo RackSwitch) Modifique la información del sistema al seleccionar un conmutador y después seleccionar **Editar propiedades**.
- Exportar información detallada acerca del conmutador a un archivo CSV pulsando **Acciones → Inventario → Exportar inventario**.

  Notas:

  – Para obtener más información sobre datos de inventario en el archivo CSV, consulte la GET /switches/*<UUID_list>* REST API en la documentación en línea de XClarity Administrator.

  – Al importar un archivo CSV en Microsoft Excel, Excel trata los valores de texto que contienen solo números como valores numéricos (por ejemplo, para UUID). Formatee cada celda como texto para corregir este error.
- Excluya los sucesos que no sean de su interés de todas las páginas en las que se muestran sucesos al hacer clic en el icono **Acciones → Restablecer servicio → Sucesos excluidos** (consulte Exclusión de sucesos).
- Solucione los problemas que puedan surgir entre el certificado de seguridad de XClarity Administrator y el certificado de seguridad del RackSwitch o el CMM del chasis en el que está instalado el conmutador Flex System al seleccionar un conmutador y hacer clic en **Acciones → Seguridad → Resolver certificados no fiables** (consulte Resolución de un certificado de servidor no fiable).

Encendido y apagado de un conmutador

Puede encender, apagar y reiniciar un conmutador Flex System o RackSwitch desde Lenovo XClarity Administrator.

Procedimiento

Lleve a cabo los pasos siguientes para encender o apagar un conmutador gestionado.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Hardware → Conmutadores**. Se muestra la página Conmutadores con una vista de tabla de todos los conmutadores que están instalados en el chasis gestionado.

Puede ordenar las columnas de la tabla para que sea más fácil encontrar los conmutadores que desea gestionar. Además, puede introducir texto (como un nombre o una dirección IP) en el campo **Filtro** para filtrar mejor los conmutadores que se muestran.

Paso 2. Seleccione el conmutador que debe encenderse, apagarse o reiniciarse.

Paso 3. Haga clic en **Todas las acciones** y, a continuación, haga clic en una de las siguientes acciones de alimentación:
- **Encendido** (únicamente conmutadores Flex System)

- **Apagado** (solo conmutadores Flex System)
- **Reinicio**. Una vez finalizadas todas las operaciones que se están ejecutando, se reinicia el conmutador. Las operaciones que se iniciaron mientras se reinicia el conmutador se rechazan.

Habilitar y deshabilitar puertos del conmutador

Puede habilitar o deshabilitar puertos específicos de un conmutador RackSwitch o Flex System.

Procedimiento

Para habilitar o deshabilitar puertos de conmutador, lleve a cabo los pasos siguientes.

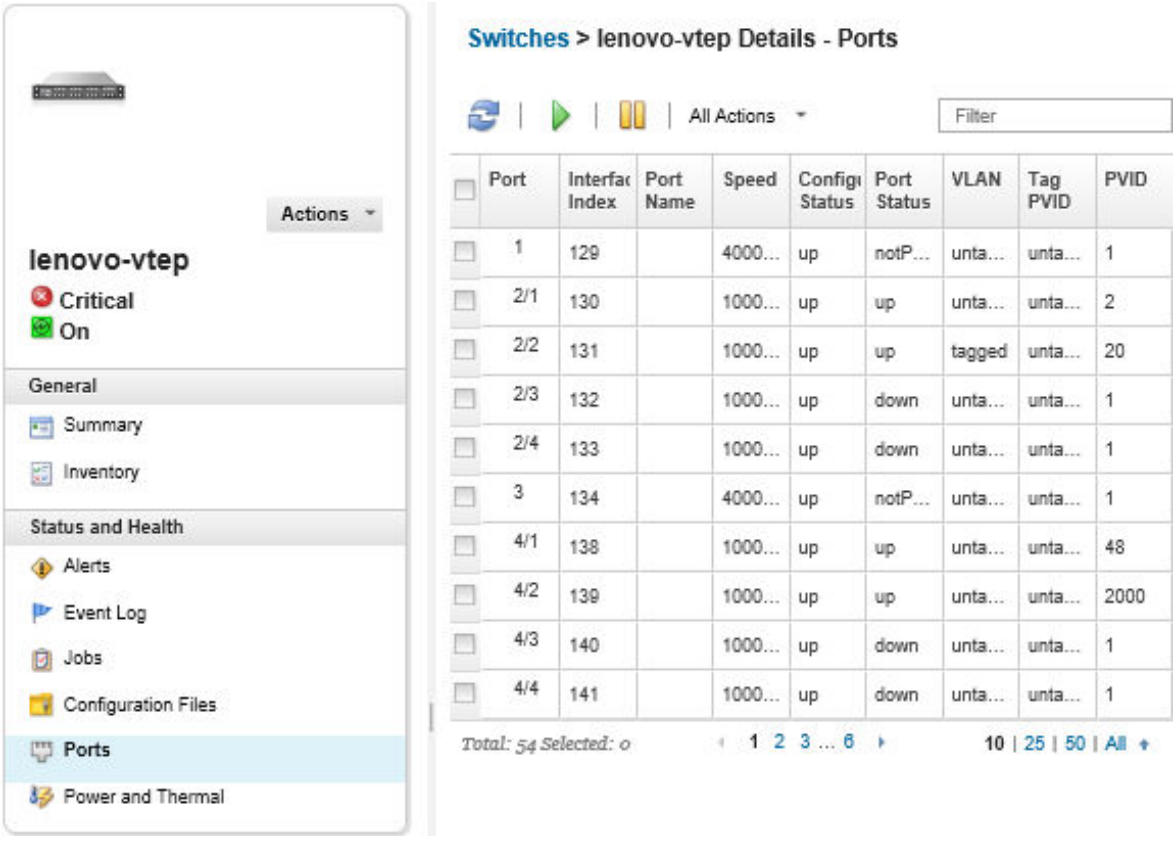
Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Hardware → Conmutadores**. Se muestra la página Conmutadores con una vista de tabla de todos los conmutadores que están instalados en el chasis gestionado.

Puede ordenar las columnas de la tabla para que sea más fácil encontrar los conmutadores que desea gestionar. Además, puede introducir texto (como un nombre o una dirección IP) en el campo **Filtro** para filtrar mejor los conmutadores que se muestran.

Paso 2. Haga clic en el conmutador en la columna **Conmutadores**. Se muestra la página Resumen con las propiedades y una lista de los componentes que están instalados en ese conmutador.

Paso 3. Haga clic en **Puertos** en el panel de navegación izquierdo para mostrar el estado y la configuración de todos los puertos en el conmutador:

Nota: Para los conmutadores Flex, haga clic en el icono **Actualizar** ( ) para recopilar los datos de puerto actuales. La recopilación de datos puede durar varios minutos



Paso 4. Seleccione el puerto y, a continuación, haga clic en el icono **Habilitar** ( ) o **Deshabilitar** ( ).

Creación de copia de seguridad y restauración de datos de configuración de conmutador

Puede usar Lenovo XClarity Administrator para crear copias de seguridad y restaurar los datos de configuración de conmutadores RackSwitch y Flex System. También puede exportar los archivos de configuración del conmutador a su sistema local e importar los archivos de configuración del conmutador en XClarity Administrator.

Creación de copia de seguridad de datos de configuración de conmutador

Puede realizar una copia de seguridad de los datos de configuración de un conmutador Flex System o RackSwitch. Durante la creación de copias de seguridad de un conmutador, los datos de configuración se importan desde el destino del conmutador a Lenovo XClarity Administrator como un archivo de datos de configuración de conmutador.

Procedimiento

Para crear una copia de seguridad de datos de configuración de un conmutador gestionado, lleve a cabo los pasos siguientes.

- Para un solo conmutador:
  1. En la barra de menús de XClarity Administrator, haga clic en **Hardware → Conmutadores**. Se muestra la página Conmutadores con una vista de tabla de todos los conmutadores que están instalados en el chasis gestionado.

Puede ordenar las columnas de la tabla para que sea más fácil encontrar los conmutadores que desea gestionar. Además, puede introducir texto (como un nombre o una dirección IP) en el campo **Filtro** para filtrar mejor los conmutadores que se muestran.

2. Haga clic en el conmutador en la columna **Conmutadores**. Se muestra la página Resumen con las propiedades y una lista de los componentes que están instalados en ese conmutador.
3. Haga clic en **Configuración** para ver los archivos de configuración del conmutador.
4. Haga clic en el icono **Crear una copia de seguridad de los datos de configuración** ( ) para crear una copia de seguridad de la configuración del conmutador.
5. (Opcional) Especifique un nombre para el archivo de configuración del conmutador.

   En dispositivos CNOS, el nombre de archivo puede contener caracteres alfanuméricos y los siguientes caracteres especiales: guion bajo (_), guiones (-) y punto (.). En conmutadores ENOS, el nombre de archivo puede contener caracteres alfanuméricos y cualquier caracter especial.

   Si no se especifica un nombre de archivo, se utiliza el siguiente nombre predeterminado: "*<nombre_de_conmutador>_<dirección_IP>_<marca_de_tiempo>*.cfg."
6. (Opcional) Agregue un comentario que describa la copia de seguridad.
7. Haga clic en **Crear copia de seguridad** crear una copia con datos de configuración del conmutador de inmediato, o bien haga clic en **Programación** para programar esta copia de seguridad para que se ejecute posteriormente.

   Si elige programar una copia de seguridad, puede seleccionar **Sobrescribir** para crear la copia de seguridad de los datos de configuración del conmutador en el mismo archivo en cada trabajo en ejecución, sobrescribiendo su contenido. Si elige no sobrescribir el archivo, se adjuntan los nombres de archivo de copias de seguridad posteriores con un número único (por ejemplo, MyBackup_33.cfg).

   Nota: Cuando programa una copia de seguridad, no puede elegir nombres de archivo dinámicos o comentarios para cada trabajo programado.

- Para varios conmutadores:
  1. En la barra de menús de XClarity Administrator, haga clic en **Hardware → Conmutadores**. Se muestra la página Conmutadores con una vista de tabla de todos los conmutadores que están instalados en el chasis gestionado.
  2. Seleccione uno o varios conmutadores.
  3. Haga clic en **Todas las acciones → Configuración → Configuración de copia de seguridad**.
  4. (Opcional) Especifique un nombre para el archivo de configuración del conmutador.

En dispositivos CNOS, el nombre de archivo puede contener caracteres alfanuméricos y los siguientes caracteres especiales: guion bajo (_), guiones (-) y punto (.). En conmutadores ENOS, el nombre de archivo puede contener caracteres alfanuméricos y cualquier caracter especial.

Si no se especifica un nombre de archivo, se utiliza el siguiente nombre predeterminado: "<*nombre_de_conmutador*>_<*dirección_IP*>_<*marca_de_tiempo*>.cfg."

5. (Opcional) Agregue un comentario que describa la copia de seguridad.
6. Haga clic en **Crear copia de seguridad** crear una copia con datos de configuración del conmutador de inmediato, o bien haga clic en **Programación** para programar esta copia de seguridad para que se ejecute posteriormente.

   Si elige programar una copia de seguridad, puede seleccionar **Sobrescribir** para crear la copia de seguridad de los datos de configuración del conmutador en el mismo archivo en cada trabajo en ejecución, sobrescribiendo su contenido. Si elige no sobrescribir el archivo, se adjuntan los nombres de archivo de copias de seguridad posteriores con un número único (por ejemplo, MyBackup_33.cfg).

   Nota: Cuando programa una copia de seguridad, no puede elegir nombres de archivo dinámicos o comentarios para cada trabajo programado.

Después de finalizar

Una vez completado el proceso de copia de seguridad, el archivo de configuración del conmutador se agrega a la pestaña **Archivos de configuración** en la página de detalles del conmutador.

Desde esta página, también puede realizar las acciones siguientes en un archivo de configuración de conmutador seleccionado:

- Restaurar la configuración del conmutador al seleccionar el archivo de configuración del conmutador y al hacer clic en el icono **Restaurar datos de configuración** ( ).
- Eliminar archivos de configuración del conmutador de XClarity Administrator al hacer clic en el icono **Eliminar** ( ).
- Exportar archivos de configuración del conmutador a su sistema local al seleccionar los archivos y al hacer clic en el icono **Archivo de configuración de exportación** ( ).
- Importar los archivos de configuración del conmutador a XClarity Administrator al hacer clic en el icono **Importar archivo de configuración** ( ).

Restauración de datos de configuración de conmutador

Puede restaurar los datos de configuración de los cuales se haya creado una copia de seguridad o que se hayan importado en Lenovo XClarity Administrator para conmutadores Flex System o RackSwitch. El archivo de configuración del conmutador se descarga desde XClarity Administrator al conmutador de destino y la configuración se lleva a cabo automáticamente.

Los archivos de configuración se asocian con un conmutador específico. Puede restaurar un archivo de configuración solo en el conmutador con el que está asociado. No se puede utilizar una copia de seguridad de un archivo de configuración que se creó para un conmutador con el fin de restaurar la configuración de otro conmutador.

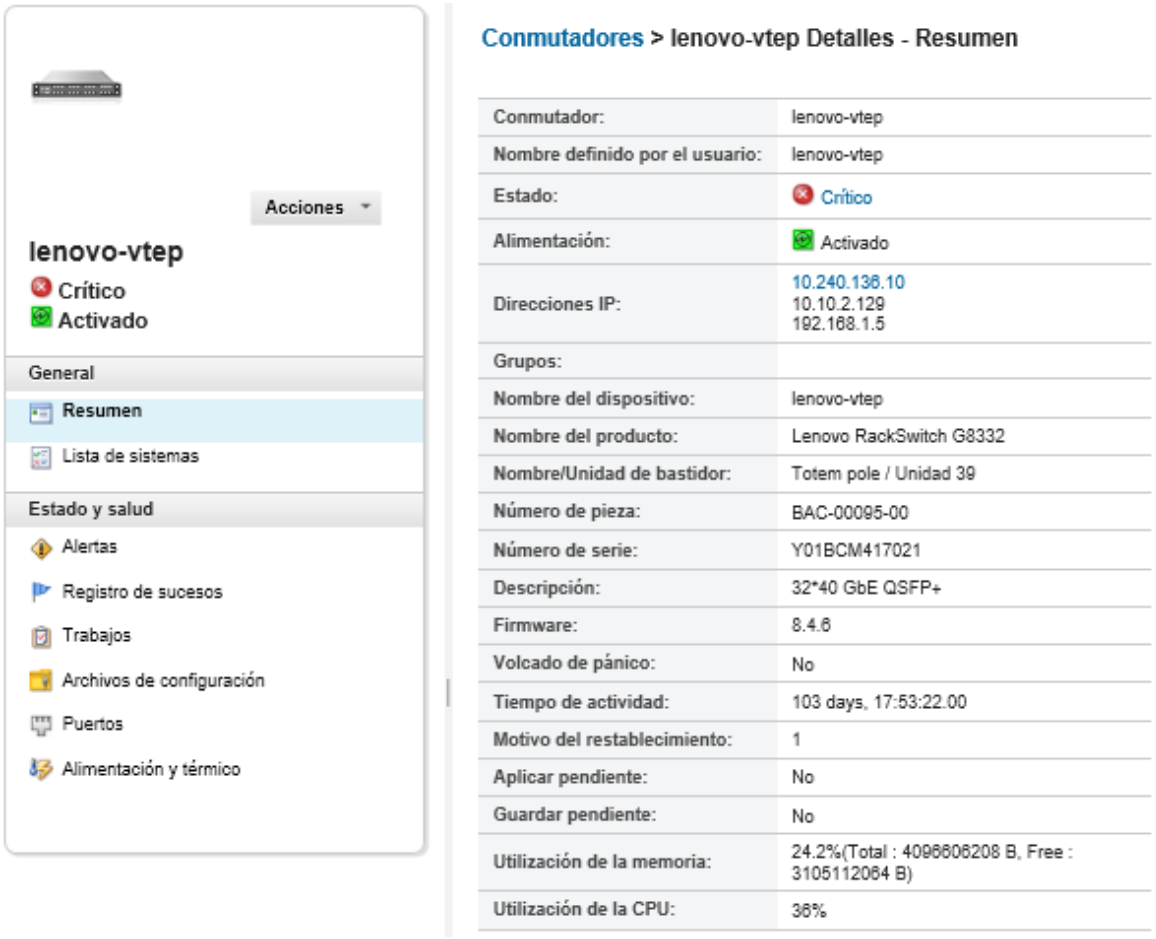
Procedimiento

Para restaurar los datos de configuración de un conmutador gestionado, lleve a cabo los pasos siguientes.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Hardware → Conmutadores**. Se muestra la página Conmutadores con una vista de tabla de todos los conmutadores que están instalados en el chasis gestionado.

Puede ordenar las columnas de la tabla para que sea más fácil encontrar los conmutadores que desea gestionar. Además, puede introducir texto (como un nombre o una dirección IP) en el campo **Filtro** para filtrar mejor los conmutadores que se muestran.

Paso 2. Haga clic en el conmutador en la columna **Conmutadores**. Se muestra la página Resumen con las propiedades y una lista de los componentes que están instalados en ese conmutador.



Paso 3. Haga clic en **Archivos de configuración** para ver los archivos de configuración del conmutador.

Paso 4. Seleccione el archivo de configuración que desee restaurar en el conmutador y pulse el icono **Restaurar datos de configuración** (). Se muestra el cuadro de diálogo Restaurar.

Paso 5. (Solo conmutadores que ejecuten CNOS) Elija si desea que se reinicie el conmutador, después de finalizar la operación de restauración.

Si elige no reiniciar el conmutador automáticamente, debe reiniciar el conmutador CNOS manualmente para activar los datos de configuración restaurados. Si espera demasiado tiempo y ocurre una operación de guardado (por ejemplo, si un puerto está habilitado o deshabilitado), se anula la operación de restauración y se utilizan los datos de configuración de ejecución.

Paso 6. Haga clic en **Restaurar** para restaurar con datos de configuración en el conmutador de inmediato, o bien haga clic en **Programación** para programar esta tarea de restauración para que se ejecute posteriormente.

Nota: Tenga cuidado cuando programe un trabajo de restauración periódico. Si el conmutador se restablece a una configuración anterior, compruebe la página Trabajos programados para los trabajos de restauración programados.

Exportación e importación de archivos de configuración del conmutador

También puede exportar archivos de configuración del conmutador a su sistema local e importar archivos de configuración del conmutador en Lenovo XClarity Administrator.

Procedimiento

Para crear una copia de seguridad de datos de configuración de un conmutador gestionado, lleve a cabo los pasos siguientes.

- Exportar archivos de configuración de conmutador
  1. En la barra de menús de XClarity Administrator, haga clic en **Hardware → Conmutadores**. Se muestra la página Conmutadores con una vista de tabla de todos los conmutadores que están instalados en el chasis gestionado.

     Puede ordenar las columnas de la tabla para que sea más fácil encontrar los conmutadores que desea gestionar. Además, puede introducir texto (como un nombre o una dirección IP) en el campo **Filtro** para filtrar mejor los conmutadores que se muestran.

  2. Haga clic en el conmutador en la columna **Conmutadores**. Se muestra la página Resumen con las propiedades y una lista de los componentes que están instalados en ese conmutador.
  3. Haga clic en **Configuración** para ver los archivos de configuración del conmutador.
  4. Seleccione los archivos de configuración de conmutador para exportar.

5. Haga clic en el icono **Exportar archivo de configuración** ( ) para crear una copia de seguridad de la configuración del conmutador.

- Importar archivos de configuración de conmutador
  1. En la barra de menús de XClarity Administrator, haga clic en **Hardware → Conmutadores**. Se muestra la página Conmutadores con una vista de tabla de todos los conmutadores que están instalados en el chasis gestionado.

     Puede ordenar las columnas de la tabla para que sea más fácil encontrar los conmutadores que desea gestionar. Además, puede introducir texto (como un nombre o una dirección IP) en el campo **Filtro** para filtrar mejor los conmutadores que se muestran.

  2. Haga clic en el conmutador en la columna **Conmutadores**. Se muestra la página Resumen con las propiedades y una lista de los componentes que están instalados en ese conmutador.
  3. Haga clic en **Configuración** para ver los archivos de configuración del conmutador.
  4. Haga clic en el icono **Importar archivo de configuración** ( ) para crear una copia de seguridad de la configuración del conmutador.
  5. Ingrese el nombre del archivo de configuración de conmutador o haga clic en **Examinar** para buscar el archivo de arranque que desea importar.
  6. **Opcional:** Escriba una descripción para el archivo de configuración del conmutador.
  7. Haga clic en **Importar**.

     Si cierra la pestaña del navegador web o la ventana en la que se está cargando el archivo antes de que finalice el proceso, la importación fallará.

Inicio de la interfaz del controlador de gestión para un conmutador

Puede iniciar la interfaz web del controlador de gestión de un RackSwitch o Flex System que ejecuta ENOS desde Lenovo XClarity Administrator.

Procedimiento

Lleve a cabo los pasos siguientes para iniciar la interfaz del controlador de gestión de un conmutador.

Nota: No se admite el inicio de ninguna interfaz web del controlador de gestión desde XClarity Administrator mediante el navegador web Safari.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Hardware → Conmutadores**. Se muestra la página Conmutadores con una vista de tabla de todos los conmutadores que están instalados en el chasis gestionado.

Puede ordenar las columnas de la tabla para que sea más fácil encontrar los conmutadores que desea gestionar. Además, puede introducir texto (como un nombre o una dirección IP) en el campo **Filtro** para filtrar mejor los conmutadores que se muestran.

Paso 2. Seleccione el conmutador y haga clic en **Todas las acciones → Iniciar → Interfaz web de gestión**. Se muestra la interfaz web del controlador de gestión del conmutador.

Consejo: también puede iniciar la interfaz del controlador de gestión pulsando el enlace de la **dirección IP** que se muestra en la columna Dirección IP y en las páginas de resumen y detalles del conmutador.

Paso 3. Inicie sesión en la interfaz del controlador de gestión.

Consejo: para conmutadores Flex, utilice sus credenciales de usuario de XClarity Administrator. Para conmutadores XClarity Administrator, use las credenciales del conmutador.

Inicia una sesión SSH remota para un conmutador

Puede iniciar una sesión SSH remota para un conmutador RackSwitch o Flex gestionado desde Lenovo XClarity Administrator. En la sesión SSH remota, puede utilizar la interfaz de línea de mandatos para realizar las tareas de gestión que no son proporcionadas por XClarity Administrator.

Antes de empezar

Asegúrese de que el conmutador esté configurado para habilitar SSH. Para los conmutadores RackSwitch, se habilita SSH cuando el conmutador está gestionando por XClarity Administrator. Para los conmutadores Flex, SSH está habilitado generalmente de forma predeterminada. Si no está habilitado, se debe habilitar SSH antes de que el conmutador se gestione mediante XClarity Administrator.

Procedimiento

Lleve a cabo los pasos siguientes para iniciar una sesión SSH remota para un conmutador gestionado.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Hardware → Conmutadores**. Se muestra la página Conmutadores con una vista de tabla de todos los conmutadores que están instalados en el chasis gestionado.

Puede ordenar las columnas de la tabla para que sea más fácil encontrar los conmutadores que desea gestionar. Además, puede introducir texto (como un nombre o una dirección IP) en el campo **Filtro** para filtrar mejor los conmutadores que se muestran.

Paso 2. Seleccione el conmutador para iniciar una sesión SSH.

Paso 3. Pulse **Todas las acciones → Iniciar → Consola de SSH**.

Paso 4. Si es necesario, inicie sesión en el conmutador utilizando su Id. de usuario y la contraseña.

Modificación de las propiedades del sistema de un conmutador

Puede modificar las propiedades del sistema de un conmutador Flex System o RackSwitch específico.

Procedimiento

Lleve a cabo los pasos siguientes para modificar las propiedades del sistema.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Hardware → Conmutadores** para mostrar la página Conmutadores.

Paso 2. Seleccione el conmutador que se va a actualizar.

Paso 3. Haga clic en **Todas las acciones → Inventario → Editar propiedades**para mostrar el cuadro de diálogo Editar.

Paso 4. Cambie la siguiente información según sea necesario.

- Nombre del conmutador
- Contacto de soporte
- Descripción

Nota: Las propiedades de ubicación, sala, bastidor y unidad de bastidor más baja se actualizan mediante XClarity Administrator cuando se agregan o quitan dispositivos de un bastidor en la interfaz web (consulte Gestión de bastidores).

Paso 5. Haga clic en **Guardar**.

Nota: Al cambiar estas propiedades, pueden transcurrir unos instantes antes de que los cambios aparezcan en la interfaz web de XClarity Administrator.

Resolución de credenciales almacenadas caducadas o no válidas para un conmutador

Cuando una credencial almacenada caduca o deja de funcionar en un dispositivo, el estado de ese dispositivo pasa a ser “Fuera de línea.”

Procedimiento

Para resolver una credencial almacenada caducada o no válida para un conmutador, lleve a cabo los siguientes pasos.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Hardware → Conmutadores**. Se muestra la página Conmutadores con una vista de tabla de todos los conmutadores gestionados.

Paso 2. Haga clic en el encabezado de la columna **Alimentación** para agrupar todos los conmutadores fuera de línea en la parte superior de la tabla.

Puede ordenar las columnas de la tabla para que sea más fácil encontrar el conmutador que desea gestionar. Además, puede introducir texto (como un nombre de sistema o una dirección IP) en el campo **Filtro** para filtrar mejor los conmutadores que se muestran.

Paso 3. Seleccione el conmutador que va a resolver.

Paso 4. Haga clic en **Todas las acciones → Seguridad → Edtiar las credenciales almacenadas**.

Paso 5. Cambie la contraseña de la credencial almacenada o seleccione otra credencial almacenada a utilizar en el dispositivo gestionado.

Nota: Si gestionó más de un dispositivo utilizando las mismas credenciales almacenadas y cambiar la contraseña de las credenciales almacenadas, la cambiar la contraseña afecta a todos los dispositivos que estén utilizando las credenciales almacenadas.

Recuperación de la gestión con un conmutador tras un error de servidor de gestión

Puede recuperar la gestión de un conmutador cuya gestión no se anuló correctamente (por ejemplo, debido a problemas de conectividad durante la anulación de gestión o por un error de la gestión de Lenovo XClarity Administrator).

Procedimiento

- Gestione el conmutador de nuevo utilizando la opción **Forzar gestión** (consulte Gestión de conmutadores).
- Para quitar de forma permanente la configuración específica de XClarity Administrator en un conmutador cuya gestión no se anuló correctamente y no se volverá a gestionar, lleve a cabo estos pasos.
  - Gestione el conmutador de nuevo utilizando la opción **Forzar gestión** (consulte Gestión de conmutadores) y luego anule la gestión del conmutador para borrar la configuración (consulte Dejar de gestionar un conmutador).
  - (ENOS) Inicie sesión en el conmutador utilizando el puerto de consola del conmutador o un SSH o la sesión de Telnet y ejecute los siguientes comandos de configuración en el orden especificado para borrar la configuración del conmutador.

```
no snmp-server access 32
no snmp-server group 16
no snmp-server notify 16
no snmp-server target-parameters 16
no snmp-server target-address 16
no snmp-server user 16
```

Dejar de gestionar un conmutador

Puede quitar un conmutador de la gestión mediante Lenovo XClarity Administrator. Este proceso se denomina *anular la gestión* (no gestionar).

Antes de empezar

Puede habilitar XClarity Administrator para que se anule automáticamente la gestión de los dispositivos que están fuera de línea durante un período de tiempo específico. Esto está deshabilitado de forma predeterminada. Para habilitar la anulación automática de gestión de dispositivos fuera de línea, haga clic en **Hardware → Detectar y gestionar dispositivos nuevos** en el menú de XClarity Administrator y, a continuación, haga clic en **Editar**, ubicado junto a la opción **No gestionar los dispositivos fuera de línea está Deshabilitado**. A continuación, seleccione **Habilitar dispositivos no gestionados fuera de línea** y establezca el intervalo de tiempo. De manera predeterminada, se anula la gestión de los dispositivos después de estar fuera de línea durante 24 horas.

Antes de eliminar la gestión de un conmutador, asegúrese de que no hay trabajos activos en ejecución en el conmutador.

Acerca de esta tarea

Cuando se anula la gestión de un conmutador, XClarity Administrator conserva determinada información sobre el conmutador. Esta información se vuelve a aplicar cuando se gestiona de nuevo el mismo conmutador.

Consejo: todos los dispositivos de demostración que se añaden opcionalmente durante la configuración inicial son nodos en un chasis. Para anular la gestión de los dispositivos de demostración, anule la gestión

del chasis utilizando la opción **Forzar anulación de gestión incluso si no se puede acceder al dispositivo**.

Procedimiento

Para anular la gestión de un conmutador, lleve a cabo los pasos siguientes.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Hardware → Conmutadores** para mostrar la página Conmutadores.

Paso 2. Seleccione uno o más conmutadores de las listas de conmutadores gestionados.

Paso 3. Haga clic en **No gestionar conmutador**. Se muestra el cuadro de diálogo No gestionar.

Paso 4. **Opcional:** seleccione **Forzar anulación de gestión aunque el dispositivo no esté accesible**.

Importante: Asegúrese de seleccionar esta opción si está anulando la gestión de un hardware de demostración.

Paso 5. Haga clic en **No gestionar**.El cuadro de diálogo No gestionar muestra el progreso de cada paso en el proceso de anulación de la gestión.

Paso 6. Cuando el proceso de anulación de la gestión esté completo, pulse **Aceptar**.

Recuperación de un conmutador en el que no se ha anulado la gestión correctamente

Si un conmutador se gestiona mediante Lenovo XClarity Administrator y XClarity Administrator produce un error, puede recuperar las funciones de gestión cuando el servidor de gestión se restaure o se sustituya.

Procedimiento

- Gestione el conmutador de nuevo utilizando la opción **Forzar gestión** (consulte Gestión de conmutadores).
- Para quitar de forma permanente la configuración específica de XClarity Administrator en un conmutador cuya gestión no se anuló correctamente y no se volverá a gestionar, lleve a cabo estos pasos.
  - Gestione el conmutador de nuevo utilizando la opción **Forzar gestión** (consulte Gestión de conmutadores) y luego anule la gestión del conmutador para borrar la configuración (consulte Dejar de gestionar un conmutador).
  - (ENOS) Inicie sesión en el conmutador utilizando el puerto de consola del conmutador o un SSH o la sesión de Telnet y ejecute los siguientes comandos de configuración en el orden especificado para borrar la configuración del conmutador.

```
no snmp-server access 32
no snmp-server group 16
no snmp-server notify 16
no snmp-server target-parameters 16
no snmp-server target-address 16
no snmp-server user 16
```

Capítulo 11. Configuración de servidores mediante el uso de patrones de configuración

Los patrones de servidores se utilizan para aprovisionar o preaprovisionar varios servidores (servidores de bastidor y de torre y nodos de cálculo) desde un solo conjunto de valores de configuración definidos.

Más información:

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

Antes de empezar

Después de que la prueba gratuita de 90 días termine, puede continuar utilizando XClarity Administrator para gestionar y supervisar el hardware de manera gratuita; sin embargo, debe comprar licencias de habilitación de todas las funciones para cada servidor gestionado que admita las funciones avanzadas de XClarity Administrator para continuar usando la función de configuración del servidor. Lenovo XClarity Pro proporciona titularidad para servicios y soporte y la licencia rehabilitación de funciones completas. Para obtener más información acerca de cómo adquirir Lenovo XClarity Pro, póngase en contacto con su representante de Lenovo o un business partner autorizado. Para obtener más información, consulte Instalación de licencia de habilitación de funciones completas en la XClarity Administrator documentación en línea.

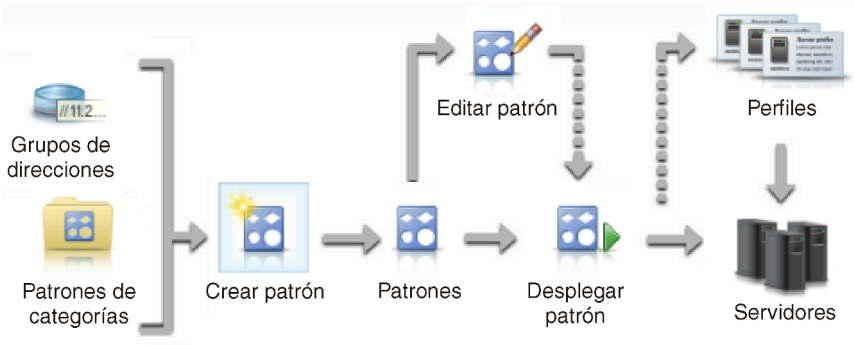
Revise Consideraciones sobre la configuración para ver información importante acerca de la compatibilidad de la configuración para servidores y dispositivos específicos.

Acerca de esta tarea

Puede utilizar patrones de servidor en XClarity Administrator para configurar el almacenamiento local, los adaptadores de E/S, el orden de arranque y otros valores del controlador de gestión de la placa base y de Unified Extensible Firmware Interface (UEFI) en servidores gestionados. Los patrones de servidor también integran el soporte para la virtualización de direcciones de E/S, de modo que puede virtualizar conexiones de malla del servidor o readaptar servidores sin interrupciones en la malla. También puede iniciar solicitudes de cambio de zonas de SAN antes de recibir nuevo hardware virtualizando (preconfigurando) las direcciones de Fibre Channel.

Procedimiento

En la siguiente figura se ilustra el flujo de trabajo para configurar servidores gestionados. Las flechas sólidas indican las acciones que usted realiza. Las flechas punteadas indican acciones que se realizan automáticamente mediante XClarity Administrator.



Paso 1. **Crear grupos de direcciones.**Un *grupo de direcciones* es un conjunto de rangos de direcciones definido. Lenovo XClarity Administrator utiliza grupos de direcciones para asignar direcciones IP y de E/S a servidores individuales cuando los patrones de servidor se despliegan en dichos servidores.

Para obtener información acerca de cómo crear grupos de direcciones, consulte Definición de grupos de direcciones

Paso 2. **Crear patrones de categorías.**

Un *patrón de categoría* agrupa valores de firmware relacionados y se puede reutilizar en varios patrones de servidor. Puede crear patrones para las siguientes categorías de firmware:

- Información del sistema
- Interfaces de gestión
- Dispositivos y puertos de E/S
- Destinos de arranque FC
- Puertos de adaptador de E/S

Para obtener más información acerca de los patrones de categorías, consulte Trabajo con patrones de servidor

Paso 3. **Crear un patrón de servidor.**

Un *patrón de servidor* representa configuraciones de servidor anteriores al SO, incluidos la configuración del almacenamiento local, la configuración de los adaptadores de E/S, los valores de arranque y otros valores de firmware del controlador de gestión de la placa base y de la UEFI. Un patrón de servidor se utiliza como patrón general para configurar rápidamente varios servidores a la vez.

Puede definir varios patrones de servidor para representar las distintas configuraciones que se utilizarán en su centro de datos.

Al definir un patrón de servidor, seleccione patrones de categorías y grupos de dirección según sea necesario para construir la configuración deseada para un grupo de servidores específico. Un patrón de categoría agrupa valores de configuración relacionados que se pueden reutilizar en varios patrones de servidor.

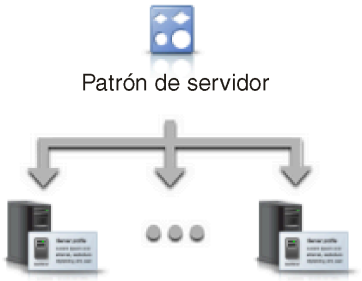
Puede crear un patrón de servidor desde cero para servidores convergidos, Flex System, NeXtScale y System x a fin de definir la configuración deseada antes de que se reciba el hardware. O bien puede crear un patrón de servidor a partir de un servidor gestionado existente. Cuando se crea un patrón de servidor a partir de un servidor existente, XClarity Administrator extrae patrones de categorías del servidor seleccionado.

Para obtener más información sobre la creación de patrones de servidor, consulte Creación de un patrón de servidor.

Paso 4. **Desplegar el patrón de servidor.**

Puede desplegar un patrón de servidor en uno o más servidores individuales o en grupos de servidores. Por ejemplo, puede desplegar un patrón de servidor en un chasis de modo que todos los nodos de cálculo de ese chasis se configuren igual. Durante el despliegue, XClarity Administrator crea un perfil de servidor para cada servidor en el que se ha desplegado el patrón de servidor. Cada *perfil de servidor* representa la configuración específica de un solo servidor. Hereda valores del patrón de servidor y contiene también información específica del servidor (como las direcciones IP y las direcciones MAC asignadas). Debido a que el perfil de servidor hereda los valores del patrón de servidor, si hace cambios en el patrón de servidor, los cambios se actualizan

automáticamente en el perfil de servidor. De esta forma, puede mantener configuraciones comunes en un solo lugar.



Nota: Es posible que los valores en un servidor dejen de ajustarse a la conformidad con el perfil de servidor si se cambia la configuración sin utilizar patrones de configuración o si se produjo un problema durante el despliegue, como un problema con el firmware o una configuración no válida. Puede determinar el estado de cumplimiento de cada servidor desde la página Patrones de configuración: Perfiles de servidor.

Puede desplegar un patrón de servidor en:

- **Servidores existentes**. Se crea un perfil de servidor para cada servidor. El perfil de servidor se activa después de que el servidor asociado se haya rearrancado.
- **Bahías vacías en un chasis existente**. Se crea un perfil de servidor para bahía vacía. A continuación, una vez que el nodo de cálculo se haya instalado físicamente, se podrá activar el perfil de servidor que esté asociado a la bahía vacía.
- **Espacio reservado para un chasis que aún no tiene**. Puede preaprovisionar los nodos de cálculo en un chasis que aún no tiene definido un *chasis de espacio reservado* para que actúe como destino del patrón de servidor antes de que llegue el hardware. El chasis de espacio reservado empaqueta todos los perfiles de servidor que se crean para cada bahía de nodos de cálculo vacía. De este modo, cuando llega el hardware, puede asignar los perfiles de servidor a todos los nodos de cálculo en el nuevo chasis desplegando el chasis de espacio reservado en el nuevo chasis. Cada perfil de servidor se activa después de que el nodo de cálculo se haya rearrancado.

Nota: Puede desplegar un patrón de servidor en varios servidores; sin embargo, no se pueden desplegar varios patrones en un solo servidor.

Para obtener más información acerca de cómo desplegar un patrón de servidor, consulte Despliegue de un patrón de servidor en un servidor y Despliegue de un chasis de espacio reservado

Paso 5. **Editar el patrón de servidor.**

Puede utilizar patrones de servidor para controlar una configuración común desde un solo lugar. Ya no tiene que actualizar los valores directamente en los servidores. En su lugar, puede actualizar los patrones de categorías y los patrones de servidor y los cambios se despliegan automáticamente en todos los perfiles asociados y sus servidores.

Para obtener más información acerca de cómo editar un patrón de servidor, consulte Modificación de un patrón de servidor

Consideraciones sobre la configuración

Antes de empezar a configurar servidores mediante Lenovo XClarity Administrator, tenga en cuenta las siguientes consideraciones importantes.

- Si un perfil de servidor incluye niveles de firmware anteriores y actualiza el firmware con niveles posteriores, XClarity Administrator compara los valores del perfil almacenados con los valores del servidor e informa los estados “No conforme”. Sitúe el cursor por encima del estado “No conforme” para determinar el motivo del no cumplimiento.

  Si selecciona los dispositivos y pulsa **Todas las acciones → Hacer cumplir los requisitos**, puede cambiar manualmente el estado de los dispositivos “no conforme” a “conforme” sin volver a desplegar el perfil.
- Después de actualizar el firmware (como UEFI, BMC o controladores de E/S) en un servidor, algunas configuraciones pueden cambiar (por ejemplo, al añadir nuevos elementos, eliminar elementos existentes o cambiar los comportamientos o el rango de valores de un elemento). Como resultado, es posible que el perfil de servidor se vuelva no conforme o que la aplicación del patrón de servidor falle si se crea utilizando un nivel de firmware anterior. En este caso, se recomienda que elija un nuevo patrón basado en el firmware actualizado o que edite el patrón con error para excluir la configuración de elementos específicos y, a continuación, aplicar ese patrón al servidor.
- El adaptador QLogic 8200 2-Port 10GbE SFP+ VFA tiene valores no válidos para estos valores: iSCSIFirstTargetParameters_iSCSIName, iSCSISecondTargetParameters_iSCSIName y IPv6LinkLocalAddress. Debe corregir manualmente estos valores en la configuración del sistema antes de conocer el patrón de configuración del servidor o corregir los valores del patrón de configuración aprendida.
- Para los nodos de cálculo Flex Systems System x240 y x440 con adaptadores RAID integrados, los patrones de servidor que definen las configuraciones RAID pueden desplegarse solo en uno o varios servidores que no tengan configuraciones RAID existentes. Si un patrón de servidor se despliega en un servidor que tiene una configuración RAID existente, las matrices y los volúmenes existentes no se sobrescriben. Para aplicar la configuración RAID que se define en el patrón de servidor, en primer lugar debe borrar la configuración RAID existente del servidor (consulte Restablecer adaptadores de almacenamiento a los valores predeterminados) y, a continuación, volver a desplegar el perfil de servidor seleccionando el servidor y pulsando **Más → Desplegar perfil de servidor**.
- Los controladores de almacenamiento incorporados en Flex System x220, Flex System x222 y los servidores ThinkSystem admiten software basado en RAID. Sin embargo, no admiten la configuración de software RAID mediante patrones de configuración.
- Al configurar RAID mediante Patrones de configuración, si el servidor está apagado, el servidor arranca automáticamente a la configuración de BIOS/UEFI antes de activar el perfil de servidor.
- Para los servidores ThinkServer, no se admite Patrones de configuración.
- Algunos dispositivos de E/S no se pueden configurar usando patrones de servidor. Para obtener más información, consulte el apartado Soporte de XClarity Administrator: página web de compatibilidad.
- Si ha habilitado características avanzadas (tales como SPAR, Easy Connect y la pila) en los conmutadores Flex EN4093R, CN4093, SI4093 o SI4091, puede que las configuraciones de red no se apliquen correctamente en los puertos internos.
- De manera predeterminada, el conmutador Flex SI4093 se entrega con SPAR habilitado. Si desea desplegar los valores de red en puertos internos de estos conmutadores utilizando patrones de puerto, debe quitar manualmente los puertos internos del conmutador de SPAR o quitar las configuraciones SPAR del conmutador.
- Se recomienda *no* usar XClarity Administrator para configurar los dispositivos Converged y ThinkAgile utilizando patrones de configuración.

- Asegúrese de que estén habilitados todos los puertos disponibles en los adaptadores instalados antes de crear los patrones de configuración desde un servidor existente, de modo que todos los puertos y valores disponibles se incluyan en el patrón. A continuación, de ser necesario, puede deshabilitar cualquier puertos utilizando los valores adecuados definidos en el patrón. Si los puertos se deshabilitan cuando se crea el patrón, puede que este no cree correctamente y que no pueda desplegarse correctamente.

Definición de grupos de direcciones

Un *grupo de direcciones* es un conjunto de rangos de direcciones definido. Lenovo XClarity Administrator utiliza grupos de direcciones para asignar direcciones IP y de E/S a servidores individuales cuando los patrones de servidor se despliegan en dichos servidores.

Acerca de esta tarea

XClarity Administrator admite grupos de direcciones IP y grupos de direcciones de E/S.

Grupos de direcciones IP

Los *grupos de direcciones IP* definen rangos de direcciones IP para utilizarlos al configurar la interfaz de red del controlador de gestión de la placa base de sus servidores. Puede utilizar grupos de direcciones predefinidos o personalizarlos, o bien puede crear nuevos grupos, según sea necesario. Al crear patrones de servidor, puede elegir qué grupo de direcciones IP se va a utilizar durante el despliegue. Cuando se despliega el patrón de servidor, las direcciones IP se distribuyen desde el grupo seleccionado y se asignan a los controladores de gestión de servidores individuales.

Nota: Si está satisfecho con la configuración de la red del controlador de gestión, no utilice esta opción.

Atención:

- Asegúrese de que selecciona un subrango de direcciones IP que no esté en conflicto con las direcciones de E/S existentes en su centro de datos.
- Asegúrese de que las direcciones IP de los rangos especificados forman parte de la misma subred y de que se puede acceder a ellos mediante XClarity Administrator.
- Asegúrese de que las direcciones IP de los rangos especificados son únicas para cada dominio de XClarity Administrator y las herramientas de gestión de IP existentes para evitar conflictos de direcciones.

El rango global de grupos de direcciones se deriva de la longitud del prefijo de direccionamiento especificado y la puerta de enlace o rango inicial. Puede crear grupos de distintos tamaños basados en la longitud del prefijo de direccionamiento especificado, pero los rangos de grupos globales deben ser únicos dentro del dominio de XClarity Administrator. Los rangos se crean a continuación desde el rango de grupos global.

Los rangos de direcciones pueden utilizarse para separar hosts (por ejemplo, por tipo de sistema operativo, tipos de carga de trabajo y tipo de negocio). Los rangos de direcciones también pueden estar ligados a las reglas de red de la organización.

Grupos de direcciones de Ethernet

Los *grupos de direcciones de Ethernet* son colecciones de direcciones MAC únicas que pueden asignarse a los adaptadores de red al configurar servidores. Puede utilizar grupos de direcciones predefinidos o personalizarlos según sea necesario, o bien puede crear nuevos grupos. Al crear patrones de servidor, puede elegir qué grupo de direcciones de Fibre Channel se va a utilizar durante el despliegue. Cuando se despliega el patrón de servidor, las direcciones se distribuyen desde el grupo seleccionado y se asignan a puertos de adaptadores individuales.

Está disponible el siguiente grupo de direcciones MAC predefinido:
- Grupo de direcciones MAC de Lenovo

Para obtener una lista de los rangos de direcciones MAC de este grupo, consulte Grupos de direcciones de Ethernet (MAC).

Grupos de direcciones de Fibre Channel

Los *grupos de direcciones de Fibre Channel* son colecciones de direcciones únicas WWNN y WWPN que pueden asignarse a los adaptadores de Fibre Channel al configurar servidores. Puede utilizar grupos de direcciones predefinidos o personalizarlos según sea necesario, o bien puede crear nuevos grupos. Al crear patrones de servidor, puede elegir qué grupo de direcciones de Fibre Channel se va a utilizar durante el despliegue. Cuando se despliega el patrón de servidor, las direcciones se distribuyen desde el grupo seleccionado y se asignan a puertos de adaptadores individuales.

Están disponibles los siguientes grupos de direcciones de Fibre Channel predefinidos:
- LenovoDirecciones WWN
- BrocadeDirecciones WWN
- EmulexDirecciones WWN
- QLogicDirecciones WWN

Para obtener una lista de los rangos de direcciones WWN de estos grupos, consulte Grupos de direcciones de Fibre Channel (WWN).

El rango de direcciones de los grupos de direcciones debe ser único dentro del dominio de XClarity Administrator. XClarity Administrator garantiza que los rangos definidos y las direcciones asignadas son únicos dentro de su dominio de gestión.

Importante: En entornos grandes con varias instancias de XClarity Administrator, asegúrese de que cada XClarity Administrator utilice rangos de direcciones únicos para evitar la duplicación de direcciones.

Los grupos de direcciones de Ethernet y de Fibre Channel se utilizan con el direccionamiento virtual de adaptadores de E/S para asignar direcciones de E/S únicas en la organización. Cuando crea un patrón de servidor para un nodo de cálculo, puede habilitar el direccionamiento virtual como parte de los dispositivos y la configuración de adaptadores de E/S. Cuando el direccionamiento virtual está habilitado, las direcciones se asignan desde los grupos de direcciones de Ethernet y Fibre Channel para evitar conflictos de direcciones.

Restricción: el direccionamiento virtual solo es compatible con los nodos de cálculo de Flex System. No se admiten los servidores de bastidor y de torre autónomos.

Para obtener información sobre la creación de patrones de servidor, consulte Creación de un patrón de servidor.

Creación de un grupo de direcciones IP

Un *grupo de direcciones IP* define un rango de direcciones IP para utilizarlo al configurar la interfaz de red del controlador de gestión de la placa base de sus servidores. Cuando se despliega el patrón de servidor asociado, las direcciones IP se distribuyen desde el grupo especificado y se asignan a servidores individuales.

Acerca de esta tarea

Los datos de la tabla Información general de la red del cuadro de diálogo Nuevo grupo de direcciones IP se derivan de la máscara de subred especificada y de la puerta de enlace o del rango inicial. Puede crear grupos de distintos tamaños basados en la máscara de subred específica, pero los rangos de grupos globales deben ser únicos dentro del dominio de gestión. Los rangos se crean a continuación desde el rango

de grupos global. Todos los rangos deben formar parte de la misma subred y están vinculados a los límites que se muestran en la tabla Información general de la red.

El grupo y los rangos tienen el ámbito Lenovo XClarity Administrator. En entornos grandes con varias instancias de XClarity Administrator, cree grupos y rangos únicos para cada XClarity Administrator con el fin de evitar conflictos entre direcciones y conflictos de direcciones con las herramientas de gestión de IP existentes. Los rangos también pueden utilizarse para separar hosts (por ejemplo, por tipo de sistema operativo, tipo de carga de trabajo y función empresarial) y para ligar las reglas de red de la organización.

Procedimiento

Lleve a cabo los pasos siguientes para crear un grupo de direcciones IP.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Grupos de direcciones**. Se muestra la página Patrones de configuración: Grupos de direcciones.

Paso 2. Haga clic en la pestaña **Grupos de direcciones IP**.

Paso 3. Haga clic en el icono **Crear** ( ). Se muestra el cuadro de diálogo Asistente de Nuevos grupos de direcciones IP.

Paso 4. Rellene la siguiente información.

- Nombre y descripción del grupo de direcciones.
- Elija la utilización de direcciones IPv4 o IPv6.
- Seleccione una máscara de subred (para IPv4) o una longitud del prefijo de direccionamiento (para IPv6).
- Especifique la dirección de la puerta de enlace.Los valores de información de la red se derivan de la máscara de subred especificada y la puerta de enlace o rango inicial y se rellenan en la tabla.
- Añada uno o más rangos de direcciones:
  1. Haga clic en **Añadir rango** para añadir un rango de direcciones. Se muestra el cuadro de diálogo Añadir nuevo rango de direcciones IP.
  2. Introduzca un nombre de rango, la primera dirección y el tamaño del rango.La última dirección se calcula automáticamente.
  3. Haga clic en **Aceptar**.El rango se agrega a la tabla **Definir rangos de direcciones de grupos de IP** y los campos de la sección de resumen se actualizan automáticamente.

  Puede editar el rango pulsando el icono **Editar** ( ) o quitar el rango pulsando el icono **Quitar** ( ).

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

Después de finalizar

El nuevo grupo de direcciones IP se muestra en la tabla de la página Grupos de direcciones IP:

Desde esta página puede realizar las acciones siguientes en el grupo de direcciones seleccionado:

- Modificar el grupo de direcciones haciendo clic en el icono **Editar** ( ).
- Cambiar el nombre del grupo de direcciones pulsando el icono **Cambiar nombre**.
- Eliminar el grupo de direcciones pulsando el icono **Eliminar** ( ).
- Ver detalles acerca del grupo de direcciones, lo que incluye la asignación entre direcciones virtuales y puertos del adaptador instalados, además de las direcciones virtuales reservadas, pulsando el nombre del grupo en la columna **Nombre del grupo**.

Creación de un grupo de direcciones de Ethernet

Los *grupos de direcciones de Ethernet* son colecciones de direcciones de control de acceso al medio (MAC, Media Access Control) únicas que pueden asignarse a los adaptadores de red. Puede utilizar grupos de direcciones predefinidos o personalizarlos según sea necesario, o bien puede crear nuevos grupos de direcciones. Al crear un patrón de servidor, si habilita el direccionamiento virtual para adaptadores de Ethernet, podrá elegir qué grupo de direcciones de Ethernet se va a utilizar al desplegar el patrón. Cuando se despliega el patrón de servidor asociado, las direcciones MAC se distribuyen desde el grupo de direcciones seleccionado y se asignan a los adaptadores de red individuales de los servidores.

Procedimiento

Lleve a cabo los pasos siguientes para crear un grupo de direcciones de Ethernet.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Aprovisionamiento → Grupos de direcciones**. Se muestra la página Patrones de configuración: Grupos de direcciones.

Paso 2. Haga clic en la pestaña **Grupos de direcciones de Ethernet**.

Paso 3. Haga clic en el icono **Crear** ( ). Se muestra el cuadro de diálogo Nuevos grupos de direcciones de Ethernet (MAC).

Paso 4. Escriba un nombre y una descripción para el grupo de direcciones.

Paso 5. Añada uno o más rangos de direcciones:

a. Haga clic en **Añadir rango** para añadir un rango de direcciones. Se muestra el cuadro de diálogo Rango de direcciones de Ethernet (MAC).

b. Introduzca un nombre de rango, la primera dirección MAC y el tamaño del rango.

La última dirección MAC se calcula automáticamente.

c. Haga clic en **Añadir**.

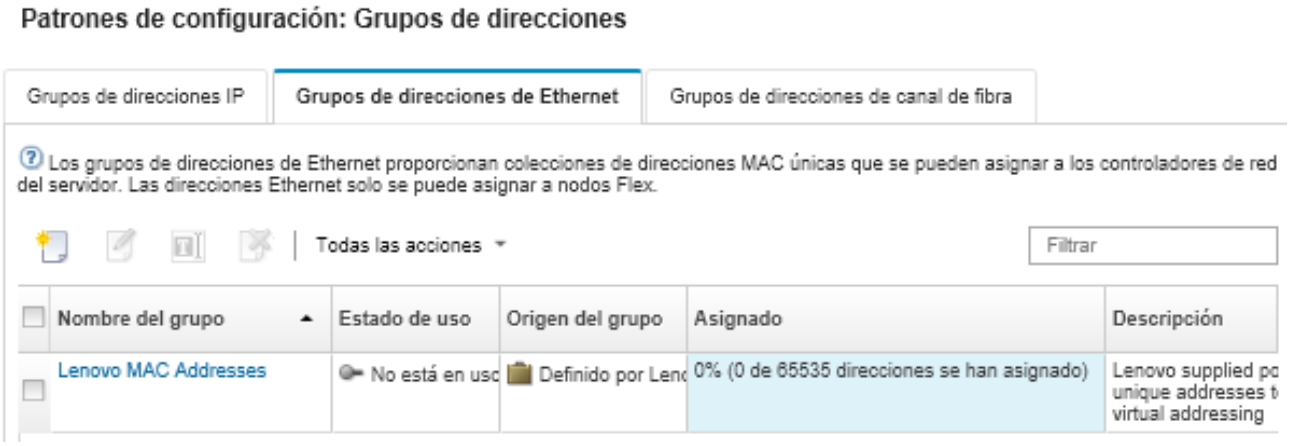
El rango se agrega a la tabla **Definir rangos de direcciones de grupos de Ethernet (MAC)** y los campos de la sección de resumen se actualizan automáticamente.

Puede editar el rango pulsando el icono **Editar** ( ) o quitar el rango pulsando el icono **Quitar** ( ).

Paso 6. Haga clic en **Guardar**.

Después de finalizar

El nuevo grupo de direcciones de Ethernet se muestra en la página Grupos de direcciones de Ethernet.



Desde esta página puede realizar las acciones siguientes en el grupo de direcciones seleccionado:

- Modificar el grupo de direcciones haciendo clic en el icono **Editar** ( ).
- Cambiar el nombre del grupo de direcciones pulsando el icono **Cambiar nombre**.
- Eliminar el grupo de direcciones pulsando el icono **Eliminar** ( ).
- Ver detalles acerca del grupo de direcciones, lo que incluye la asignación entre direcciones virtuales y puertos del adaptador instalados, además de las direcciones virtuales reservadas, pulsando el nombre del grupo en la columna **Nombre del grupo**.

Grupos de direcciones de Ethernet (MAC)

Los grupos de direcciones de Ethernet son colecciones de direcciones Media Access Control (MAC) únicas que se pueden asignar a los adaptadores de red. Puede utilizar el siguiente grupo de direcciones predefinido en sus patrones de servidor.

Tabla 3. Grupo de direcciones MAC de Lenovo

Rango predefinido	Dirección inicial	Dirección final
Rango 1	00:1A:64:76:00:00	00:1A:64:76:1C:70
Rango 2	00:1A:64:76:1C:71	00:1A:64:76:38:E1
Rango 3	00:1A:64:76:38:E2	00:1A:64:76:55:52
Rango 4	00:1A:64:76:55:53	00:1A:64:76:71:C3
Rango 5	00:1A:64:76:71:C4	00:1A:64:76:8E:34
Rango 6	00:1A:64:76:8E:35	00:1A:64:76:AA:A5
Rango 7	00:1A:64:76:AA:A6	00:1A:64:76:C7:16
Rango 8	00:1A:64:76:C7:17	00:1A:64:76:E3:87
Rango 9	00:1A:64:76:E3:88	00:1A:64:76:FF:F8

Creación de un grupo de direcciones de Fibre Channel

Los *Grupos de direcciones de Fibre Channel* son colecciones de direcciones únicas de nombre de nodo World Wide (WWNN, World Wide Node Name) y de nombre de puerto World Wide (WWPN, World Wide Port Name) que pueden asignarse a los adaptadores de Fibre Channel al configurar servidores. Puede utilizar grupos de direcciones predefinidos o personalizarlos según sea necesario, o bien puede crear nuevos grupos. Al crear patrones de servidor, si habilita el direccionamiento virtual para adaptadores de Ethernet, podrá elegir qué grupo de direcciones de Fibre Channel se va a utilizar al desplegar el patrón. Cuando se despliega el patrón de servidor asociado, las direcciones WWNN y WWPN se distribuyen desde el grupo especificado y se asignan a servidores individuales.

Procedimiento

Lleve a cabo los pasos siguientes para crear un grupo de direcciones de Fibre Channel.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Aprovisionamiento → Grupos de direcciones**. Se muestra la página Patrones de configuración: Grupos de direcciones.

Paso 2. Haga clic en la pestaña **Grupos de direcciones de Fibre Channel**.

Paso 3. Haga clic en el icono **Crear** ( ). Se muestra el cuadro de diálogo Grupos de direcciones de Fibre Channel.

Paso 4. Escriba un nombre y una descripción para el grupo de direcciones.

Paso 5. Añada uno o más rangos de direcciones:

a. Haga clic en **Añadir rango** para añadir un rango de direcciones. Se muestra el cuadro de diálogo Rango de direcciones de Fibre Channel (WWN).

b. Introduzca un nombre de rango, un tamaño de rango y la primera dirección de cada entramado.

   Las últimas direcciones se calculan automáticamente.

c. Haga clic en **Añadir**.

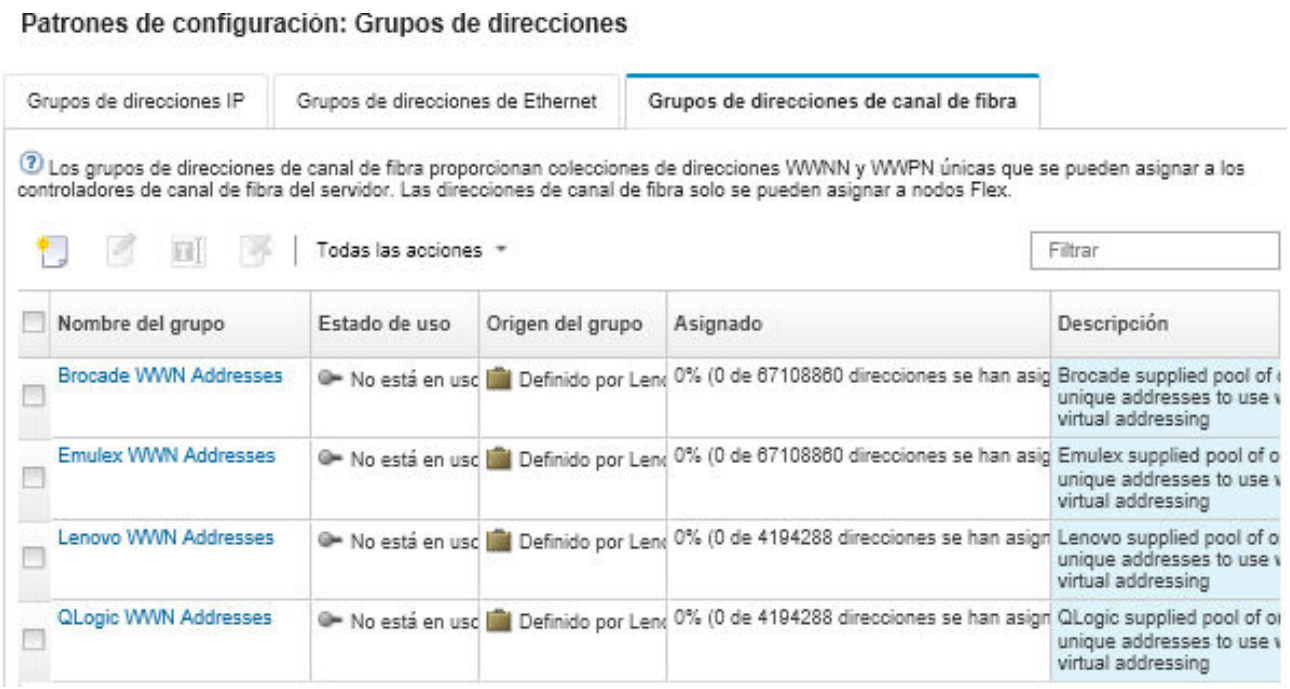
   El rango se agrega a la tabla **Definir rangos de direcciones de grupos de Fibre Channel** y los campos de la sección de resumen se actualizan automáticamente.

   Puede editar el rango pulsando el icono **Editar** ( ) o quitar el rango pulsando el icono **Quitar** ( ).

Paso 6. Haga clic en **Guardar**.

Después de finalizar

El nuevo grupo de direcciones de Fibre Channel se muestra en la tabla Grupos de direcciones de Fibre Channel.



Desde esta página puede realizar las acciones siguientes en el grupo de direcciones seleccionado:

- Modificar el grupo de direcciones haciendo clic en el icono **Editar** ( ).
- Eliminar el grupo de direcciones pulsando el icono **Eliminar** ( ).
- Ver detalles acerca del grupo de direcciones, lo que incluye la asignación entre direcciones virtuales y puertos del adaptador instalados, además de las direcciones virtuales reservadas, pulsando el nombre del grupo en la columna **Nombre del grupo**.

Grupos de direcciones de Fibre Channel (WWN)

Los grupos de direcciones de Fibre Channel son colecciones de direcciones World Wide Node Name (WWNN) y World Wide Port Name (WWPN) únicas que se pueden asignar a los adaptadores de Fibre Channel al configurar servidores. Puede utilizar los siguientes grupos de direcciones predefinidos en sus patrones de servidor.

Tabla 4 “Grupo de direcciones WWN de Brocade” en la página 352 muestra una lista de los grupos de direcciones World Wide Name (WWN) de Brocade. Cada rango WWN de Brocade contiene 1.864.135 direcciones.

Tabla 5 “Grupo de direcciones WWN de Emulex” en la página 353 muestra una lista de los grupos de direcciones WWN de Emulex. Cada rango WWN de Emulex contiene 1.864.135 direcciones.

Tabla 6 “Grupo de direcciones WWN de Lenovo” en la página 354 muestra una lista de los grupos de direcciones WWN de Lenovo. Cada rango WWN de Lenovo contiene 116.508 direcciones.

Tabla 7 “Grupo de direcciones WWN de QLogic” en la página 355 muestra una lista de los grupos de direcciones WWN de QLogic. Cada rango WWN de QLogic contiene 116.508 direcciones.

Tabla 4. Grupo de direcciones WWN de Brocade

Rango predefinido	Dirección WWNN inicial	Dirección WWNN final	Dirección WWPN inicial	Dirección WWPN final
Malla A				
Rango 1	2B:FA:00:05:1E:00:00:00	2B:FA:00:05:1E:1C:71:C6	2B:FC:00:05:1E:00:00:00	2B:FC:00:05:1E:1C:71:C6
Rango 2	2B:FA:00:05:1E:1C:71:C7	2B:FA:00:05:1E:38:E3:8D	2B:FC:00:05:1E:1C:71:C7	2B:FC:00:05:1E:38:E3:8D
Rango 3	2B:FA:00:05:1E:38:E3:8E	2B:FA:00:05:1E:55:55:54	2B:FC:00:05:1E:38:E3:8E	2B:FC:00:05:1E:55:55:54
Rango 4	2B:FA:00:05:1E:55:55:55	2B:FA:00:05:1E:71:C7:1B	2B:FC:00:05:1E:55:55:55	2B:FC:00:05:1E:71:C7:1B
Rango 5	2B:FA:00:05:1E:71:C7:1C	2B:FA:00:05:1E:8E:38:E2	2B:FC:00:05:1E:71:C7:1C	2B:FC:00:05:1E:8E:38:E2
Rango 6	2B:FA:00:05:1E:8E:38:E3	2B:FA:00:05:1E:AA:AA:A9	2B:FC:00:05:1E:8E:38:E3	2B:FC:00:05:1E:AA:AA:A9
Rango 7	2B:FA:00:05:1E:AA:AA:AA	2B:FA:00:05:1E:C7:1C:70	2B:FC:00:05:1E:AA:AA:AA	2B:FC:00:05:1E:C7:1C:70
Rango 8	2B:FA:00:05:1E:C7:1C:71	2B:FA:00:05:1E:E3:8E:37	2B:FC:00:05:1E:C7:1C:71	2B:FC:00:05:1E:E3:8E:37
Rango 9	2B:FA:00:05:1E:E3:8E:38	2B:FA:00:05:1E:FF:FF:FE	2B:FC:00:05:1E:E3:8E:38	2B:FC:00:05:1E:FF:FF:FE
Malla B				
Rango 1	2B:FB:00:05:1E:00:00:00	2B:FB:00:05:1E:1C:71:C6	2B:FD:00:05:1E:00:00:00	2B:FD:00:05:1E:1C:71:C6
Rango 2	2B:FB:00:05:1E:1C:71:C7	2B:FB:00:05:1E:38:E3:8D	2B:FD:00:05:1E:1C:71:C7	2B:FD:00:05:1E:38:E3:8D
Rango 3	2B:FB:00:05:1E:38:E3:8E	2B:FB:00:05:1E:55:55:54	2B:FD:00:05:1E:38:E3:8E	2B:FD:00:05:1E:55:55:54
Rango 4	2B:FB:00:05:1E:55:55:55	2B:FB:00:05:1E:71:C7:1B	2B:FD:00:05:1E:55:55:55	2B:FD:00:05:1E:71:C7:1B
Rango 5	2B:FB:00:05:1E:71:C7:1C	2B:FB:00:05:1E:8E:38:E2	2B:FD:00:05:1E:71:C7:1C	2B:FD:00:05:1E:8E:38:E2
Rango 6	2B:FB:00:05:1E:8E:38:E3	2B:FB:00:05:1E:AA:AA:A9	2B:FD:00:05:1E:8E:38:E3	2B:FD:00:05:1E:AA:AA:A9
Rango 7	2B:FB:00:05:1E:AA:AA:AA	2B:FB:00:05:1E:C7:1C:70	2B:FD:00:05:1E:AA:AA:AA	2B:FD:00:05:1E:C7:1C:70
Rango 8	2B:FB:00:05:1E:C7:1C:71	2B:FB:00:05:1E:E3:8E:37	2B:FD:00:05:1E:C7:1C:71	2B:FD:00:05:1E:E3:8E:37
Rango 9	2B:FB:00:05:1E:E3:8E:38	2B:FB:00:05:1E:FF:FF:FE	2B:FD:00:05:1E:E3:8E:38	2B:FD:00:05:1E:FF:FF:FE

Tabla 5. Grupo de direcciones WWN de Emulex

Rango predefinido	Dirección WWNN inicial	Dirección WWNN final	Dirección WWPN inicial	Dirección WWPN final
Malla A				
Rango 1	2F:FE:00:00:C9:00:00:00	2F:FE:00:00:C9:1C:71:C6	2F:FC:00:00:C9:00:00:00	2F:FC:00:00:C9:1C:71:C6
Rango 2	2F:FE:00:00:C9:1C:71:C7	2F:FE:00:00:C9:38:E3:8D	2F:FC:00:00:C9:1C:71:C7	2F:FC:00:00:C9:38:E3:8D
Rango 3	2F:FE:00:00:C9:38:E3:8E	2F:FE:00:00:C9:55:55:54	2F:FC:00:00:C9:38:E3:8E	2F:FC:00:00:C9:55:55:54
Rango 4	2F:FE:00:00:C9:55:55:55	2F:FE:00:00:C9:71:C7:1B	2F:FC:00:00:C9:55:55:55	2F:FC:00:00:C9:71:C7:1B
Rango 5	2F:FE:00:00:C9:71:C7:1C	2F:FE:00:00:C9:8E:38:E2	2F:FC:00:00:C9:71:C7:1C	2F:FC:00:00:C9:8E:38:E2
Rango 6	2F:FE:00:00:C9:8E:38:E3	2F:FE:00:00:C9:AA:AA:A9	2F:FC:00:00:C9:8E:38:E3	2F:FC:00:00:C9:AA:AA:A9
Rango 7	2F:FE:00:00:C9:AA:AA:AA	2F:FE:00:00:C9:C7:1C:70	2F:FC:00:00:C9:AA:AA:AA	2F:FC:00:00:C9:C7:1C:70
Rango 8	2F:FE:00:00:C9:C7:1C:71	2F:FE:00:00:C9:E3:8E:37	2F:FC:00:00:C9:C7:1C:71	2F:FC:00:00:C9:E3:8E:37
Rango 9	2F:FE:00:00:C9:E3:8E:38	2F:FE:00:00:C9:FF:FF:FE	2F:FC:00:00:C9:E3:8E:38	2F:FC:00:00:C9:FF:FF:FE
Malla B				
Rango 1	2F:FF:00:00:C9:00:00:00	2F:FF:00:00:C9:1C:71:C6	2F:FD:00:00:C9:00:00:00	2F:FD:00:00:C9:1C:71:C6
Rango 2	2F:FF:00:00:C9:1C:71:C7	2F:FF:00:00:C9:38:E3:8D	2F:FD:00:00:C9:1C:71:C7	2F:FD:00:00:C9:38:E3:8D
Rango 3	2F:FF:00:00:C9:38:E3:8E	2F:FF:00:00:C9:55:55:54	2F:FD:00:00:C9:38:E3:8E	2F:FD:00:00:C9:55:55:54
Rango 4	2F:FF:00:00:C9:55:55:55	2F:FF:00:00:C9:71:C7:1B	2F:FD:00:00:C9:55:55:55	2F:FD:00:00:C9:71:C7:1B
Rango 5	2F:FF:00:00:C9:71:C7:1C	2F:FF:00:00:C9:8E:38:E2	2F:FD:00:00:C9:71:C7:1C	2F:FD:00:00:C9:8E:38:E2
Rango 6	2F:FF:00:00:C9:8E:38:E3	2F:FF:00:00:C9:AA:AA:A9	2F:FD:00:00:C9:8E:38:E3	2F:FD:00:00:C9:AA:AA:A9
Rango 7	2F:FF:00:00:C9:AA:AA:AA	2F:FF:00:00:C9:C7:1C:70	2F:FD:00:00:C9:AA:AA:AA	2F:FD:00:00:C9:C7:1C:70
Rango 8	2F:FF:00:00:C9:C7:1C:71	2F:FF:00:00:C9:E3:8E:37	2F:FD:00:00:C9:C7:1C:71	2F:FD:00:00:C9:E3:8E:37
Rango 9	2F:FF:00:00:C9:E3:8E:38	2F:FF:00:00:C9:FF:FF:FE	2F:FD:00:00:C9:E3:8E:38	2F:FD:00:00:C9:FF:FF:FE

Tabla 6. Grupo de direcciones WWN de Lenovo

Rango predefinido	Dirección WWNN inicial	Dirección WWNN final	Dirección WWPN inicial	Dirección WWPN final
Malla A				
Rango 1	20:80:00:50:76:00:00:00	20:80:00:50:76:01:C7:1B	21:80:00:50:76:00:00:00	21:80:00:50:76:01:C7:1B
Rango 2	20:80:00:50:76:01:C7:1C	20:80:00:50:76:03:8E:37	21:80:00:50:76:01:C7:1C	21:80:00:50:76:03:8E:37
Rango 3	20:80:00:50:76:03:8E:38	20:80:00:50:76:05:55:53	21:80:00:50:76:03:8E:38	21:80:00:50:76:05:55:53
Rango 4	20:80:00:50:76:05:55:54	20:80:00:50:76:07:1C:6F	21:80:00:50:76:05:55:54	21:80:00:50:76:07:1C:6F
Rango 5	20:80:00:50:76:07:1C:70	20:80:00:50:76:08:E3:8B	21:80:00:50:76:07:1C:70	21:80:00:50:76:08:E3:8B
Rango 6	20:80:00:50:76:08:E3:8C	20:80:00:50:76:0A:AA:A7	21:80:00:50:76:08:E3:8C	21:80:00:50:76:0A:AA:A7
Rango 7	20:80:00:50:76:0A:AA:A8	20:80:00:50:76:0C:71:C3	21:80:00:50:76:0A:AA:A8	21:80:00:50:76:0C:71:C3
Rango 8	20:80:00:50:76:0C:71:C4	20:80:00:50:76:0E:38:DF	21:80:00:50:76:0C:71:C4	21:80:00:50:76:0E:38:DF
Rango 9	20:80:00:50:76:0E:38:E0	20:80:00:50:76:0F:FF:FB	21:80:00:50:76:0E:38:E0	21:80:00:50:76:0F:FF:FB
Malla B				
Rango 1	20:81:00:50:76:20:00:00	20:81:00:50:76:21:C7:1B	21:81:00:50:76:20:00:00	21:81:00:50:76:21:C7:1B
Rango 2	20:81:00:50:76:21:C7:1C	20:81:00:50:76:23:8E:37	21:81:00:50:76:21:C7:1C	21:81:00:50:76:23:8E:37
Rango 3	20:81:00:50:76:23:8E:38	20:81:00:50:76:25:55:53	21:81:00:50:76:23:8E:38	21:81:00:50:76:25:55:53
Rango 4	20:81:00:50:76:25:55:54	20:81:00:50:76:27:1C:6F	21:81:00:50:76:25:55:54	21:81:00:50:76:27:1C:6F
Rango 5	20:81:00:50:76:27:1C:70	20:81:00:50:76:28:E3:8B	21:81:00:50:76:27:1C:70	21:81:00:50:76:28:E3:8B
Rango 6	20:81:00:50:76:28:E3:8C	20:81:00:50:76:2A:AA:A7	21:81:00:50:76:28:E3:8C	21:81:00:50:76:2A:AA:A7
Rango 7	20:81:00:50:76:2A:AA:A8	20:81:00:50:76:2C:71:C3	21:81:00:50:76:2A:AA:A8	21:81:00:50:76:2C:71:C3
Rango 8	20:81:00:50:76:2C:71:C4	20:81:00:50:76:2E:38:DF	21:81:00:50:76:2C:71:C4	21:81:00:50:76:2E:38:DF
Rango 9	20:81:00:50:76:2E:38:E0	20:81:00:50:76:2F:FF:FB	21:81:00:50:76:2E:38:E0	21:81:00:50:76:2F:FF:FB

Tabla 7. Grupo de direcciones WWN de QLogic

Rango predefinido	Dirección WWNN inicial	Dirección WWNN final	Dirección WWPN final	Dirección WWPN final
Malla A				
Rango 1	20:80:00:E0:8B:00:00:00	20:80:00:E0:8B:01:C7:1B	21:80:00:E0:8B:00:00:00	21:80:00:E0:8B:01:C7:1B
Rango 2	20:80:00:E0:8B:01:C7:1C	20:80:00:E0:8B:03:8E:37	21:80:00:E0:8B:01:C7:1C	21:80:00:E0:8B:03:8E:37
Rango 3	20:80:00:E0:8B:03:8E:38	20:80:00:E0:8B:05:55:53	21:80:00:E0:8B:03:8E:38	21:80:00:E0:8B:05:55:53
Rango 4	20:80:00:E0:8B:05:55:54	20:80:00:E0:8B:07:1C:6F	21:80:00:E0:8B:05:55:54	21:80:00:E0:8B:07:1C:6F
Rango 5	20:80:00:E0:8B:07:1C:70	20:80:00:E0:8B:08:E3:8B	21:80:00:E0:8B:07:1C:70	21:80:00:E0:8B:08:E3:8B
Rango 6	20:80:00:E0:8B:08:E3:8C	20:80:00:E0:8B:0A:AA:A7	21:80:00:E0:8B:08:E3:8C	21:80:00:E0:8B:0A:AA:A7
Rango 7	20:80:00:E0:8B:0A:AA:A8	20:80:00:E0:8B:0C:71:C3	21:80:00:E0:8B:0A:AA:A8	21:80:00:E0:8B:0C:71:C3
Rango 8	20:80:00:E0:8B:0C:71:C4	20:80:00:E0:8B:0E:38:DF	21:80:00:E0:8B:0C:71:C4	21:80:00:E0:8B:0E:38:DF
Rango 9	20:80:00:E0:8B:0E:38:E0	20:80:00:E0:8B:0F:FF:FB	21:80:00:E0:8B:0E:38:E0	21:80:00:E0:8B:0F:FF:FB
Malla B				
Rango 1	20:81:00:E0:8B:20:00:00	20:81:00:E0:8B:21:C7:1B	21:81:00:E0:8B:20:00:00	21:81:00:E0:8B:21:C7:1B
Rango 2	20:81:00:E0:8B:21:C7:1C	20:81:00:E0:8B:23:8E:37	21:81:00:E0:8B:21:C7:1C	21:81:00:E0:8B:23:8E:37
Rango 3	20:81:00:E0:8B:23:8E:38	20:81:00:E0:8B:25:55:53	21:81:00:E0:8B:23:8E:38	21:81:00:E0:8B:25:55:53
Rango 4	20:81:00:E0:8B:25:55:54	20:81:00:E0:8B:27:1C:6F	21:81:00:E0:8B:25:55:54	21:81:00:E0:8B:27:1C:6F
Rango 5	20:81:00:E0:8B:27:1C:70	20:81:00:E0:8B:28:E3:8B	21:81:00:E0:8B:27:1C:70	21:81:00:E0:8B:28:E3:8B
Rango 6	20:81:00:E0:8B:28:E3:8C	20:81:00:E0:8B:2A:AA:A7	21:81:00:E0:8B:28:E3:8C	21:81:00:E0:8B:2A:AA:A7
Rango 7	20:81:00:E0:8B:2A:AA:A8	20:81:00:E0:8B:2C:71:C3	21:81:00:E0:8B:2A:AA:A8	21:81:00:E0:8B:2C:71:C3
Rango 8	20:81:00:E0:8B:2C:71:C4	20:81:00:E0:8B:2E:38:DF	21:81:00:E0:8B:2C:71:C4	21:81:00:E0:8B:2E:38:DF
Rango 9	20:81:00:E0:8B:2E:38:E0	20:81:00:E0:8B:2F:FF:FB	21:81:00:E0:8B:2E:38:E0	21:81:00:E0:8B:2F:FF:FB

Trabajo con patrones de servidor

Un *patrón de servidor* representa la configuración de servidor anterior al SO, incluidos la del almacenamiento local, del adaptador de E/S, de arranque de SAN y otros valores de firmware del controlador de gestión de la placa base y de la UEFI. Los patrones de servidor también integran el soporte para la virtualización de

direcciones de E/S, de modo que puede virtualizar conexiones de malla del servidor o readaptar servidores sin interrupción. Un patrón de servidor se utiliza como patrón general para configurar rápidamente varios servidores a la vez.

Acerca de esta tarea

Puede definir varios patrones de servidor para representar las distintas configuraciones que se utilizarán en su centro de datos.

Cuando defina un patrón de servidor, seleccione o cree patrones de categorías y grupos de direcciones según sea necesario para construir la configuración deseada para un grupo de servidores específico. Un *patrón de categoría* define valores de firmware específicos que pueden reutilizarse en varios patrones de servidor. Puede utilizar grupos de direcciones para definir los rangos de direcciones que se van a utilizar para asignar direcciones a servidores individuales al desplegar patrones de servidor. Hay grupos de direcciones IP, grupos de direcciones de Ethernet (MAC) y grupos de direcciones de Fibre Channel (WWN).

Cuando se despliega un patrón de servidor en varios servidores, se generan varios perfiles de servidor de forma automática (un perfil por cada servidor). Cada perfil hereda valores del patrón de servidor principal, de modo que puede controlar una configuración común desde un solo lugar.

Puede crear un patrón de servidor desde cero y definir la configuración deseada antes de que llegue el hardware. También puede crear un patrón de servidor a partir de un servidor existente y utilizar después ese patrón para aprovisionar el resto de los servidores. Si crea un patrón de servidor a partir de un servidor existente, los patrones de categorías extendidos se extraen y se crean dinámicamente a partir de los valores actuales del servidor. Si desea cambiar los valores de categoría, puede editarlos directamente desde los patrones de servidor.

Atención: Si crea un nuevo patrón de servidor desde cero, debe definir los valores de arranque de los servidores. Cuando despliega el patrón de servidor en los servidores, el orden de arranque existente en los servidores se sobrescribe con los valores del orden de arranque predeterminados del patrón de servidor. Si los servidores no se inician después de desplegar un patrón de servidor en ellos, el problema se puede deber a que los valores de arranque originales se hayan sobrescrito con los valores de orden de arranque predeterminados que están en el nuevo patrón de servidor. Para restaurar los valores de arranque originales en los servidores, consulte Recuperación de los valores de arranque tras el despliegue de patrones de servidor.

Importante: Cuando cree patrones de servidor, asegúrese de que los crea para cada tipo de servidor. Por ejemplo, cree un patrón de servidor para todos los nodos de cálculo x240 de Flex System y otro patrón de servidor para todos los nodos de cálculo x440 de Flex System. No despliegue un patrón de servidor que fue creado para un tipo de servidor en otro tipo de servidor.

Importante: Si el nodo de gestión falla, puede perder los patrones de servidor. Realice siempre una copia de seguridad del software de gestión después de crear o modificar patrones de servidor (consulte Copia de seguridad de Lenovo XClarity Administrator).

Valores para los dispositivos de red

Algunos dispositivos de red de Flex System ofrecen más opciones de configuración de patrones de servidor que otros.

Aunque los patrones de servidor se pueden aplicar en cualquier dispositivo de red, la funcionalidad de algunos patrones de servidor está limitada a determinados adaptadores de red. Además, algunos valores avanzados de los adaptadores de red de Ethernet (como las preferencias de compatibilidad del adaptador y del puerto) no se admiten en la actualidad.

Los patrones de servidor pueden extraer los datos y valores de configuración existentes para los adaptadores de red compatibles y pueden cambiar los valores de configuración mediante el despliegue del patrón.

Patrones de categorías

Los valores de firmware están organizados en categorías que agrupan los valores relacionados. Para cada categoría, puede crear un *patrón de categoría* que contenga los valores de firmware comunes y pueda reutilizarse en varios patrones de servidor. La mayoría de los valores de firmware que se pueden configurar directamente en el servidor del controlador de gestión de la placa base y de la UEFI también se pueden configurar a través de patrones de categorías. Los valores de firmware que están disponibles dependen del tipo de servidor, de su entorno de Flex System y del ámbito del patrón de servidor.

Puede crear patrones de categorías aparte de los patrones de servidor.

Los patrones de categorías pueden predefinise o extraerse de los servidores existentes, o bien estar definidos por el usuario.

- **Patrones de categorías extendidos**

  Los *patrones de categorías extendidos* son patrones para los valores de algunos puertos de adaptadores de E/S, de Unified Extensible Firmware Interface (UEFI) avanzada y del controlador de gestión de la placa base (BMC), que se extraen y se crean dinámicamente desde un servidor gestionado específico. Lenovo XClarity Administrator crea estos patrones cuando se crea un patrón de servidor a partir de un servidor existente. No se pueden crear manualmente patrones de categorías extendidos; sin embargo, sí se pueden editar después de haberlos creado.

  Los siguientes patrones de UEFI extendida se predefinen mediante XClarity Administrator para optimizar los servidores para entornos específicos.
  - **Opciones de instalación de ESXi**
  - **Eficiencia: favorecer el rendimiento**
  - **Modo Eficiencia: favorecer la energía**
  - **Rendimiento máximo**
  - **Energía mínima**
- **Patrones de categorías definidos por el usuario**

  Los *patrones de categorías definidos por el usuario* son los patrones que el usuario puede crear, incluidos la información del sistema, las interfaces de gestión, los dispositivos y puertos de E/S, los destinos de arranque de Fibre Channel y los puertos de adaptadores de E/S. Puede crear los siguientes patrones de categorías:

  - **Información del sistema**. Los valores incluyen el nombre del sistema, la ubicación y los contactos generados automáticamente.
  - **Interfaz de gestión**. Los valores incluyen el nombre de host, direcciones IP, el espacio de nombre de dominio (DNS), la velocidad de interfaz y las asignaciones de puertos para la interfaz de gestión generados automáticamente.Los patrones de servidor no admiten valores dúplex.
  - **Dispositivos y puertos de E/S**. Los valores incluyen el redireccionamiento de la consola y los puertos COM. Puede utilizar patrones de servidor para habilitar el puerto serie sobre IP en el área de redireccionamiento de la consola. No obstante, cuando el puerto serie sobre IP está habilitado, el único valor del modo de acceso del puerto serie que admiten los patrones de servidor es **Dedicado**; los valores de IPMI **Compartido** y **Prearranque** del modo de acceso del puerto serie no están disponibles en los patrones de servidor.

    Importante: Si crea un patrón de servidor a partir de un servidor existente y ese servidor tiene un valor de modo de acceso del puerto serie **Compartido** o **Prearranque**, el patrón del dispositivo y de los puertos de E/S que se extrae del servidor tiene el valor del modo de acceso del puerto serie **Dedicado**.

- **Destinos de arranque de Fibre Channel**. Los valores incluyen los destinos de arranque WWN de Fibre Channel Fibre Channel.
- **Puertos**. Los valores incluyen los adaptadores de E/S y los puertos para la configuración de interconexiones de malla.

Creación de un patrón de servidor

Cuando cree un patrón de servidor, defina las características de configuración de un tipo de servidor específico. Puede crear un patrón de servidor desde cero utilizando los valores predeterminados o utilizar los valores de un servidor existente.

Acerca de esta tarea

Antes de crear un patrón de servidor, tenga en cuenta las siguientes sugerencias.

- La primera vez que cree un patrón de servidor, considere la posibilidad de crearlo a partir de un servidor existente. Cuando se crea un patrón de servidor a partir de un servidor existente, Lenovo XClarity Administrator extrae y crea patrones extendidos de categorías para algunos valores de puertos de adaptadores de E/S, UEFI y controlador de gestión de la placa base. Luego, esos patrones de categorías están disponibles para su uso en cualquier patrón de servidor que cree posteriormente. Para obtener más información sobre patrones de categorías, consulte Definición de valores de firmware.
- Identifique los grupos de servidores que tengan las mismas opciones de hardware y que desee configurar del mismo modo. Puede utilizar un patrón de servidor para aplicar los mismos valores de configuración de varios servidores y, por tanto, controlar una configuración común desde un solo lugar.
- Identifique los aspectos de la configuración que desee personalizar para el patrón de servidor (por ejemplo, almacenamiento local, adaptadores de red, valores de arranque, valores del controlador de gestión, valores de UEFI).
- No puede gestionar cuentas de usuarios locales ni configurar el servidor LDAP utilizando patrones de configuración.

Importante: Si el nodo de gestión falla, puede perder los patrones de servidor. Realice siempre una copia de seguridad del software de gestión después de crear o modificar patrones de servidor (consulte Copia de seguridad de Lenovo XClarity Administrator).

Procedimiento

Lleve a cabo los pasos siguientes para crear un patrón de servidor.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Patrones de configuración del servidor**. Se muestra la página Patrones de configuración de servidor.

Paso 2. Haga clic en la pestaña **Patrones de servidor**.

Paso 3. Haga clic en el icono **Crear** ( ). Se muestra el Asistente de nuevo patrón de servidor.

Paso 4. Realice una de las siguientes acciones para crear el patrón de servidor.

- Haga clic en **Crear un nuevo patrón desde un servidor existente** para utilizar los valores de un servidor existente. A continuación, selecciones el servidor gestionado en el que se basará el nuevo patrón en la lista que se muestra.

  Cuando se crea un patrón de servidor desde un servidor existente, XClarity Administrator extrae los valores del servidor gestionado especificado (incluida la configuración de puerto extendido, el UEFI y el controlador de gestión) y crea patrones de categorías de forma dinámica para dichos valores. Si el servidor es nuevo, Lenovo XClarity Administrator extrae los valores de fabricación. Si XClarity Administrator está gestionando el servidor, XClarity Administrator usa los valores personalizados. A continuación, puede personalizar los valores específicos de los servidores en los que se va a desplegar este patrón.

- Haga clic en **Crear un nuevo patrón desde cero** para utilizar los valores predeterminados. A continuación, seleccione el tipo de servidor en el campo **Factor de forma**.

Nota: Las opciones que se presentan en las demás pestañas pueden variar, en función del tipo de servidor para el cual va a crear un patrón nuevo.

Paso 5. Introduzca el nombre del patrón y una descripción.

Paso 6. Personalice el nombre del perfil de servidor seleccionando el activador **Personalizado** y seleccione uno o más elementos para incluir en el esquema de nombre (como texto, nombre del servidor y número de incremento personalizados) y el orden.

Paso 7. Haga clic en **Siguiente**.

Paso 8. Elija la configuración del almacenamiento local que se va aplicar cuando este patrón se despliegue en un servidor y haga clic en **Siguiente**.

Para obtener información sobre los valores del almacenamiento local, consulte Definición de almacenamiento local.

Paso 9. **Opcional:** modifique el direccionamiento del adaptador de E/S, defina adaptadores de E/S adicionales para que coincidan con el hardware que espera configurar con este patrón y, a continuación, haga clic en **Siguiente**.

Para obtener información sobre los valores del adaptador de E/S, consulte Definición de adaptadores de E/S.

Paso 10. Defina el orden de arranque que se aplicará cuando este patrón se despliegue en un servidor y haga clic en **Siguiente**.

Para obtener información sobre los valores de los destinos de arranque de SAN, consulte Definición de opciones de arranque.

Paso 11. Seleccione los valores de firmware de la lista de patrones existentes de la categoría.

Puede crear nuevos patrones de categoría pulsando el icono **Crear** ( ).

Para obtener información sobre los valores de firmware, consulte Definición de valores de firmware.

Paso 12. Haga clic en **Guardar** para guardar el patrón o haga clic en **Guardar y desplegar** para guardar y desplegar inmediatamente el patrón en uno o más servidores.

Para obtener información acerca del despliegue de un patrón de servidor, consulte Despliegue de un patrón de servidor en un servidor.

Después de finalizar

Si pulsa **Guardar y desplegar**, se muestra la página Desplegar el patrón de servidor. Desde esta página, puede desplegar el patrón de servidor en servidores específicos.

Si pulsa **Guardar**, el patrón de servidor y todos los patrones de categorías se guardan en la página Patrones de servidor.

Desde esta página puede realizar las acciones siguientes en los patrones de servidor seleccionados:

- Ver los detalles del patrón pulsando el nombre del patrón en la columna **Nombre**.
- Desplegar el patrón (consulte Despliegue de un patrón de servidor en un servidor).
- Copiar el patrón haciendo clic en el icono **Copiar** ( ).
- Editar el patrón (consulte Modificación de un patrón de servidor).
- Cambiar el nombre del patrón haciendo clic en el icono **Cambiar nombre** ( ).
- Eliminar el patrón haciendo clic en el icono **Eliminar** ( ).
- Exportar e importar patrones de servidor (consulte Exportación e importación de patrones de servidor y categorías).

Definición de almacenamiento local

Puede definir la configuración de almacenamiento local que se va aplicar a los servidores de destino cuando se despliegue este patrón.

Acerca de esta tarea

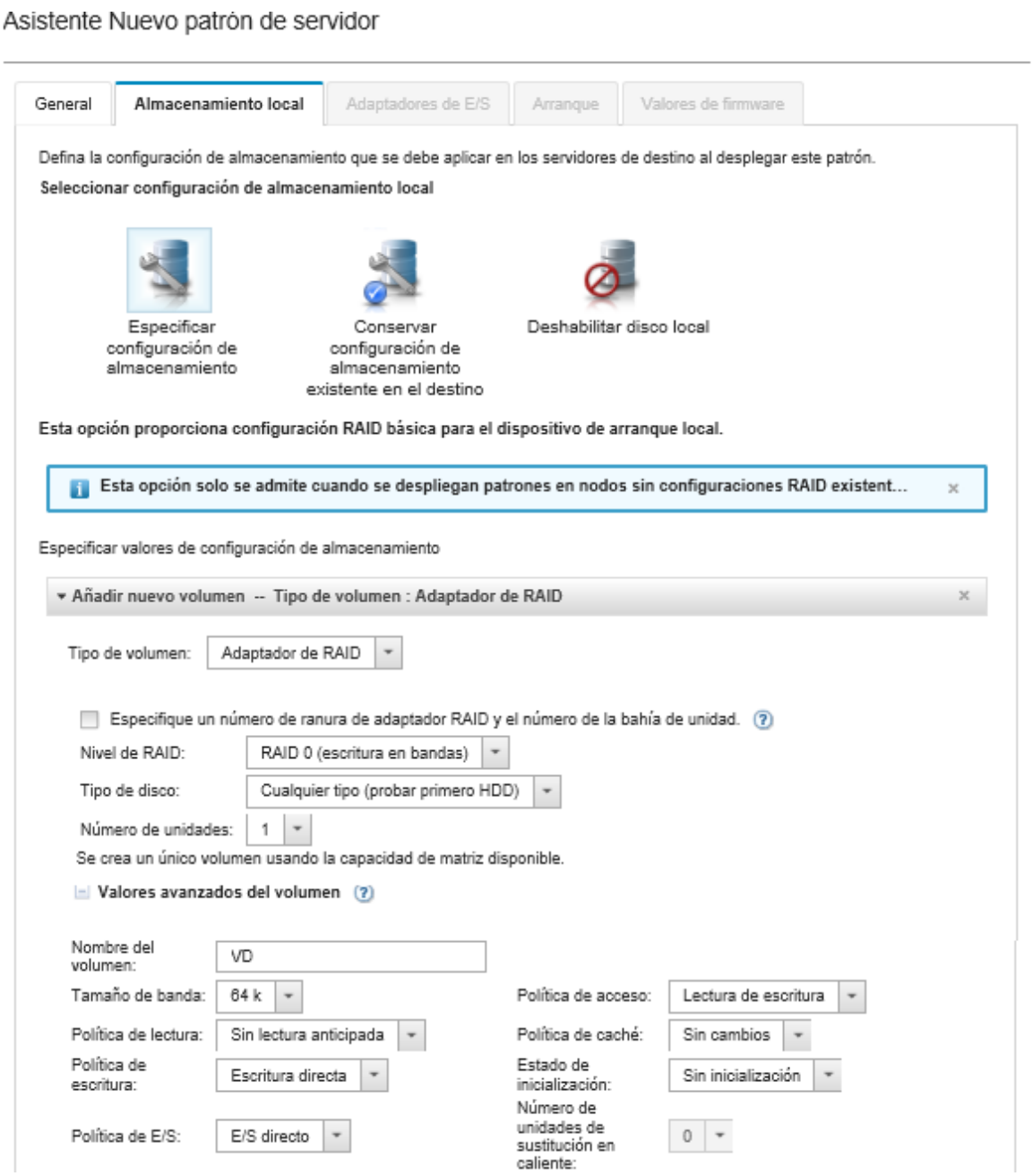
Notas:

- Los controladores de almacenamiento incorporados en Flex System x220, Flex System x222 y los servidores ThinkSystem admiten software basado en RAID. Sin embargo, no admiten la configuración de software RAID mediante patrones de configuración.
- Al configurar RAID mediante Patrones de configuración, si el servidor está apagado, el servidor arranca automáticamente a la configuración de BIOS/UEFI antes de activar el perfil de servidor.

Procedimiento

Lleve a cabo los pasos siguientes para definir la configuración de almacenamiento local.

Paso 1. En el Asistente Nuevo patrón de servidor, haga clic en la pestaña **Almacenamiento local**.



Paso 2. Para definir los valores de almacenamiento local, elija una de las opciones siguientes.

- **Especificar configuración de almacenamiento**. (Solo dispositivos sin cerrar las configuraciones RAID) Los valores RAID básicos está configurados en el dispositivo de arranque local durante el despliegue

  Especifique la configuración de almacenamiento, según la opción de almacenamiento. Puede añadir opciones de almacenamiento adicionales haciendo clic en el icono **Añadir** ( ).

  – **Adaptador RAID**. Seleccione el nivel RAID, las características y el número de unidades que están instaladas en el servidor. RAID 0, 1, 5 son compatibles. Además, puede elegir los valores de volumen avanzados, como el tamaño de banda, las políticas y el número de unidades de repuesto dinámico.

Los servidores de ThinkSystem con XCC versión 2.1 y posterior (ThinkSystem SR950 requiere XCC versión 1.4 o posterior), también puede especificar el número de ranura del adaptador RAID y los números de bahía de unidad para crear un volumen con la capacidad de matriz disponible. En este caso, se admite el nivel RAID 0, 1, 5, 6, 10, 50, 60 y 00. Además, puede elegir los valores de volumen avanzados, como el tamaño de banda, las políticas y las unidades de repuesto dinámico.

Nota: En el servidor de destino, asegúrese de que hay un número suficiente de unidades disponibles del tipo especificado, así como de que el estado de RAID de las unidades sea "Bueno sin configurar", tal como se indica en la sección **Unidades** de la página Detalles del inventario del servidor (consulte Visualización de los detalles de un servidor gestionado).

- **Adaptador de medios SD Lenovo**. Elija dónde crear el volumen y el tamaño del volumen. Puede elegir los valores de volumen avanzados, como tipo de soportes y política de acceso.
- **ThinkSystem M.2 con duplicación**. Seleccione la ranura PCI, el nivel de RAID, el nombre de volumen y el tamaño de banda para crear un volumen con la capacidad de matriz disponible.
  - Se puede definir varios ThinkSystem M. 2 con adaptadores de almacenamiento de duplicación, cada uno en una ranura PCI diferente.
  - En el caso de servidores Edge ThinkSystem, debe especificar un número de ranura de PCI específico. Para otros servidores ThinkSystem que tienen solo un adaptador RAID M.2 instalado, puede elegir la primera coincidencia (el valor predeterminado) o especificar un número de ranura de PCI específico.
- **Memoria persistente de Intel Optane DC**. Elija el tipo de memoria persistente, el umbral de advertencia para el porcentaje de capacidad restante y de capacidad total que se utiliza como memoria. (La memoria restante se utiliza como almacenamiento persistente).

  Atención:
  - Para configurar DIMM de memoria persistente de Intel Optane DC, se debe deshabilitar la seguridad y no se debe crear un espacio de nombres.
  - Solo se permite habilitar la seguridad cuando el estado de seguridad es "Disabled" (Deshabilitado) para todos los DIMM de memoria persistente de Intel Optane DC en el servidor.
  - Solo se permite la deshabilitación de seguridad y el borrado seguro cuando el estado de seguridad es "Locked" (Bloqueado) y la frase de contraseña es la misma para todos los DIMM de memoria persistente Intel Optane DC en el servidor.
  - El estado de seguridad de Intel Optane DC PMEM no está incluido en el inventario de XClarity Administrator. Puede comprobar el estado de seguridad de UEFI manualmente.

- **Conservar configuración de almacenamiento existente en el destino**. No se cambia la configuración de almacenamiento existente durante el despliegue. Elija esta opción para utilizar la configuración de almacenamiento que ya se está utilizando en el servidor de destino.
- **Disable local disk**. (Solo Nodo de cálculo Flex System x240) Durante el despliegue, se deshabilitan el controlador de almacenamiento incorporado y la opción de almacenamiento ROM (tanto de UEFI como de valores heredados). Al deshabilitar la unidad de disco local disminuye el tiempo de arranque global cuando se arranca desde SAN.

Definición de adaptadores de E/S

Puede definir los valores de los puertos de E/S y el modo de direccionamiento que se van a aplicar a los servidores de destino cuando se despliegue este patrón.

Acerca de esta tarea

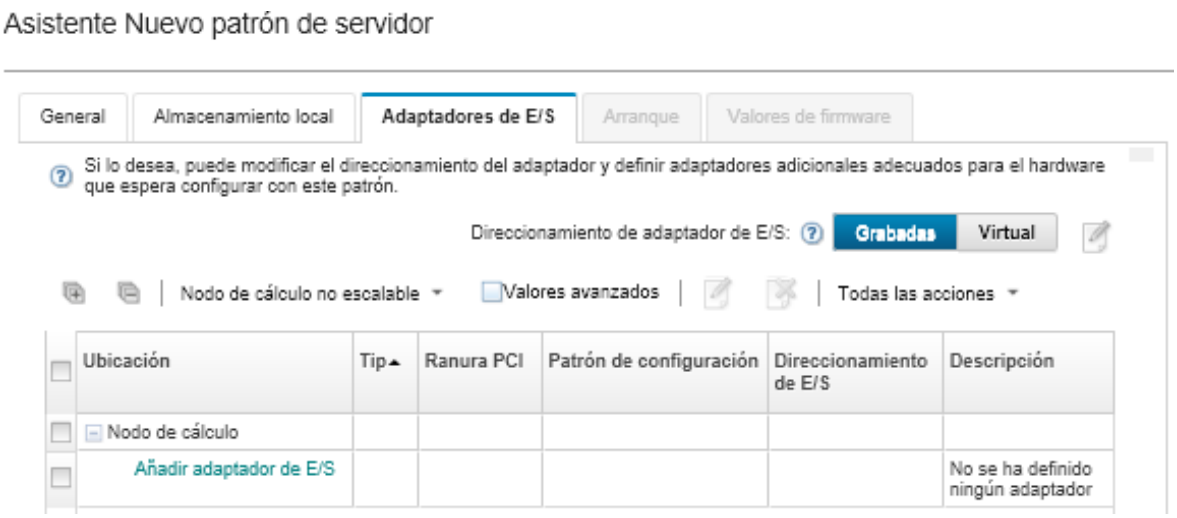
Si tiene previsto virtualizar o reasignar las direcciones del adaptador de E/S, puede configurar este patrón para usar el direccionamiento de adaptador de E/S virtual.

Si crea un patrón a partir de un servidor existente, parte de la información del adaptador se podría extraer automáticamente. Puede definir patrones de adaptador de E/S adicionales para que coincidan con el hardware que espera tener en los servidores cuando se despliegue este patrón. Al definir patrones de adaptador de E/S, puede configurar valores de puerto para el adaptador compatible. Si utiliza direcciones de adaptador de E/S virtuales, también puede definir destinos de arranque de SAN para los adaptadores de Fibre Channel que ha añadido (consulte Definición de opciones de arranque).

Procedimiento

Para definir los valores de los adaptadores de E/S, lleve a cabo los pasos siguientes.

Paso 1. En el Asistente Nuevo patrón de servidor, haga clic en la pestaña **Adaptadores de E/S**.



Nota: Puede mostrar información adicional sobre los adaptadores de E/S pulsando **Valores avanzados**.

Paso 2. Si va a crear un patrón de servidor para un servidor en un chasis de Flex System, elija el tipo de modo de direccionamiento del adaptador de E/S:

- **Grabado**. Utilice las direcciones World Wide Name (WWN) y Media Access Control (MAC) que se proporcionan de fábrica con el adaptador.
- **Virtual**. Utilice el direccionamiento de adaptador de E/S virtual para simplificar la gestión de las conexiones LAN y SAN. La virtualización de direcciones de E/S reasigna las direcciones de hardware grabadas con direcciones de fibra WWN y Ethernet MAC virtualizadas, lo que puede acelerar el despliegue preconfigurando la calidad de miembro de la zona SAN, así como facilitar la conmutación por error eliminando la necesidad de volver a configurar las zonas SAN y las asignaciones de enmascaramiento LUN al sustituir el hardware.

  Cuando se habilita el direccionamiento virtual, tanto las direcciones de Ethernet como las de Fibre Channel se asignan de manera predeterminada independientemente de los adaptadores definidos. Puede elegir el grupo desde el cual se asignan las direcciones de Ethernet y las de Fibre Channel.

  También puede editar los valores de las direcciones virtuales haciendo clic en el icono **Editar** ( ) que se encuentra situado junto a los modos de dirección.

  Restricción: UI direccionamiento virtual solo se admite para los servidores del chasis de Flex System. No se admiten los servidores de bastidor y de torre.

Paso 3. Si va a crear un patrón de servidor para un servidor en un chasis de Flex System, seleccione una de las siguientes opciones de escalabilidad. Las filas de la tabla cambian según lo que se seleccione.
- Flex System no escalable
- Flex System de 2 nodos escalables
- Flex System de 4 nodos escalables

Paso 4. Elija los adaptadores de E/S que espera que estén instalados en los servidores en los cuales se va a desplegar el patrón. Para añadir un adaptador:

a. Haga clic en el enlace **Añadir adaptador de E/S** en la tabla para mostrar el cuadro de diálogo Añadir adaptador de E/S 1 o LOM.

b. Seleccione la ranura PCI del adaptador.

c. Seleccione el tipo de adaptador en la tabla.

Nota: De forma predeterminada, la tabla enumera únicamente los adaptadores de E/S actualmente instalados en los servidores gestionados. Para ver todos los adaptadores de E/S, haga clic en **Todos los adaptadores admitidos**.

d. Seleccione el patrón de puerto inicial que se asignará a todos los puertos del grupo de puertos cuando se despliegue el patrón.

Los *patrones de puertos* se utilizan para modificar los valores de puertos que se van a extraer del servidor. Estos patrones de puerto iniciales se asignan cuando el adaptador se añade por primera vez. Después de añadir el adaptador, puede asignar distintos patrones a puertos individuales desde la página Adaptador de E/S.

Puede crear un patrón de puerto haciendo clic en el icono **Crear** (). Puede crear un patrón de puerto basado en un patrón existente haciendo clic en el icono **Editar** ().

Para obtener más información sobre patrones de puertos, consulte Definición de los valores de puerto.

e. Pulse **Añadir** para añadir el patrón de puerto a la tabla de la página Adaptador de E/S.

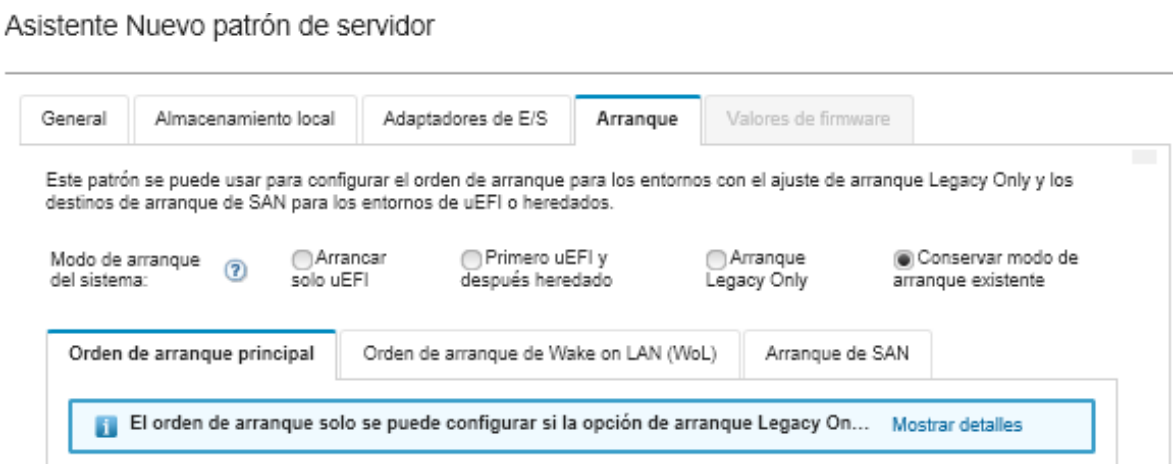
Definición de opciones de arranque

Puede definir el orden de arranque que debe aplicarse a los servidores de destino al desplegar este patrón.

Procedimiento

Lleve a cabo los pasos siguientes para crear un patrón de opciones de arranque.

Paso 1. En el Asistente Nuevo patrón de servidor, haga clic en la pestaña **Boot**.



Paso 2. Seleccione uno de los siguientes modos de arranque del sistema:

- **Arrancar solo UEFI**. Seleccione esta opción para configurar un servidor compatible con la Unified Extensible Firmware Interface (UEFI). Si arranca sistemas operativos habilitados para la UEFI, esta opción podría acortar el tiempo de arranque deshabilitando la opción de ROM de valores heredados.

  Si el patrón se aprende desde un servidor Thinksystem, puede hacer clic en la pestaña **Orden de arranque principal** para especificar el orden de arranque. Puede mantener el orden de arranque especificado en el servidor en el que se va a desplegar el patrón o bien configurar el orden de arranque para especificar el orden en el que deben aplicarse las opciones de arranque. Sin embargo, no se admite la prioridad de arranque de los dispositivos de arranque en un grupo de dispositivos (opción de arranque).

- **Primero UEFI y después heredado**. Seleccione esta opción para configurar un servidor y tratar de arrancar utilizando primero UEFI. Si hay un problema, el servidor intenta arrancar en modo heredado.

  Si el patrón se aprende desde un servidor Thinksystem, puede hacer clic en la pestaña **Orden de arranque principal** para especificar el orden de arranque. Puede mantener el orden de arranque especificado en el servidor en el que se va a desplegar el patrón o bien configurar el orden de arranque para especificar el orden en el que deben aplicarse las opciones de arranque. Sin embargo, no se admite la prioridad de arranque de los dispositivos de arranque en un grupo de dispositivos (opción de arranque).

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

  Consejo: Si selecciona el modo Arrancar solo heredado (que hace que el tiempo de arranque sea mucho más rápido), no puede activar ninguna clave de característica bajo demanda (FoD).

  Si elige esta opción, puede especificar:

  – **Orden de arranque principal**. Elíjalo para mantener el orden de arranque especificado en el servidor en el que se va a desplegar el patrón. También puede elegir configurar el orden de arranque Arrancar solo heredado para especificar el orden en el que deben aplicarse las opciones de arranque.

  – **Orden de arranque de Wake on LAN (WoL)**. Elíjalo para mantener el orden de arranque WoL actual en el servidor en el que se va a desplegar el patrón. También puede elegir configurar el orden de arranque Arrancar solo heredado para especificar el orden en el que deben aplicarse las opciones de arranque WoL.

- **Conservar modo de arranque existente**. Seleccione esta opción para mantener los valores existentes en el servidor de destino. No se realizarán cambios en el orden de arranque cuando se despliegue el patrón.

Paso 3. Seleccione la pestaña **Arranque de SAN** para elegir un patrón de destino de arranque y especificar los destinos delos dispositivos de arranque.

Nota: Si definió adaptadores de Fibre Channel y habilitó el direccionamiento virtual al definir los adaptadores de E/S, puede establecer los destinos de arranque principal y secundario de SAN para los adaptadores de Fibre Channel. Puede especificar varios nombres de puertos de todo el mundo (WWPN) e identificadores de número de unidad lógica (LUN) para los destinos de almacenamiento.

Definición de valores de firmware

Puede especificar los valores de firmware del controlador de gestión de la placa base y de la UEFI que se van a aplicar a los servidores de destino cuando se despliegue este patrón.

Acerca de esta tarea

Los valores de firmware están organizados en categorías que agrupan los valores relacionados. Para cada categoría, puede crear un *patrón de categoría* que contenga los valores de firmware comunes y pueda reutilizarse en varios patrones de servidor. La mayoría de los valores de firmware que se pueden configurar directamente en el servidor del controlador de gestión de la placa base y de la UEFI también se pueden configurar a través de patrones de categorías. Los valores de firmware que están disponibles dependen del tipo de servidor, de su entorno de Flex System y del ámbito del patrón de servidor.

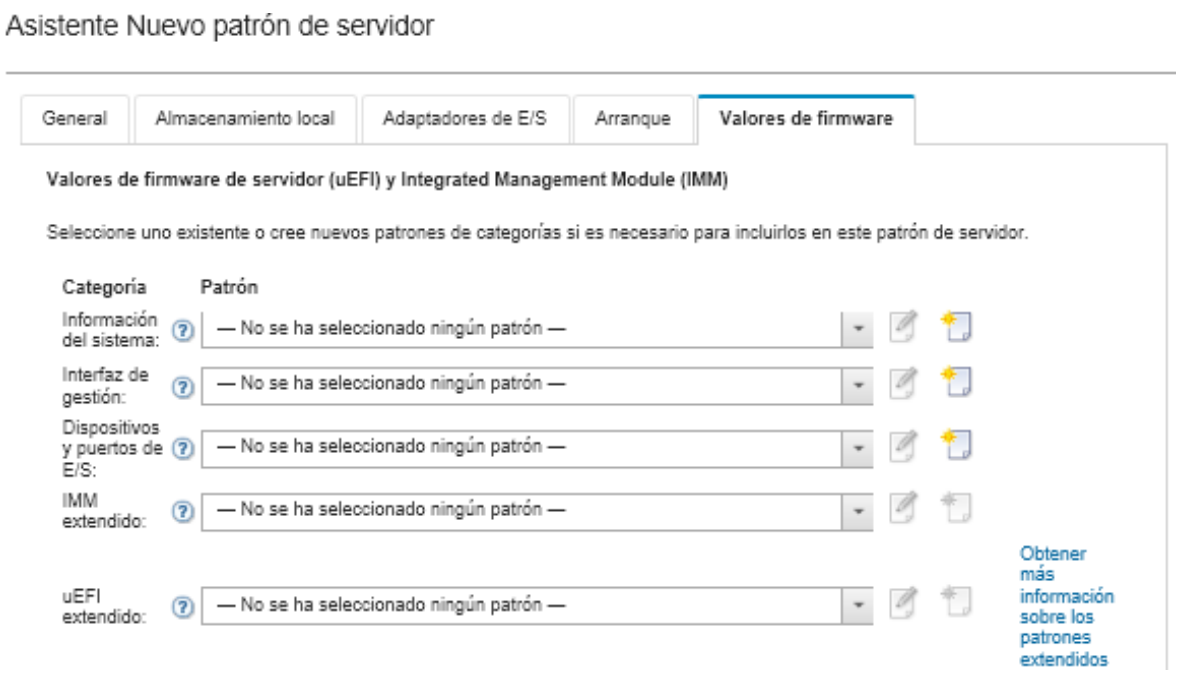
Los patrones de categoría pueden ser predefinidos, definidos por el usuario o extraídos de los servidores existentes.

- Los *patrones de categorías extendidos* son patrones para los valores de algunos puertos de adaptadores de E/S, de Unified Extensible Firmware Interface (UEFI) avanzada y del controlador de gestión de la placa base (BMC), que se extraen y se crean dinámicamente desde un servidor gestionado específico. Lenovo XClarity Administrator crea estos patrones cuando se crea un patrón de servidor a partir de un servidor existente. No se pueden crear manualmente patrones de categorías extendidos; sin embargo, sí se pueden editar después de haberlos creado.
- Los *patrones de categorías definidos por el usuario* son los patrones que el usuario puede crear, incluidos la información del sistema, las interfaces de gestión, los dispositivos y puertos de E/S, los destinos de arranque de Fibre Channel y los puertos de adaptadores de E/S.

Procedimiento

Lleve a cabo los pasos siguientes para definir los valores de firmware.

Paso 1. En el Asistente Nuevo patrón de servidor, haga clic en la pestaña **Valores de firmware**.



Paso 2. Elija el tipo de patrón de categoría que incluya los valores que desee definir.

- **Información del sistema**. Utilice este patrón de categoría para definir la generación automática del nombre del sistema, los nombres de contacto y las ubicaciones. Para obtener más información sobre los patrones de información del sistema, consulte Definición de los valores de la información del sistema.
- **Interfaces de gestión**. Utilice este patrón de categoría para definir la generación automática del nombre de host, asignaciones de direcciones IP de gestión, valores de sistema de nombres de dominio (DNS) y valores de velocidad de Internet. Para obtener más información acerca de los patrones de las interfaces de gestión, consulte Definición de los valores de la interfaz de gestión.
- **Dispositivos y puertos de E/S**. Utilice este patrón de categoría para definir la redirección de la consola y los puertos COM, la velocidad del PCIe, los dispositivos incorporados, la opción ROM del adaptador y el orden de ejecución de la opción ROM. Para obtener más información acerca de los patrones de dispositivos y puertos de E/S, consulte Definición de los valores de los dispositivos y puertos de E/S.
- **BMC extendido**. Utilice este patrón de categoría para definir otros valores del controlador de gestión de la placa base. Los patrones de los valores del controlador de gestión se crean automáticamente al crear un patrón de servidor desde un servidor existente. No se puede crear manualmente un patrón del controlador de gestión extendido. Para obtener más información acerca de los patrones de las interfaces de gestión, consulte Definición de configuración de controlador de gestión extendido.
- **UEFI extendido**. Utilice este patrón de categoría para definir otros valores de Unified Extensible Firmware Interface (UEFI). Los patrones extendidos de la UEFI se crean automáticamente al crear un patrón de servidor desde un servidor existente. No se puede crear manualmente un patrón de UEFI extendido. Para obtener más información acerca de los patrones de las interfaces de gestión, consulte Definición de los valores extendidos de UEFI.

Paso 3. Cree nuevos patrones de categorías pulsando el icono **Crear** ( ) que se encuentra situado junto a dicho tipo de patrón de categoría.

También puede editar un patrón de categoría existente seleccionando un patrón específico en la lista desplegable y haciendo clic en el icono **Editar** ( ) que se encuentra situado junto a dicho tipo

de patrón de categoría. También puede copiar un patrón de categoría existente editando el patrón y pulsando **Guardar como** para guardarlo con un nombre nuevo.

Definición de los valores de la información del sistema

Puede crear un patrón de información del sistema para definir la información de nombre del sistema, contacto y ubicación.

Procedimiento

Lleve a cabo los pasos siguientes para crear un patrón de información del sistema.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Aprovisionamiento → Patrones**. Se muestra la página Patrones de configuración: Patrones.

Paso 2. Haga clic en la pestaña **Patrones de categorías**.

Paso 3. Haga clic en la pestaña vertical **Patrones de información del sistema** y haga clic en el icono **Crear** ( ).

Consejo: también puede crear un nuevo patrón de información del sistema desde la página Valores de firmware del asistente Nuevo patrón de servidor haciendo clic en el icono **Crear** que se encuentra situado junto a la selección **Información del sistema**.

Paso 4. En el cuadro de diálogo Nuevo patrón de información del sistema, especifique la siguiente información.

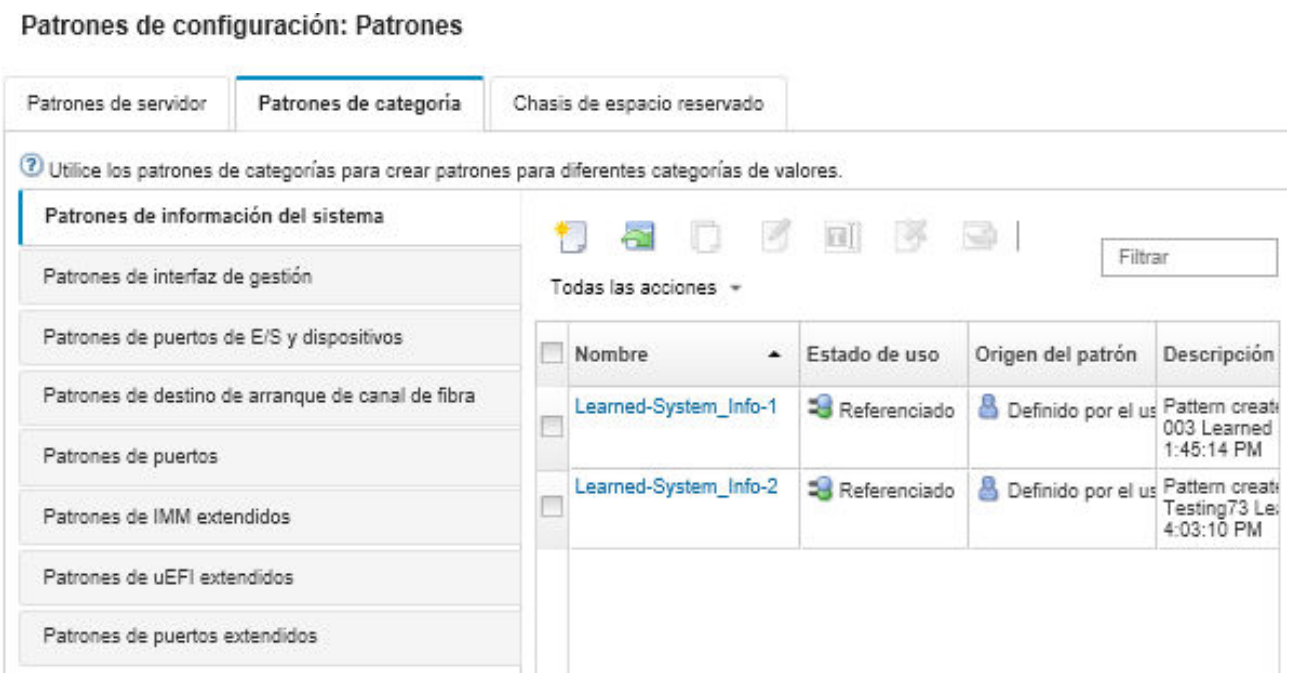
- Introduzca el nombre y la descripción del patrón.
- Elija si se van a generar los nombres de sistemas automáticamente o no. Si pulsa **Personalizado**, puede especificar cómo se generan los nombres cuando se despliega el patrón. Si pulsa **Deshabilitar**, el nombre del sistema se mantiene sin cambios en cada servidor cuando se despliega el patrón. En la mayor parte de los dispositivos, el nombre tiene un límite de 256 caracteres en inglés determinado por el controlador de gestión de la placa base. Los nombres generados automáticamente se truncan en 256 caracteres.
- Especifique la persona a contactar para este servidor y la ubicación del mismo.

  Nota: Si SNMP está habilitado, debe especificar un contacto y una ubicación del sistema.

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

Resultados

El nuevo patrón se muestra en la pestaña **Patrones de información del sistema** de la página Patrones de configuración: Patrones de categorías:



Desde esta página, puede realizar también las acciones siguientes en el patrón de categoría seleccionado:

- Modificar los valores del patrón actual haciendo clic en el icono **Editar** ( ).
- Copiar un patrón existente haciendo clic en el icono **Copiar** ( ).
- Eliminar un patrón haciendo clic en el icono **Eliminar** ( ).
- Cambiar el nombre de un patrón haciendo clic en el icono **Cambiar nombre** ( ).
- Importar y exportar patrones de servidor (consulte Exportación e importación de patrones de servidor y categorías).

Definición de los valores de la interfaz de gestión

Puede crear un patrón de interfaz de gestión para definir los nombres de host, la dirección IP, el sistema de nombre de dominio (DNS), la velocidad de interfaz y las asignaciones de puertos para la interfaz de gestión.

Procedimiento

Lleve a cabo los pasos siguientes para crear un patrón de interfaz de gestión.

Nota: Los patrones de servidor no admiten valores dúplex.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Aprovisionamiento → Patrones**. Se muestra la página Patrones de configuración: Patrones.

Paso 2. Haga clic en la pestaña **Patrones de categorías**.

Paso 3. Haga clic en la pestaña vertical **Patrones de interfaz de gestión** y haga clic en el icono **Crear** ( ).

Consejo: también puede crear un nuevo patrón de interfaz de gestión desde la página Valores de firmware del asistente Nuevo patrón de servidor pulsando el icono **Crear** ( ) que se encuentra situado junto a la selección **Interfaz de gestión**.

Paso 4. En el cuadro de diálogo Nuevo patrón de interfaz de gestión, especifique la siguiente información.

- Introduzca el nombre y la descripción del patrón.

- Haga clic en la pestaña **Nombre de host** y elija si genera los nombres de host automáticamente o no. Si pulsa **Personalizado**, puede especificar cómo se generan los nombres cuando se despliega el patrón. Si pulsa **Deshabilitar**, el nombre de host se mantiene sin cambios en cada servidor cuando se despliega el patrón.

  El controlador de gestión de la placa base limita los nombres de host a 63 caracteres en inglés. Los nombres generados automáticamente se truncan en 63 caracteres.
- Haga clic en la pestaña **Direcciones IP de gestión** y configure los valores de las direcciones IPv4 e IPv6.

  Para las direcciones **IPv4** puede elegir una de las siguientes opciones:
  - **Obtenga una dirección IP dinámica del servidor DHCP**.
  - **Primero por DHCP**. Si no es satisfactorio, obtener una dirección IP estática del grupo de direcciones.
  - **Obtener una dirección IP estática del grupo de direcciones.**

  Para las direcciones **IPv6** puede elegir:

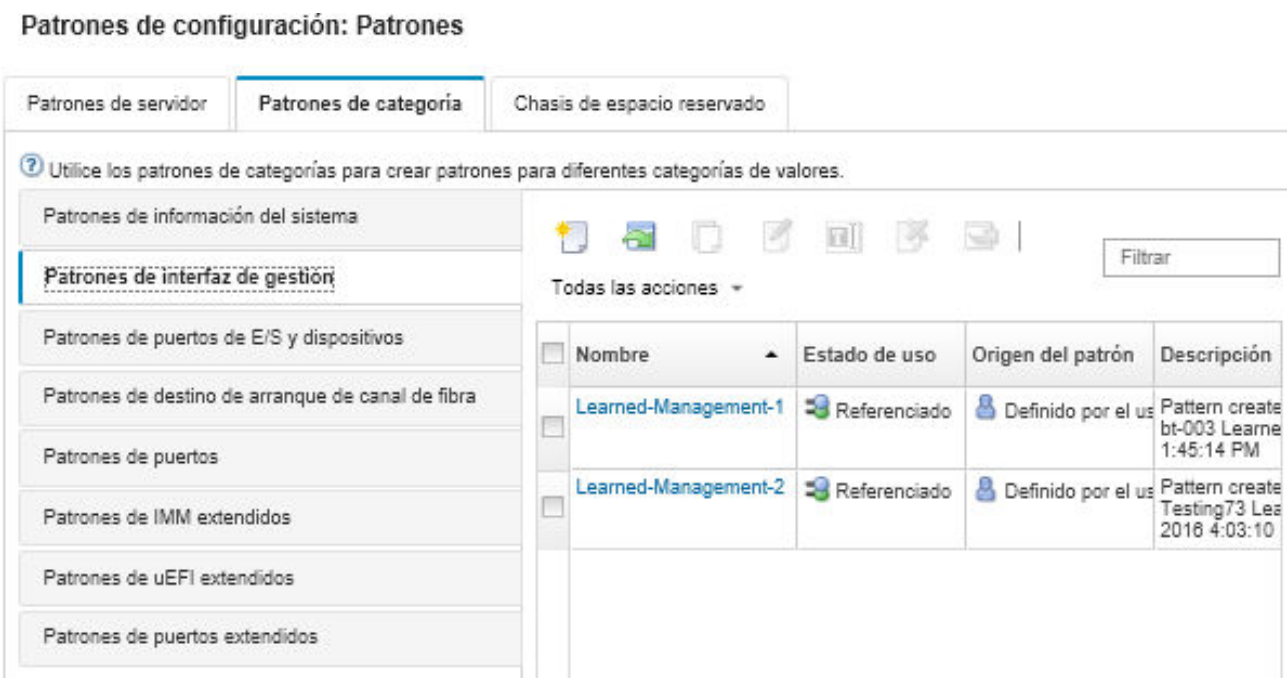
  - **Utilizar la configuración automática de dirección sin estado**.
  - **Obtener una dirección IP dinámica desde un servidor DHCP**.
  - **Obtener una dirección IP estática del grupo de direcciones**.

  En la pestaña **Sistema de nombres de dominio (DNS)**, elija entre habilitar y deshabilitar el Servicio del nombre de dominio dinámico (DDNS). Si habilita DDNS, puede elegir una de las siguientes opciones:
  - Obtener nombre de dominio del servidor DHCP.
  - Especifique un nombre de dominio.
- Haga clic en la pestaña **Valores de la interfaz** y especifique la unidad de transmisión máxima (MTU). El valor predeterminado es 1500.
- Haga clic en la pestaña **Asignaciones de puertos** y especifique los números que se van a utilizar para los siguientes puertos:
  - HTTP
  - HTTPS
  - Telnet CLI
  - SSH CLI
  - Agente SNMP
  - Trampas SNMP
  - Consola de control remoto
  - CIM sobre HTTP
  - CIM sobre HTTPS

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

Resultados

El nuevo patrón se muestra en la pestaña **Patrones de interfaz de gestión** de la página Patrones de configuración: Patrones de categorías:



Desde esta página, puede realizar también las acciones siguientes en el patrón de categoría seleccionado:

- Modificar los valores del patrón actual haciendo clic en el icono **Editar** ( ).
- Copiar un patrón existente haciendo clic en el icono **Copiar** ( ).
- Eliminar un patrón haciendo clic en el icono **Eliminar** ( ).
- Cambiar el nombre de un patrón haciendo clic en el icono **Cambiar nombre** ( ).
- Importar y exportar patrones de servidor (consulte Exportación e importación de patrones de servidor y categorías).

Definición de los valores de los dispositivos y puertos de E/S

Puede habilitar el redireccionamiento de la consola y habilitar y definir las características del puerto COM 1; para ello, debe crear un dispositivo y un patrón de puertos de E/S.

Procedimiento

Para crear un patrón de dispositivos y puertos de E/S, lleve a cabo los pasos siguientes.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Aprovisionamiento → Patrones**. Se muestra la página Patrones de configuración: Patrones.

Paso 2. Haga clic en la pestaña **Patrones de categorías**.

Paso 3. Haga clic en la pestaña vertical **Patrones de dispositivos y puertos de E/S**; a continuación, haga clic en el icono **Crear** ( ).

Consejo: también puede crear un nuevo patrón de dispositivos y puertos de E/S desde la página Valores de firmware del asistente Nuevo patrón de servidor pulsando el icono **Crear** ( ) situado junto a la selección **Devices and I/O Ports**.

Paso 4. En el cuadro de diálogo Nuevo patrón de dispositivos y puertos de E/S, especifique la siguiente información.

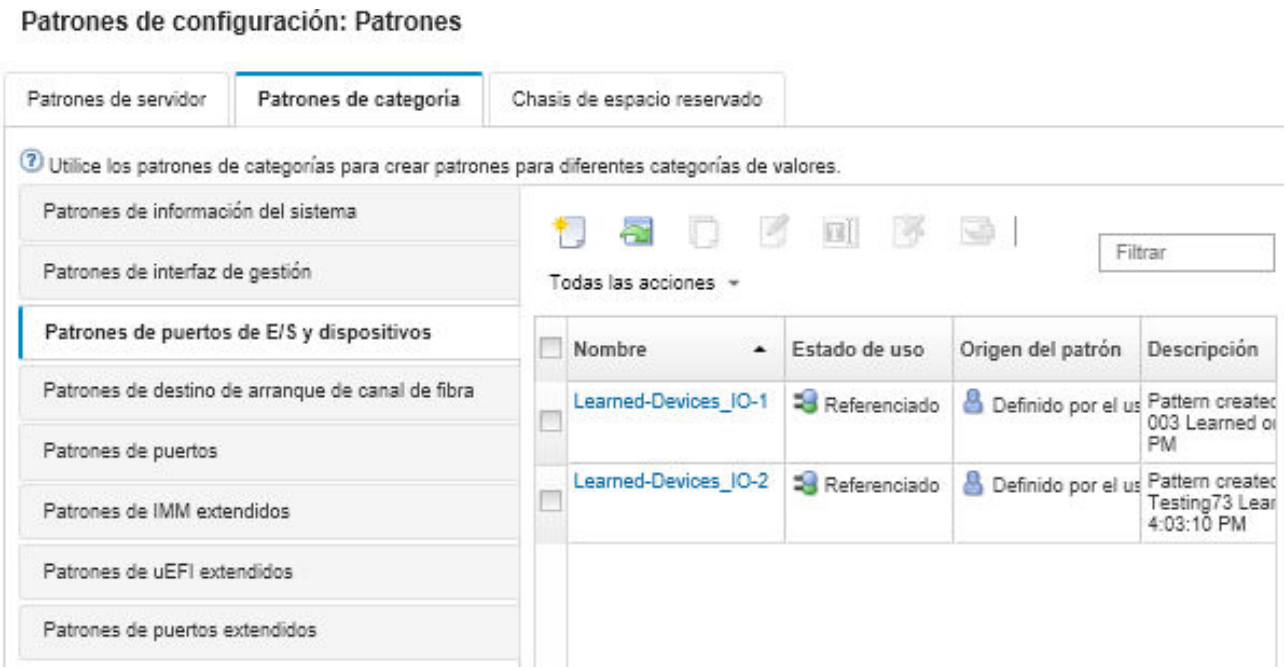
- Introduzca el nombre y la descripción del patrón.
- Elija entre habilitar o deshabilitar el redireccionamiento de la consola. Si habilita el redireccionamiento de la consola, puede elegir entre habilitar o deshabilitar lo siguiente:

  - **Serie sobre IP**.
  - **Redireccionamiento del procesador de servicios**. Si habilita el redireccionamiento del procesador de servicios, puede elegir utilizar el puerto COM 1 o 2 para el puerto de datos en serie opcional heredado. Tenga en cuenta que si se deshabilita, el puerto COM 1 siempre se utiliza.También puede elegir uno de los siguientes modos de CLI:
    - Deshabilitar
    - Habilitar con la secuencia de teclas definida por el usuario
    - Habilitar con la secuencia de teclas compatible con ESM
- Elija entre habilitar o deshabilitar los puertos COM 1 y 2. Si elige habilitarlos, especifique los siguientes valores:
  - Velocidad en baudios
  - Bits de datos
  - Paridad
  - Bits de parada
  - Emulación de texto
  - Activar tras el arranque
  - Control de flujo

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

Resultados

El nuevo patrón se muestra en la pestaña **Patrones de dispositivos y puertos de E/S** de la página Patrones de configuración: Patrones de categorías:



Desde esta página, puede realizar también las acciones siguientes en el patrón de categoría seleccionado:

- Modificar los valores del patrón actual haciendo clic en el icono **Editar** ( ).
- Copiar un patrón existente haciendo clic en el icono **Copiar** ( ).
- Eliminar un patrón haciendo clic en el icono **Eliminar** ( ).
- Cambiar el nombre de un patrón haciendo clic en el icono **Cambiar nombre** ( ).

- Importar y exportar patrones de servidor (consulte Exportación e importación de patrones de servidor y categorías).

Definición de los valores del destino de arranque del Fibre Channel

Puede configurar el servidor de modo que arranque desde un dispositivo de red de área de almacenamiento (SAN) en vez de hacerlo desde una unidad de disco local; para ello, debe crear un patrón de destino de arranque de Fibre Channel.

Procedimiento

Lleve a cabo los pasos siguientes para crear un patrón de destino de arranque de Fibre Channel.

Restricción: los destinos de arranque de Fibre Channel solo son compatibles con los nodos de cálculo Flex. No se admiten los servidores de bastidor y de torre autónomos.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Aprovisionamiento** → **Patrones**. Se muestra la página Patrones de configuración: Patrones.

Paso 2. Haga clic en la pestaña **Patrones de categorías**.

Paso 3. Haga clic en la pestaña vertical **Patrón de destino de arranque de Fibre Channel** y, a continuación, haga clic en el icono **Crear** ( ).

Paso 4. En el cuadro de diálogo Nuevo patrón de destino de arranque de Fibre Channel, especifique la siguiente información.

- Introduzca el nombre y la descripción del patrón.
- Especifique una o más direcciones WWPN e identificadores de LUN para utilizar como destinos de arranque principales. Además, puede especificar opcionalmente una o más direcciones WWPN e identificadores de LUN para utilizar como destinos de arranque secundarios.

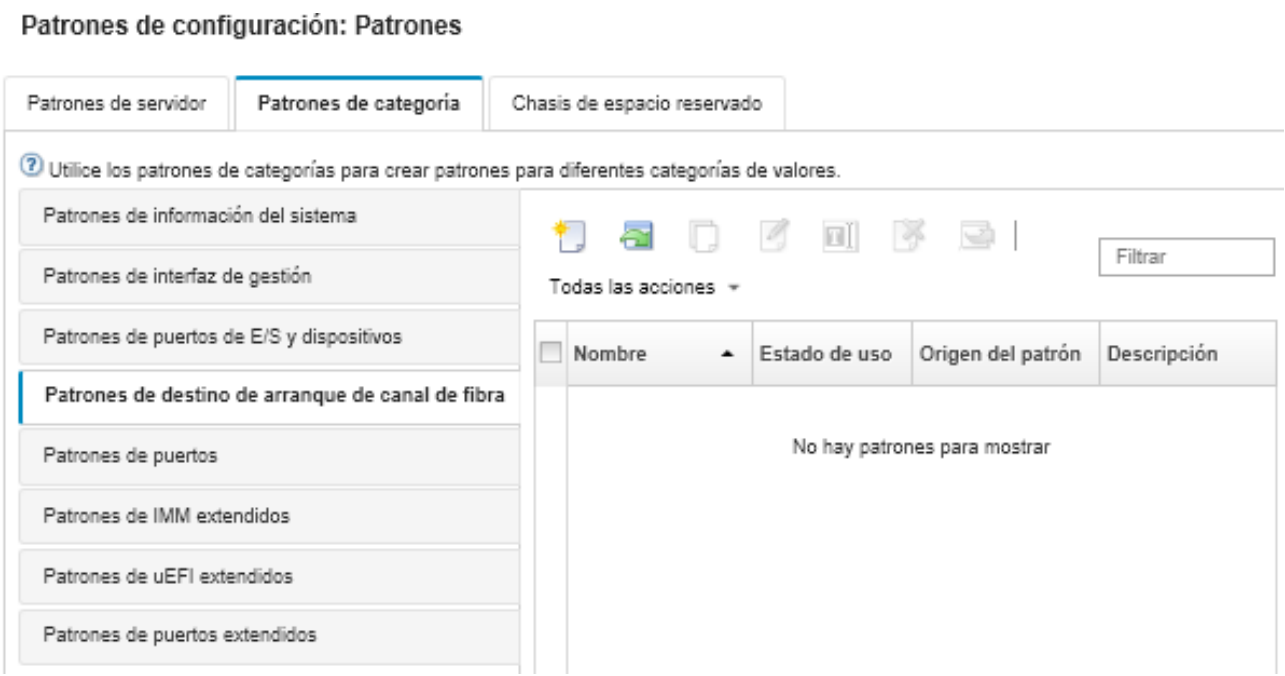
  Por ejemplo, puede añadir las rutas principales de almacenamiento como destinos principales y las rutas secundarias de almacenamiento como destinos secundarios. Si utiliza grupos de destino distintos en diferentes patrones de servidor, puede equilibrar la carga de almacenamiento cuando haya solicitudes de arranque simultáneas desde varios hosts.

  Consejo: si especifica `00:00:00:00:00:00:00:00` para las direcciones WWPN, XClarity Administrator intenta arrancar desde el primer destino detectado.

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

Resultados

El nuevo patrón se muestra en la pestaña **Patrones de destino de arranque de Fibre Channel** de la página Patrones de configuración: Patrones de categorías:



Desde esta página, puede realizar también las acciones siguientes en el patrón de categoría seleccionado:

- Modificar los valores del patrón actual haciendo clic en el icono **Editar** ( ).
- Copiar un patrón existente haciendo clic en el icono **Copiar** ( ).
- Eliminar un patrón haciendo clic en el icono **Eliminar** ( ).
- Cambiar el nombre de un patrón haciendo clic en el icono **Cambiar nombre** ( ).
- Importar y exportar patrones de servidor (consulte Exportación e importación de patrones de servidor y categorías).

Definición de los valores de puerto

Mediante la creación de un patrón de puerto, puede definir los valores de puerto típicos de un tipo de adaptador de E/S específico.

Acerca de esta tarea

Puede utilizar los valores de red en patrones de puerto para configurar los puertos internos de un conmutador. No obstante, no puede utilizar patrones de puerto para configurar los valores globales de un conmutador, como los ID de VLAN, el modo UFP global, el modo CEE global y las FIP globales. Antes de desplegar los patrones de puerto, debe configurar manualmente los valores globales utilizando las reglas siguientes, si son compatibles con los valores de puerto interno que pretende desplegar. Tampoco puede utilizar patrones de puerto para configurar el etiquetado PVID. Consulte la documentación incluida con su conmutador para determinar las comprobaciones de compatibilidad entre los valores globales y los valores de puerto interno, así como para saber cómo configurar dichos valores para este conmutador.

- Asegúrese de que **globalCEEState** esté establecido en “Activado” si se ha configurado el PFC.
- Asegúrese de que **globalCEEState** esté establecido en “Activado” si vport se ha configurado en el modo “FCoE”.
- Asegúrese de que **globalCEEState** esté establecido en “Activado” y de que **globalFIPsState** esté establecido en “Activado” si se han configurado FIP.

- Asegúrese de que **globalUFPMode** esté establecido en “Habilitar” si el modo de puerto interno del conmutador se ha configurado en el modo “UFP”.
- Asegúrese de que el Id. de VLAN se creó antes de agregar un puerto a una VLAN específica.

Procedimiento

Lleve a cabo los pasos siguientes para crear un patrón de puerto de adaptador de E/S.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Aprovisionamiento → Patrones**. Se muestra la página Patrones de configuración: Patrones.

Paso 2. Haga clic en la pestaña **Patrones de categorías**.

Paso 3. Haga clic en la pestaña vertical **Patrón de puerto** y, a continuación, haga clic en el icono **Crear** ( ).

Consejo: también puede crear un nuevo patrón de puerto desde la página Añadir adaptador de E/S haciendo clic en el icono **Crear** ( ), que se encuentra situado junto a la selección **Patrón de puertos inicial**.

Paso 4. En el cuadro de diálogo Nuevo patrón de puerto, especifique la siguiente información.

- Introduzca el nombre y la descripción del patrón.
- Especifique siguientes valores de compatibilidad del adaptador y el puerto. Cuando se asignan patrones a adaptadores y puertos, los valores de los patrones se filtran basándose en la compatibilidad con el adaptador o el puerto de destino.
  - Tipo de adaptador de destino
  - Modo operativo de puerto de destino, que incluye:
    - Modo pNIC
    - Modo de entramado virtual vNIC
    - Modo independiente de conmutador vNIC
    - Modo de protocolo de entramado unificado vNIC

    Estos valores habilitan la virtualización NIC. Para obtener más información, consulte el apartado Virtualización de NIC en soluciones de Flex System Fabric.
  - Protocolos de puertos de destino, incluidos:
    - Solo Ethernet
    - Ethernet y FCoE
    - Ethernet e iSCSI
  - Patrón de valores extendidos del puerto, que se utiliza para configurar valores de puerto adicionales que se extraen del servidor.
- Si establece el modo operativo del puerto de destino en **Modo pNIC**, elija aplicar los valores correspondientes a los puertos internos del conmutador Flex cuando proceda. Si se ha seleccionado, puede configurar una VLAN adicional y valores avanzados:
  - Especifique el protocolos de puerto de destino.
  - Si establece el protocolo de puerto de destino en **Ethernet y FCoE**, puede seleccionar y especificar opcionalmente el Id. de prioridad 2.
- Si establece el modo operativo del puerto de destino en **Modo de entramado virtual vNIC**, configure los valores de la función física, incluidos el tipo y la etiqueta de VLAN de cada función.
- Si establece el modo operativo del puerto de destino en **Modo independiente de conmutador vNIC**, especifique el tipo, el ancho de banda mínimo y la etiqueta VLAN para cada función habilitada. También puede elegir aplicar los valores correspondientes a los puertos internos del conmutador Flex cuando proceda. Si está seleccionado, puede configurar un puerto interno de conmutador adicional y valores avanzados:

- Especifique la LAN predeterminada, que el sistema operativo solo utiliza cuando envía paquetes sin etiquetar.
- Escriba una lista de VLAN separada por comas.
- Elija configurar el control manual y especifique los activadores.
- Elija configurar el tipo de control de flujo, lo que incluye:
  - Mantener control de flujo existente
  - Control de flujo basado en prioridades
  - Control de flujo de nivel de vínculo

  Para obtener más información sobre estos tipos de control de flujo, consulte la documentación suministrada con el conmutador Flex.

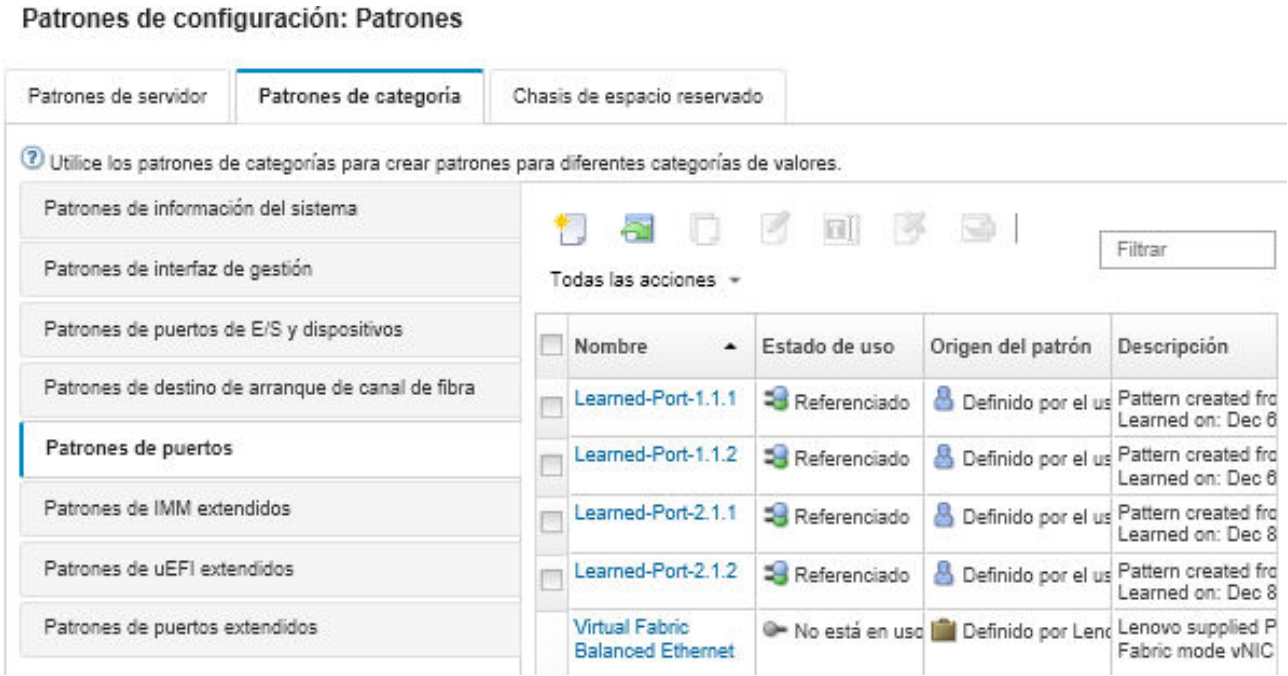
- Si establece el modo operativo del puerto de destino en **Modo de protocolo de entramado unificado vNIC**, elija aplicar los valores correspondientes a los puertos internos del conmutador Flex cuando proceda. Si se ha seleccionado, puede configurar una función de UFP adicional y valores avanzados:
  - Especifique el modo de QoS (ancho de banda o prioridad).
  - Elija habilitar el etiquetado de Id. de VLAN predeterminado y especifique el modo, el ancho de banda mínimo y la etiqueta de VLAN para cada función habilitada.
  - Elija configurar el error de capa 2 y especifique el número de activadores para cada función.
  - Para el modo de QoS de ancho de banda, especifique el tipo de control de flujo (según el orden de prioridad, nivel de vínculo o control de flujo existente).
  - Para el modo de QoS de ancho de banda, elija si está habilitada la prioridad 4 cuando se selecciona iSCSI.

  Nota: Asegúrese de que la conmutación por error global esté “Activada” a definir la activación de la conmutación por error.

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

Resultados

El nuevo patrón se muestra en la pestaña **Patrones de puertos** de la página Patrones de configuración: Patrones de categorías:



Desde esta página, puede realizar también las acciones siguientes en el patrón de categoría seleccionado:

- Modificar los valores del patrón actual haciendo clic en el icono **Editar** ().
- Copiar un patrón existente haciendo clic en el icono **Copiar** ().
- Eliminar un patrón haciendo clic en el icono **Eliminar** ().
- Cambiar el nombre de un patrón haciendo clic en el icono **Cambiar nombre** ().
- Importar y exportar patrones de servidor (consulte Exportación e importación de patrones de servidor y categorías).

Definición de configuración de controlador de gestión extendido

La configuración de controlador de gestión de la placa base extendido se aprende y crea dinámicamente a partir de un servidor gestionado específico. Lenovo XClarity Administrator crea estos patrones al crear un patrón de servidor desde un servidor existente. No se pueden crear manualmente patrones de controlador de gestión extendido; sin embargo, sí se pueden copiar y modificar aquellos que ya se han creado.

Antes de empezar

Nota: La configuración térmica de IMM podría entrar en conflicto con los valores del modo operativo de UEFI. Si entran en conflicto, los valores de UEFI sobrescriben la configuración de IMM al reiniciar el dispositivo y los valores térmicos que se hayan definido en un patrón del controlador de gestión de placa base extendido quedarán fuera de conformidad. Para resolver el problema de no conformidad, tiene la alternativa de quitar el valor del patrón del controlador de gestión de placa base extendido o de seleccionar valores que no estén en conflicto con el valor del modo operativo de UEFI actual.

Procedimiento

Lleve a cabo los pasos siguientes para modificar los patrones de controlador de gestión extendido.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Patrones**. Se muestra la página Patrones de configuración: Patrones.

Paso 2. Haga clic en la pestaña **Patrones de categorías**.

Paso 3. Haga clic en la pestaña vertical **Patrones de BMC extendidos**.

Paso 4. Seleccione el patrón que desee modificar y, a continuación, haga clic en el icono **Editar** ().

Paso 5. Modifique los campos apropiados.

Puede seleccionar los valores que desee incluir en el patrón de categorías pulsando **Incluir/Excluir** valores.

- Para configurar los valores de DNS, haga clic en **Interfaz de valores de red → Configuración DNS**. Puede habilitar DNS, seleccionar el protocolo IP y especificar hasta tres direcciones IPv4 o IPv6 y habilitar la detección de las direcciones IP de XClarity Administrator.

  Nota: Para los dispositivos Flex System, solo puede configurar la dirección IP que se va a utilizar para detectar el servidor XClarity Administrator.

- Para configurar los valores de NTP, haga clic en **Interfaz de valores de red → Configuración NTP del módulo integrado**. Puede especificar el nombre de host para un máximo de 4 servidores NTP y la frecuencia.

  Nota: Para los dispositivos Flex System, no puede configurar los valores de NTP.

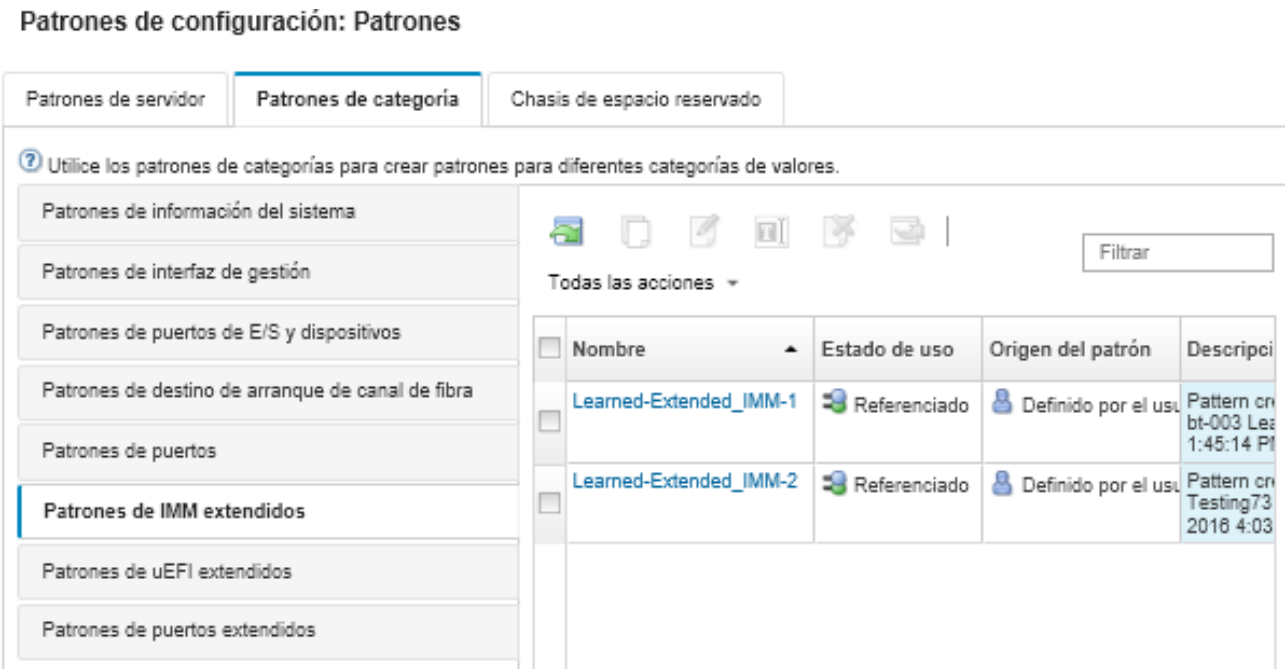
- (Solo servidores de bastidor) A valores de datos y hora, haga clic en **Valores generales → Valores del reloj del módulo integrado**. Puede especificar la zona horaria (desplazamiento UTC), habilitar o deshabilitar el horario de verano (DST) y elegir si va a utilizar la hora UTC o la hora local en el host.

- Para cambiar los valores de seguridad de la cuenta de usuario, haga clic en **Configuración de seguridad de la cuenta**.

Paso 6. Haga clic en **Guardar** para guardar los cambios del patrón de categoría actual o bien haga clic en **Guardar como** para guardar los cambios en un nuevo patrón de categoría.

Resultados

El patrón de categoría modificado se muestra en la pestaña **Patrones de BMC extendidos** de la página Patrones de configuración: Patrones de categorías:



Desde esta página, puede realizar también las acciones siguientes en el patrón de categoría seleccionado:

- Copiar un patrón existente haciendo clic en el icono **Copiar** ( ).
- Eliminar un patrón haciendo clic en el icono **Eliminar** ( ).
- Cambiar el nombre de un patrón haciendo clic en el icono **Cambiar nombre** ( ).
- Importar y exportar patrones de servidor (consulte Exportación e importación de patrones de servidor y categorías).

Definición de los valores extendidos de UEFI

Los valores de Unified Extensible Firmware Interface (UEFI) se aprenden y crean dinámicamente a partir de un servidor gestionado específico. Lenovo XClarity Administrator crea estos patrones al crear un patrón de servidor desde un servidor existente. No se pueden crear manualmente patrones de UEFI extendidos; sin embargo, sí se pueden copiar modificar aquellos que ya se han creado.

Acerca de esta tarea

Los siguientes patrones de UEFI extendida se predefinen mediante Lenovo XClarity Administrator para optimizar los servidores para entornos específicos.

- **Opciones de instalación de ESXi**
- **Eficiencia: favorecer el rendimiento**
- **Modo Eficiencia: favorecer la energía**
- **Rendimiento máximo**

- **Energía mínima**

Notas:

- La modificación de los valores de seguridad de UEFI (incluyendo arranque seguro, módulo de plataforma fiable (TPM) y configuración de la política de presencia física) no se admite utilizando patrones de UEFI extendida.
- Puede modificar la contraseña de administrador de UEFI para servidores ThinkSystem y ThinkAgile seleccionados desde la página Servidores, haciendo clic en **Todas las acciones → Seguridad → Contraseña de administrador de la UEFI**. Lenovo XClarity Controller, se requiere firmware de nivel 20A.

Procedimiento

Lleve a cabo los pasos siguientes para modificar los patrones extendidos de la UEFI.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Patrones**. Se muestra la página Patrones de configuración: Patrones.

Paso 2. Haga clic en la pestaña **Patrones de categorías**.

Paso 3. Haga clic en la pestaña vertical **Patrones de UEFI extendidos**.

Paso 4. Seleccione el patrón que desee modificar y, a continuación, haga clic en el icono **Editar** ( ).

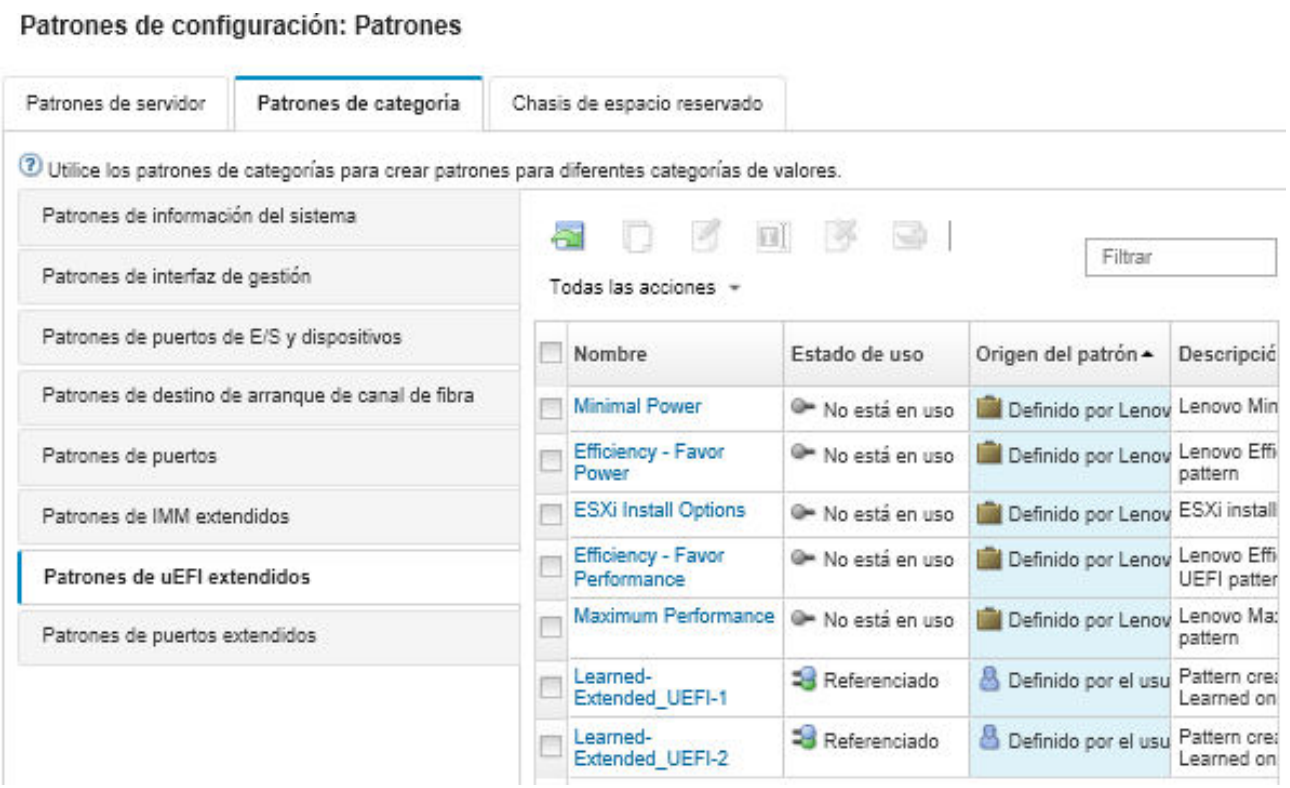
Paso 5. Modifique los campos apropiados.

Puede seleccionar los valores que desee incluir en el patrón de categorías pulsando **Incluir/Excluir** valores.

Paso 6. Haga clic en **Guardar** para guardar los cambios del patrón de categoría actual o bien haga clic en **Guardar como** para guardar los cambios en un nuevo patrón de categoría.

Resultados

El patrón de categoría modificado se muestra en la pestaña **Patrones de UEFI extendidos** de la página Patrones de configuración: Patrones de categorías:



Desde esta página, puede realizar también las acciones siguientes en el patrón de categoría seleccionado:

- Copiar un patrón existente haciendo clic en el icono **Copiar** ( ).
- Eliminar un patrón haciendo clic en el icono **Eliminar** ( ).
- Cambiar el nombre de un patrón haciendo clic en el icono **Cambiar nombre** ( ).
- Importar y exportar patrones de servidor (consulte Exportación e importación de patrones de servidor y categorías).

Definición de los valores extendidos de puerto

Los valores extendidos de puerto se aprenden y crean dinámicamente a partir de un servidor gestionado específico. Lenovo XClarity Administrator crea estos patrones al crear un patrón de servidor desde un servidor existente. No se pueden crear manualmente patrones extendidos de puerto; sin embargo, sí se pueden copiar modificar aquellos que ya se han creado.

Acerca de esta tarea

XClarity Administrator proporciona el siguiente patrón de puerto extendido predefinido:

- **Ethernet equilibrada de entramado virtual**. Patrón de puerto suministrado por Lenovo para el modo de entramado virtual vNIC, solo Ethernet.

Algunos valores del nivel de dispositivo en los adaptadores de E/S Mellanox y Broadcom deben configurarse con el mismo valor en todos los puertos. Si los valores están configurados en valores diferentes en puertos diferentes, se utilizarán los valores de un puerto y los valores de otros puertos estarán fuera de conformidad. Para resolver el problema de no conformidad, seleccione el mismo valor para esos valores de nivel de dispositivo.

Para los adaptadores de E/S Mellanox, los siguientes valores se deben establecer en el mismo valor en todos los puertos.

- Valores de energía avanzados

- Funciones virtuales de PCI anunciadas
- Limitador de alimentación de ranura
- Modo de virtualización

Para los adaptadores de E/S Broadcom, los siguientes valores se deben establecer en el mismo valor en todos los puertos.
- Tiempo de espera de mensaje de encabezado
- Límite de ancho de banda
- Límite de ancho de banda válido
- Reserva de ancho de banda
- Reserva de ancho de banda válida
- Habilitar capacidad PME
- Número máximo de vectores MSI-X PF
- Modo de varias funciones
- Número de vectores MSI-X por VF
- Número de VF por PF
- ROM opcional
- SR-IOV
- Soporte RDMA

Procedimiento

Lleve a cabo los pasos siguientes para modificar los patrones extendidos de puerto.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Patrones**. Se muestra la página Patrones de configuración: Patrones.

Paso 2. Haga clic en la pestaña **Patrones de categorías**.

Paso 3. Haga clic en la pestaña vertical **Patrones extendidos de puerto**.

Paso 4. Seleccione el patrón que desee modificar y, a continuación, haga clic en el icono **Editar** ().

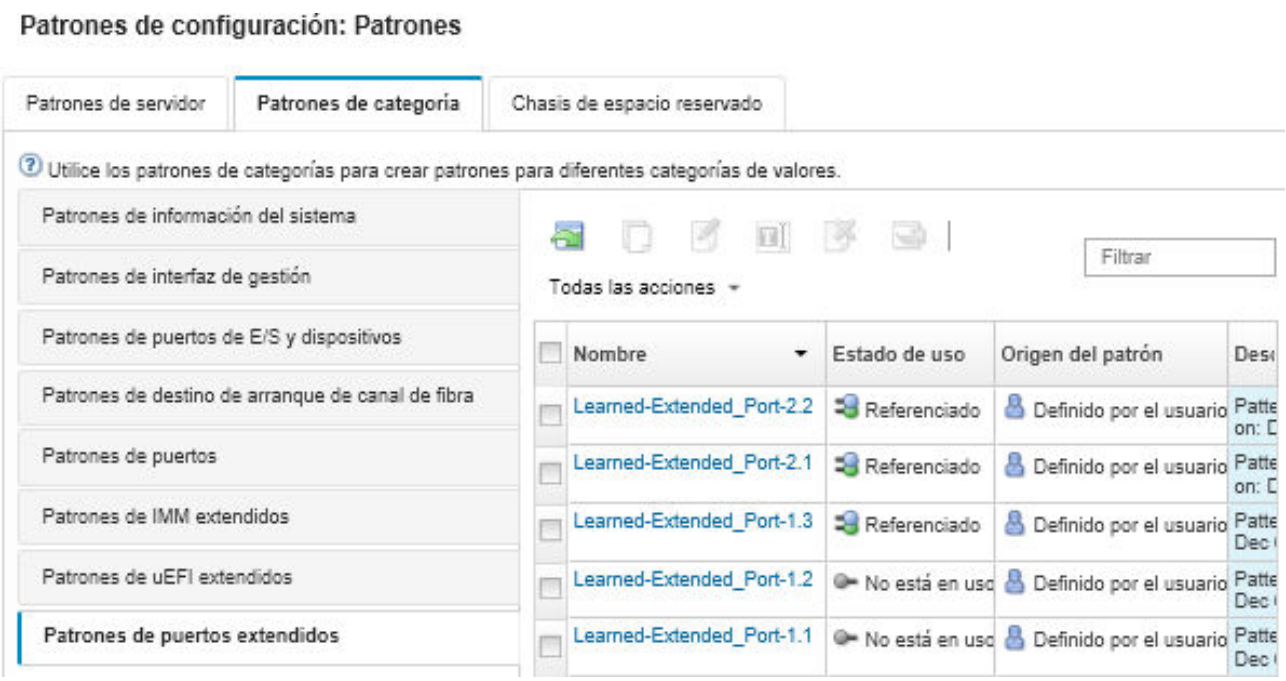
Paso 5. Modifique los campos apropiados.

Puede seleccionar los valores que desee incluir en el patrón de categorías pulsando **Incluir/Excluir** valores.

Paso 6. Haga clic en **Guardar** para guardar los cambios del patrón de categoría actual o bien haga clic en **Guardar como** para guardar los cambios en un nuevo patrón de categoría.

Resultados

El patrón de categoría modificado se muestra en la pestaña **Patrones de puerto extendido** de la página Patrones de configuración: Patrones de categorías:



Desde esta página, puede realizar también las acciones siguientes en el patrón de categoría seleccionado:

- Copiar un patrón existente haciendo clic en el icono **Copiar** ( ).
- Eliminar un patrón haciendo clic en el icono **Eliminar** ( ).
- Cambiar el nombre de un patrón haciendo clic en el icono **Cambiar nombre** ( ).
- Importar y exportar patrones de servidor (consulte Exportación e importación de patrones de servidor y categorías).

Definición de los valores extendidos de BIOS SR635/SR655

Los valores extendidos de BIOS SR635/SR655 se aprenden y crean dinámicamente a partir de un servidor gestionado específico. Lenovo XClarity Administrator crea estos patrones al crear un patrón de servidor a partir de un servidor ThinkSystem SR635 o SR655 existente. No se pueden crear manualmente patrones de BIOS SR635/SR655 extendidos; sin embargo, sí se pueden copiar modificar aquellos que ya se han creado.

Procedimiento

Lleve a cabo los pasos siguientes para modificar los patrones de BIOS SR635/SR655 extendidos.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Patrones**. Se muestra la página Patrones de configuración: Patrones.

Paso 2. Haga clic en la pestaña **Patrones de categorías**.

Paso 3. Haga clic en la pestaña vertical **Patrones de BIOS SR635/SR655 extendidos**.

Paso 4. Seleccione el patrón que desee modificar y, a continuación, haga clic en el icono **Editar** ( ).

Paso 5. Modifique los campos apropiados.

Puede seleccionar los valores que desee incluir en el patrón de categorías pulsando **Incluir/Excluir** valores.

Paso 6. Haga clic en **Guardar** para guardar los cambios del patrón de categoría actual o bien haga clic en **Guardar como** para guardar los cambios en un nuevo patrón de categoría.

Resultados

El patrón de categoría modificado se muestra en la pestaña **Patrones de BIOS SR635/SR655 extendidos** de la página Patrones de configuración: Patrones de categorías:

Desde esta página, puede realizar también las acciones siguientes en el patrón de categoría seleccionado:

- Copiar un patrón existente haciendo clic en el icono **Copiar** ( ).
- Eliminar un patrón haciendo clic en el icono **Eliminar** ( ).
- Cambiar el nombre de un patrón haciendo clic en el icono **Cambiar nombre** ( ).
- Importar y exportar patrones de servidor (consulte Exportación e importación de patrones de servidor y categorías).

Definición de los valores de BIOS extendidos de ThinkServer CPlus

Los valores extendidos de ThinkServer CPlus BIOS se aprenden y crean dinámicamente a partir de un servidor gestionado específico. Lenovo XClarity Administrator crea estos patrones al crear un patrón de servidor a partir de un servidor ThinkServer CPlus existente. No se pueden crear manualmente patrones de ThinkServer CPlus BIOS extendidos; sin embargo, sí se pueden copiar modificar aquellos que ya se han creado.

Procedimiento

Lleve a cabo los pasos siguientes para modificar los patrones de ThinkServer CPlus BIOS extendido.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Patrones**. Se muestra la página Patrones de configuración: Patrones.

Paso 2. Haga clic en la pestaña **Patrones de categorías**.

Paso 3. Haga clic en la pestaña vertical **Patrones de CPlus BIOS De ThinkServer extendidos**.

Paso 4. Seleccione el patrón que desee modificar y, a continuación, haga clic en el icono **Editar** ( ).

Paso 5. Modifique los campos apropiados.

Puede seleccionar los valores que desee incluir en el patrón de categorías pulsando **Incluir/Excluir** valores.

Paso 6. Haga clic en **Guardar** para guardar los cambios del patrón de categoría actual o bien haga clic en **Guardar como** para guardar los cambios en un nuevo patrón de categoría.

Resultados

El patrón de categoría modificado se muestra en la pestaña **Patrones de CPlus BIOS De ThinkServer extendidos** de la página Patrones de configuración: Patrones de categoría:

Desde esta página, puede realizar también las acciones siguientes en el patrón de categoría seleccionado:

- Copiar un patrón existente haciendo clic en el icono **Copiar** ( ).
- Eliminar un patrón haciendo clic en el icono **Eliminar** ( ).
- Cambiar el nombre de un patrón haciendo clic en el icono **Cambiar nombre** ( ).
- Importar y exportar patrones de servidor (consulte Exportación e importación de patrones de servidor y categorías).

Despliegue de un patrón de servidor en un servidor

Puede desplegar un patrón de servidor en uno o más servidores gestionados. También puede desplegar un patrón de servidor en una o más bahías vacías de un chasis que se esté gestionando mediante Lenovo XClarity Administrator o en un chasis de espacio reservado. Al desplegar un patrón de servidor antes de que el servidor esté instalado, se reservan direcciones IP de gestión y direcciones de Ethernet o de Fibre

Channel virtuales. Además, se introducen los valores de red en los puertos internos del conmutador relacionado.

Antes de empezar

Antes de intentar aplicar un patrón de servidor a los dispositivos gestionados, lea las consideraciones de configuración del servidor (consulte Despliegue de un patrón de servidor en un servidor).

Procedimiento

Lleve a cabo los pasos siguientes para desplegar un patrón de servidor en un servidor gestionado.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Aprovisionamiento → Patrones de configuración del servidor**. Se muestra la página Patrones de configuración de servidor.

Paso 2. Haga clic en la pestaña **Patrones de servidor**.

Paso 3. Seleccione el patrón de servidor para desplegar y, a continuación, haga clic en el icono **Desplegar** ().

Se muestra el cuadro de diálogo Desplegar patrón de servidor y el patrón de servidor seleccionado se muestra en la lista **Patrón para desplegar**.

Paso 4. Elija cuándo se activan las configuraciones:

- **Completa**. Enciende inmediatamente el servidor para activar las configuraciones del servidor, del controlador de gestión de la placa base y de Unified Extensible Firmware Interface (UEFI).
- **Parcial**. (predeterminado) Activa inmediatamente las configuraciones del controlador de gestión, pero aplaza la activación de las configuraciones del servidor y de UEFI hasta el siguiente reinicio del servidor. El servidor debe encenderse o reiniciarse manualmente antes para que el perfil esté completamente activado.

  Nota: Al desplegar patrones de servidor que incluían solo los valores de IMM (incluida la información del sistema, la interfaz de gestión y los patrones de categorías extendidos de BMC), no es necesario reiniciar el servidor.
- **Aplazada**. Genera un perfil para las configuraciones de servidor, del controlador de gestión y de la UEFI, pero no activa los valores de configuración en el servidor. Debe activar manualmente el perfil de servidor reiniciando el servidor antes de que el perfil esté completamente activado.

Nota: Los valores de red de los puertos internos del conmutador relativo se introducen en el conmutador inmediatamente después del despliegue, sea cual sea la configuración de activación.

Paso 5. Elija uno o más servidores o bahías de chasis vacías donde desea desplegar el patrón de servidor.

Nota: Para mostrar una lista de bahías del chasis, seleccione **Mostrar bahías vacías**.

Paso 6. Haga clic en **Desplegar**. Se muestra un cuadro de diálogo con el estado de despliegue de cada bahía seleccionada.

Paso 7. Haga clic en **Desplegar** de nuevo para iniciar el proceso de despliegue.

Nota: El despliegue puede tardar en completarse varios minutos. Durante el despliegue se crea un perfil de servidor que se asigna a cada servidor o bahía de chasis seleccionados.

Paso 8. Haga clic en **Cerrar**.

Después de finalizar

Puede supervisar el progreso del despliegue haciendo clic en **Supervisión → Trabajos** en la barra de menús de XClarity Administrator. También puede supervisar la creación de perfiles de servidor pulsando **Aprovisionamiento → Perfiles de servidor**. Una vez que se haya completado el despliegue, revise los perfiles de servidor generados y grabe las direcciones IP de gestión y cualquier dirección de Ethernet o de Fibre Channel virtualizada.

Si despliega un patrón de servidor en un servidor existente y selecciona:

- Activación **Completa**, se crea un perfil de servidor para cada servidor, la configuración se propaga a cada servidor y cada servidor se vuelve a arrancar para activar los cambios de la configuración.
- Activación **Parcial**, se crea un perfil de servidor para cada servidor y la configuración se propaga a cada servidor. Para activar completamente los cambios de la configuración, debe encender o reiniciar manualmente cada servidor (consulte Encendido y apagado de un servidor).
- Activación **Aplazada**, se crea un perfil de servidor para cada servidor. Debe activar manualmente el perfil de servidor en el servidor (consulte Activación de un perfil de servidor).

Si ha desplegado un patrón de servidor en una bahía vacía de un chasis gestionado o de un chasis de espacio reservado, una vez que se hayan instalado físicamente los nodos de cálculo en las bahías de chasis apropiadas y se detecten y se gestionen mediante Lenovo XClarity Administrator, debe desplegar y activar el perfil de servidor en los nodos de cálculo recién instalados (consulte Activación de un perfil de servidor).

Si uno o más servidores no se inician después de haber desplegado un nuevo patrón de servidor en ellos, el problema se puede deber a que los valores de arranque se hayan sobrescrito con los valores de arranque predeterminados que están en el patrón de servidor. Si se restauran los valores predeterminados en un sistema operativo instalado en modalidad UEFI, podrían requerirse pasos de configuración adicionales para restaurar la configuración de arranque. Para obtener ejemplos de cómo recuperar los valores de arranque en servidores que se encuentran en ejecución en Windows o Linux, consulte Recuperación de los valores de arranque tras el despliegue de patrones de servidor.

Modificación de un patrón de servidor

Puede hacer cambios de configuración posteriormente en un patrón de servidor existente. Si se despliega el patrón de servidor original en servidores (si está en uso), puede volver a desplegar el patrón de servidor cambiado a todos los servidores o a un subconjunto de ellos.

Acerca de esta tarea

Nota: Si decide no volver a desplegar el patrón de servidor cambiado en un conjunto de servidores, estos servidores seguirán asociados con el patrón de servidor original sin cambios.

Si edita el patrón de servidor, puede controlar una configuración común desde un solo lugar y mantener el conjunto de asignaciones de direcciones virtuales original.

Procedimiento

Lleve a cabo los pasos siguientes para modificar un patrón de servidor.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Aprovisionamiento → Patrones de configuración del servidor**. Se muestra la página Patrones de configuración de servidor.

Paso 2. Haga clic en la pestaña **Patrones de servidor**.

Paso 3. Seleccione el patrón de servidor que desea editar y, a continuación, haga clic en el icono **Editar** ( ). Se muestra el Asistente Editar patrones de servidor.

Paso 4. Introduzca el nombre del patrón y una descripción.

Paso 5. Elija la configuración del almacenamiento local que se va aplicar cuando este patrón se despliegue en un servidor y haga clic en **Siguiente**.

Para obtener información sobre los valores del almacenamiento local, consulte Definición de almacenamiento local.

Paso 6. **Opcional:** modifique el direccionamiento del adaptador de E/S, defina adaptadores de E/S adicionales para que coincidan con el hardware que espera configurar con este patrón y, a continuación, haga clic en **Siguiente**.

Para obtener información sobre los valores del adaptador de E/S, consulte Definición de adaptadores de E/S.

Paso 7. Defina el orden de arranque que se aplicará cuando este patrón se despliegue en un servidor y haga clic en **Siguiente**.

Para obtener información sobre los valores de los destinos de arranque de SAN, consulte Definición de opciones de arranque.

Paso 8. Seleccione los valores de firmware de la lista de patrones existentes de la categoría.

Puede crear nuevos patrones de categoría pulsando el icono **Crear** ( ).

Para obtener información sobre los valores de firmware, consulte Definición de valores de firmware.

Paso 9. Haga clic en **Guardar** para guardar los cambios de la configuración en el patrón de servidor actual o haga clic en **Guardar como** para guardar los cambios de la configuración en un nuevo patrón de servidor.

Paso 10. Seleccione esta opción para guardar los cambios en el patrón de servidor actual o en un nuevo patrón de servidor.

- Haga clic en **Guardar** para guardar los cambios en el patrón de servidor actual. Desde el cuadro de diálogo Save and Redeploy Pattern (Guardar y volver a desplegar patrón), lleve a cabo estos pasos:
  1. Elija cuándo se activan las configuraciones.
     - **Completa**. Enciende inmediatamente el servidor para activar las configuraciones del servidor, del controlador de gestión de la placa base y de Unified Extensible Firmware Interface (UEFI).
     - **Parcial**. (predeterminado) Activa inmediatamente las configuraciones del controlador de gestión, pero aplaza la activación de las configuraciones del servidor y de UEFI hasta el siguiente reinicio del servidor. El servidor debe encenderse o reiniciarse manualmente antes para que el perfil esté completamente activado.

       Nota: Al desplegar patrones de servidor que incluían solo los valores de IMM (incluida la información del sistema, la interfaz de gestión y los patrones de categorías extendidos de BMC), no es necesario reiniciar el servidor.

     Nota: Los valores de red de los puertos internos del conmutador relativo se introducen en el conmutador inmediatamente después del despliegue, sea cual sea la configuración de activación.
  2. Seleccione los servidores de destino a los que desea volver a desplegar los cambios de configuración. Puede elegir todos los servidores en los que se desplegó el patrón de servidor original o un subconjunto de esos servidores.
  3. Haga clic en **Volver a desplegar**.

- Haga clic en **Guardar como** para guardar cambios en un patrón de servidor nuevo. Para desplegar el nuevo patrón, consulte Despliegue de un patrón de servidor en un servidor.

Exportación e importación de patrones de servidor y categorías

Si tiene varias instancias de Lenovo XClarity Administrator, puede exportar patrones de servidor y categorías desde una instancia de XClarity Administrator e importarlas a otra instancia de XClarity Administrator.

Acerca de esta tarea

Solo puede exportar patrones de servidor y patrones de categorías. Las políticas, los grupos de direcciones y los perfiles no se pueden exportar. Los patrones exportados se disocian de cualquier grupo de direcciones de referencia. Para aprovechar los grupos de direcciones de un patrón importado, edite el patrón y vuelva a asociarlo con los grupos de XClarity Administrator en los que se ha realizado la importación.

Nota: Cuando exporta patrones de servidor, los patrones de categorías asociados también se exportan.

Procedimiento

- Para exportar uno o más patrones:
  1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Patrones de configuración del servidor**. Se muestra la página Patrones de configuración de servidor.
  2. Haga clic en la pestaña **Patrones de servidor** o **Patrones de categorías**.
  3. Seleccione uno o más patrones para exportar.
  4. Haga clic en el icono **Exportar** ( ).
  5. Haga clic en **Exportar** para exportar los patrones.
  6. Guarde el archivo de datos del patrón en el sistema local.

     Nota: Si un patrón exportado hace referencia a grupos de direcciones, estas referencias se quitan del patrón exportado para evitar conflictos cuando el patrón se importe a otra instancia de XClarity Administrator. Cuando el patrón se importa de nuevo, puede editar este y asignarle los grupos de direcciones deseados.
- Para importar uno o más patrones:
  1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Patrones de configuración del servidor**. Se muestra la página Patrones de configuración de servidor.
  2. Haga clic en el icono **Importar** ( ) para importar los patrones. Se muestra el cuadro de diálogo Importar patrones.
  3. Haga clic en **Seleccionar archivo** y seleccione el archivo de datos de patrón para importar. Repita los pasos para otros archivos de datos de patrón.
  4. Haga clic en **Importar** para importar los archivos seleccionados.

     Se muestra un informe de resumen con una lista de los patrones importados, los patrones que cambiaron de nombre en caso de conflictos y los patrones que se omitieron porque ya existían.

Trabajo con perfiles de servidor

Un *perfil de servidor* es una instancia de un patrón de servidor que se aplica a un servidor específico. Los perfiles de servidor se generan y se asignan automáticamente cuando se despliega un patrón de servidor en uno o más servidores. Se crea un perfil de servidor para cada servidor de destino. Cada perfil de servidor contiene la configuración específica de un solo servidor e incluye información que es única para ese servidor específico (como el nombre, las direcciones IP y las direcciones MAC que se han asignado).

Acerca de esta tarea

El perfil de servidor se activa durante el proceso de arranque del controlador de gestión de la placa base. Puede optar por:

- Rearrancar el servidor cuando se despliegue el patrón para activar inmediatamente el perfil de servidor
- Aplazar la activación hasta el siguiente rearranque.
- Aplazar la activación hasta que active manualmente el perfil de servidor.

Varios perfiles de servidor pueden heredar valores de un solo patrón de servidor. Una vez que se ha desplegado un patrón de servidor en uno o más servidores, puede desplegar rápidamente los cambios de la configuración en varios servidores editando el patrón de servidor principal y los patrones de categorías. Los perfiles de servidor dependientes se actualizan automáticamente y vuelven a desplegarse en sus servidores asociados. Si edita el patrón de servidor, puede controlar una configuración común desde un solo lugar.

Si reemplaza un servidor existente o instala un servidor preaprovisionado en una bahía vacía de un chasis, debe activar el perfil de servidor de ese nuevo servidor para aprovisionar los cambios de la configuración en el nuevo servidor.

Nota: Puede desplegar un patrón de servidor en varios servidores; sin embargo, no se pueden desplegar varios patrones en un solo servidor.

Puede cambiar el perfil de servidor que está asociado con un servidor de varias maneras, según la razón por la que se haga el cambio.

- Si desea mover o readaptar un servidor:
  1. Desactive el perfil de servidor actual en el servidor actual (consulte Desactivación de un perfil de servidor).
  2. Despliegue el nuevo patrón de servidor en el nuevo servidor (consulte Despliegue de un patrón de servidor en un servidor).
- Si hay un servidor con error y desea utilizar un servidor de repuesto en su lugar:
  1. Desactive el perfil de servidor actual en el servidor con error (consulte Desactivación de un perfil de servidor).
  2. Active el mismo perfil de servidor en el servidor de repuesto (consulte Activación de un perfil de servidor).
  3. Cuando el servidor con error esté arreglado, puede repetir estos pasos para cambiar de nuevo el perfil.
- Si hay un servidor con error y desea sustituir el hardware:
  1. Desactive el perfil de servidor actual en el servidor con error (consulte Desactivación de un perfil de servidor).
  2. Sustituya el servidor con error.
  3. Active el mismo perfil de servidor en el nuevo servidor (consulte Activación de un perfil de servidor).

Importante:

- Al utilizar la virtualización de direcciones, un servidor conserva su dirección virtual MAC o WWN asignada hasta que se apague. Al desactivar un perfil que tenga habilitada la virtualización de la dirección, la casilla de verificación **Apagar el servidor** se selecciona de forma predeterminada. Asegúrese de apagar el servidor original antes de activar el perfil no activo en un servidor distinto para evitar conflictos de dirección.
- Si elimina un perfil que no es el creado más recientemente, las direcciones MAC virtuales y WWN *no* se liberan del grupo de direcciones. Para obtener más información, consulte el apartado Eliminación de un perfil de servidor.

- Es posible que los valores en un servidor dejen de ajustarse a la conformidad con el perfil de servidor si se cambia la configuración sin utilizar patrones de configuración o si se produjo un problema durante el despliegue, como un problema con el firmware o una configuración no válida. Puede determinar el estado de cumplimiento de cada servidor desde la página Patrones de configuración: Perfiles de servidor.

Activación de un perfil de servidor

Puede activar un perfil de servidor en un servidor reemplazado, reasignado o nuevamente instalado y gestionado.

Acerca de esta tarea

Si reemplaza un servidor existente o instala un servidor preaprovisionado en una bahía vacía de un chasis, debe activar el perfil de servidor de ese nuevo servidor para aprovisionar los cambios de la configuración en el nuevo servidor.

Importante:

- Al utilizar la virtualización de direcciones, un servidor conserva su dirección virtual MAC o WWN asignada hasta que se apague. Al desactivar un perfil que tenga habilitada la virtualización de la dirección, la casilla de verificación **Apagar el servidor** se selecciona de forma predeterminada. Asegúrese de apagar el servidor original antes de activar el perfil no activo en un servidor distinto para evitar conflictos de dirección.
- Si elimina un perfil que no es el creado más recientemente, las direcciones MAC virtuales y WWN *no* se liberan del grupo de direcciones. Para obtener más información, consulte el apartado Eliminación de un perfil de servidor.
- Es posible que los valores en un servidor dejen de ajustarse a la conformidad con el perfil de servidor si se cambia la configuración sin utilizar patrones de configuración o si se produjo un problema durante el despliegue, como un problema con el firmware o una configuración no válida. Puede determinar el estado de cumplimiento de cada servidor desde la página Patrones de configuración: Perfiles de servidor.

Procedimiento

Para activar un perfil de servidor, lleve a cabo los pasos siguientes.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Aprovisionamiento → Perfiles de servidor**. Se muestra la página Patrones de configuración: Perfiles de servidor.

Paso 2. Seleccione el perfil de servidor que va a activar.

Consejo: el estado de los perfiles de servidor se muestra en la columna **Estado del perfil**. Puede activar los perfiles de servidor que se encuentran en el estado de activación “Inactivo” o “Pendiente”.

Paso 3. Haga clic en el icono **Activar perfil de servidor** ().

Paso 4. Haga clic en **Activar**.

Si el perfil se encuentra en el estado pendiente, activo o de error activo, puede elegir cuándo activar el despliegue:

- **Completa**. Enciende inmediatamente el servidor para activar las configuraciones del servidor, del controlador de gestión de la placa base y de Unified Extensible Firmware Interface (UEFI).
- **Parcial**. (predeterminado) Activa inmediatamente las configuraciones del controlador de gestión, pero aplaza la activación de las configuraciones del servidor y de UEFI hasta el siguiente reinicio del servidor. El servidor debe encenderse o reiniciarse manualmente antes para que el perfil esté completamente activado.

Nota: Al desplegar patrones de servidor que incluían solo los valores de IMM (incluida la información del sistema, la interfaz de gestión y los patrones de categorías extendidos de BMC), no es necesario reiniciar el servidor.

Al activar el perfil de servidor, el estado del perfil cambia a “Activo.” Después de verificar el cumplimiento, el estado cambia a “Conforme” o “No conforme.”

Resultados

El estado del perfil de servidor de la página Patrones de configuración: Perfiles de servidor cambia a Activo.

Desactivación de un perfil de servidor

Puede cancelar la asignación de un perfil de servidor de un servidor o una bahía de chasis desactivando el perfil.

Procedimiento

Para desactivar un perfil de servidor, lleve a cabo los pasos siguientes.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Aprovisionamiento → Perfiles de servidor**. Se muestra la página Patrones de configuración: Perfiles de servidor.

Paso 2. Seleccione el perfil de servidor que va a desactivar.

Consejo: el estado actual del perfil de servidor se muestra en la columna **Estado del perfil**.

Paso 3. Haga clic en el icono **Desactivar perfil de servidor** ( ).

Paso 4. Elija una de las siguientes opciones de desactivación:

- **Valores de identidad de Reset IMM**. Restablece los valores de identidad configurados en el perfil (incluido el nombre de host del controlador de gestión de la placa base, el nombre del dispositivo o las direcciones IP estáticas asignadas de la interfaz de gestión). Solo se restablecerán los valores configurados a través del patrón de servidor asociado.

  Nota: Para servidores con direcciones IP estáticamente asignadas, esta opción permite el modo DHCP. Si no hay un servidor DHCP habilitado en la red, el servidor se debe volver a configurar manualmente con una dirección IP estática válida. Los servidores de bastidor y de torre convergidos, NeXtScale y System x deben volver a gestionarse mediante XClarity Administrator.

- **Apagar el servidor**. Apaga el servidor. Cuando el servidor se vuelve a encender, las asignaciones de direcciones virtuales vuelven a los valores predeterminados grabados.
- **Forzar desactivación**. Desactiva el perfil de servidor incluso si el servidor se ha eliminado o no se puede alcanzar.
- **Restablecer valores de puerto interno de conmutador**. Restablece los valores de puerto interno del conmutador configurado por perfil a los valores predeterminados, incluidos deshabilitar el modo UFP y eliminar los puertos virtuales miembros asociados desde las definiciones de VLAN. Solo se restablecerán los valores configurados a través del patrón de servidor asociado.

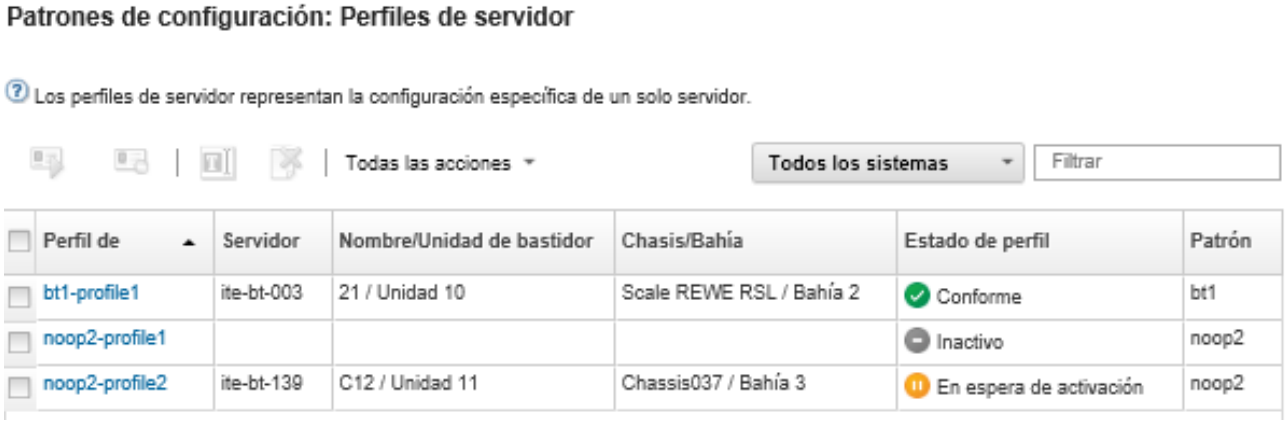
  Esta opción está deshabilitada de forma predeterminada.

  Elija esta opción para dejar los puertos del conmutador en un estado en el que el perfil del servidor se pueda desplegar a otro servidor sin valores que entren en conflicto con la configuración del puerto del conmutador anterior.

Paso 5. Haga clic en **Desactivar**.

Resultados

El estado del perfil de servidor de la página Patrones de configuración: Perfiles de servidor cambia a Inactivo.



Nota: Si XClarity Administrator no se puede comunicar con el controlador de gestión (por ejemplo si el controlador de gestión está en un estado de error o se reinicia), la desactivación de perfil del servidor falla y el perfil del servidor no se desactiva. Si esto ocurre, vuelva a intentar la desactivación y seleccione la opción de la desactivación forzada para desactivar el perfil. El servidor asignado previamente aún está configurado con las asignaciones de identidad y de dirección asignadas al perfil. El servidor se debe apagar manualmente y extraer de la infraestructura para evitar conflictos de dirección.

Eliminación de un perfil de servidor

Solo puede eliminar perfiles del servidor que se desactivaron.

Antes de empezar

Asegúrese de eliminar y desactivar los perfiles de servidor (consulte Desactivación de un perfil de servidor).

Procedimiento

Para eliminar un perfil de servidor, complete los pasos siguientes

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Aprovisionamiento → Perfiles de servidor**. Se muestra la página Patrones de configuración: Perfiles de servidor.

Paso 2. Seleccione el perfil de servidor que se encuentra en estado desactivado.

Consejo: el estado actual del perfil de servidor se muestra en la columna **Estado del perfil**.

Paso 3. Haga clic en el icono **Eliminar** ( ).

Nota: Al eliminar el perfil creado más recientemente, se liberará cualquier dirección virtual MAC o WWN del grupo de direcciones. Si elimina un perfil que no es el creado más recientemente, las direcciones MAC virtuales y WWN *no* se liberan del grupo de direcciones.

Trabajo con chasis de espacio reservado

Puede preaprovisionar servidores que se instalarán posteriormente en un chasis de Flex System definiendo un *chasis de espacio reservado* para que actúe como destino del patrón de servidor hasta que llegue el hardware físico.

Acerca de esta tarea

Al desplegar un patrón de servidor en un chasis de espacio reservado, Lenovo XClarity Administrator crea un perfil de servidor para las 14 bahías de servidor del chasis de Flex System y reserva las direcciones IP de gestión y las direcciones de Ethernet y de Fibre Channel virtuales para los servidores.

El chasis de espacio reservado empaqueta todos los perfiles de servidor, de modo que, cuando llegue el hardware, puede desplegar el chasis de espacio reservado para activar los perfiles de servidor en los servidores físicos en vez de desplegar los 14 perfiles de servidor de forma individual. Debe rearrancar cada uno de los servidores para activar completamente el perfil de servidor.

Creación de un chasis de espacio reservado

Puede crear un chasis de espacio reservado que se puede preaprovisionar antes de que se instale el hardware. El aprovisionamiento de los nodos de cálculo del chasis reserva direcciones IP de gestión y direcciones de Ethernet o de Fibre Channel virtuales.

Procedimiento

Lleve a cabo los pasos siguientes para crear un chasis de espacio reservado.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Aprovisionamiento → Patrones**. Se muestra la página Patrones de configuración: Patrones.

Paso 2. Haga clic en la pestaña **Chasis de espacio reservado**.

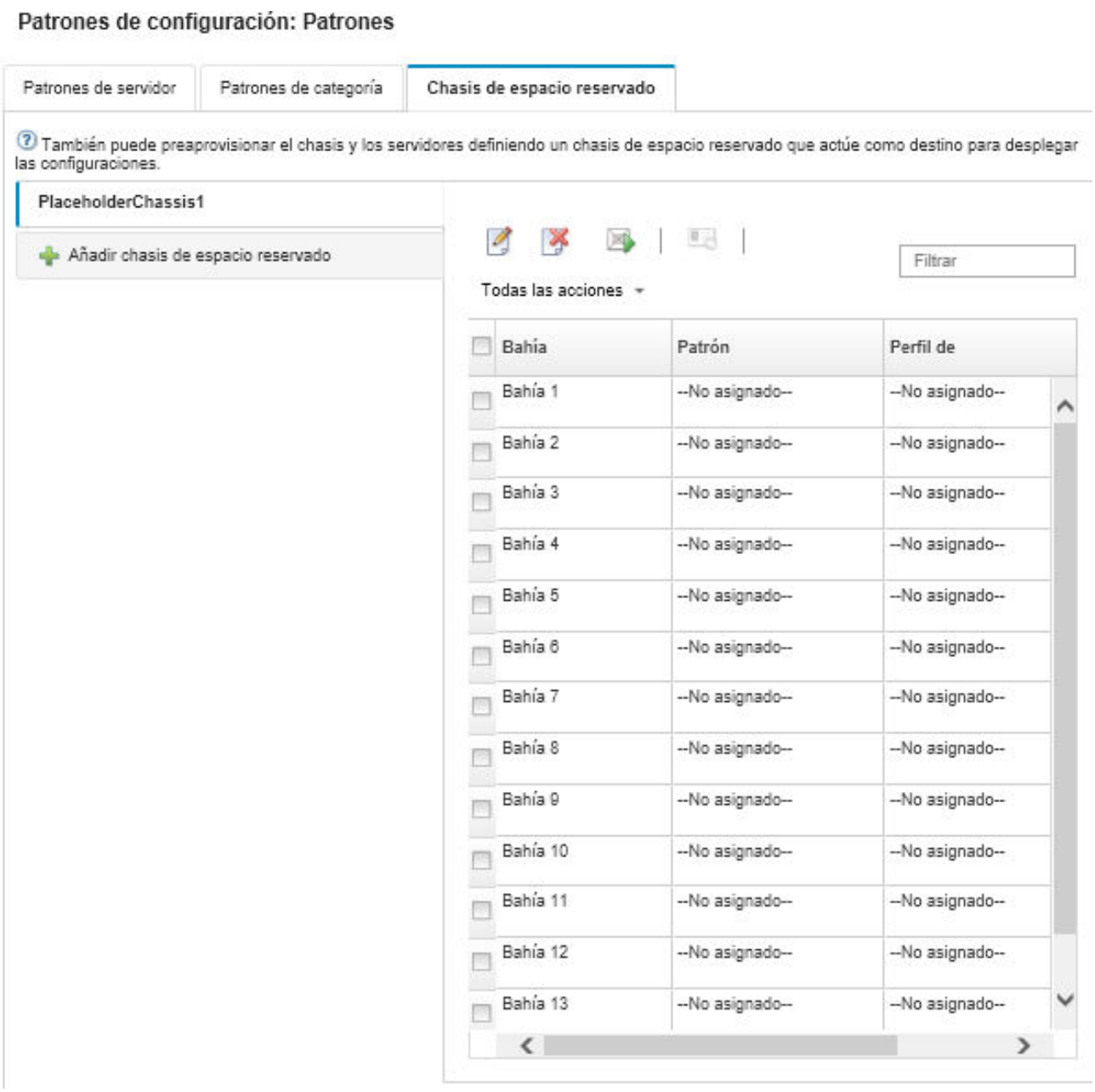
Paso 3. Haga clic en la pestaña vertical **Añadir chasis de espacio reservado**.

Paso 4. Escriba un nombre y una descripción para el chasis de espacio reservado.

Paso 5. Haga clic en **Añadir**.

Después de finalizar

Se añade una pestaña vertical para el nuevo chasis de espacio reservado en la página Patrones de configuración: Chasis de espacio reservado.



Desde esta página puede realizar las acciones siguientes en el chasis de espacio reservado seleccionado:

- Desplegar el chasis de espacio reservado haciendo clic en el icono **Desplegar** ( ).
- Modificar el nombre y la descripción del chasis de espacio reservado haciendo clic en el icono **Editar** ( ).
- Desplegar un patrón de servidor en el chasis de espacio reservado (consulte Despliegue de un patrón de servidor en un chasis de espacio reservado).
- Desactivar el perfil de servidor de un chasis de espacio reservado (consulte Desactivación de un perfil de servidor).
- Para eliminar el chasis de espacio reservado, haga clic en el icono **Eliminar** ( ).

Despliegue de un patrón de servidor en un chasis de espacio reservado

Puede desplegar un patrón de servidor en cada bahía de un chasis de espacio reservado. Al desplegar un patrón de servidor antes de que los servidores se instalen en el chasis de Flex System, se crea un perfil de

servidor para cada bahía de servidor del chasis y se reservan direcciones IP de gestión y direcciones Ethernet o de Fibre Channel virtuales.

Procedimiento

Lleve a cabo los pasos siguientes para desplegar un patrón de servidor en un chasis de espacio reservado.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Aprovisionamiento → Patrones de configuración del servidor**. Se muestra la página Patrones de configuración de servidor.

Paso 2. Haga clic en la pestaña **Patrones de servidor**.

Paso 3. Seleccione el patrón de servidor que desee desplegar en el chasis de espacio reservado.

Paso 4. Haga clic en el icono **Desplegar** (). Se muestra el cuadro de diálogo Desplegar patrón de servidor con una lista de chasis y chasis de espacio reservado disponibles.

Paso 5. Seleccione **Aplazada** en la lista **Activación**.

Paso 6. Haga clic en **Mostrar bahías vacías**.

Paso 7. Elija una o más bahías de chasis de espacio reservado donde desea desplegar el patrón de servidor.

Paso 8. Haga clic en **Desplegar**. Se muestra un cuadro de diálogo con el estado de despliegue de cada bahía seleccionada.

Paso 9. Haga clic en **Desplegar** de nuevo para iniciar el proceso de despliegue.

Se crea un perfil de servidor que se asigna a cada bahía seleccionada en el chasis de espacio reservado.

Nota: El despliegue puede tardar en completarse varios minutos.

Paso 10. Haga clic en **Cerrar**.

Después de finalizar

Puede supervisar el progreso del despliegue haciendo clic en **Supervisión → Trabajos** en la barra de menús de XClarity Administrator. También puede supervisar la creación de perfiles de servidor pulsando **Aprovisionamiento → Perfiles de servidor**. Una vez que se haya completado el despliegue, revise los perfiles de servidor generados y grabe las direcciones IP de gestión y cualquier dirección de Ethernet o de Fibre Channel virtualizada.

Una vez que el chasis de Flex System se haya instalado físicamente en el bastidor y que lo detecte y gestione XClarity Administrator, puede desplegar el chasis de espacio reservado para aprovisionar todos los servidores del chasis (consulte Despliegue de un patrón de servidor en un chasis de espacio reservado).

Despliegue de un chasis de espacio reservado

Una vez que preconfigure un chasis de espacio reservado desplegando un patrón de servidor en el mismo y descubra y gestione después el propio chasis, puede desplegar el chasis de espacio reservado para configurar los propios nodos de cálculo.

Procedimiento

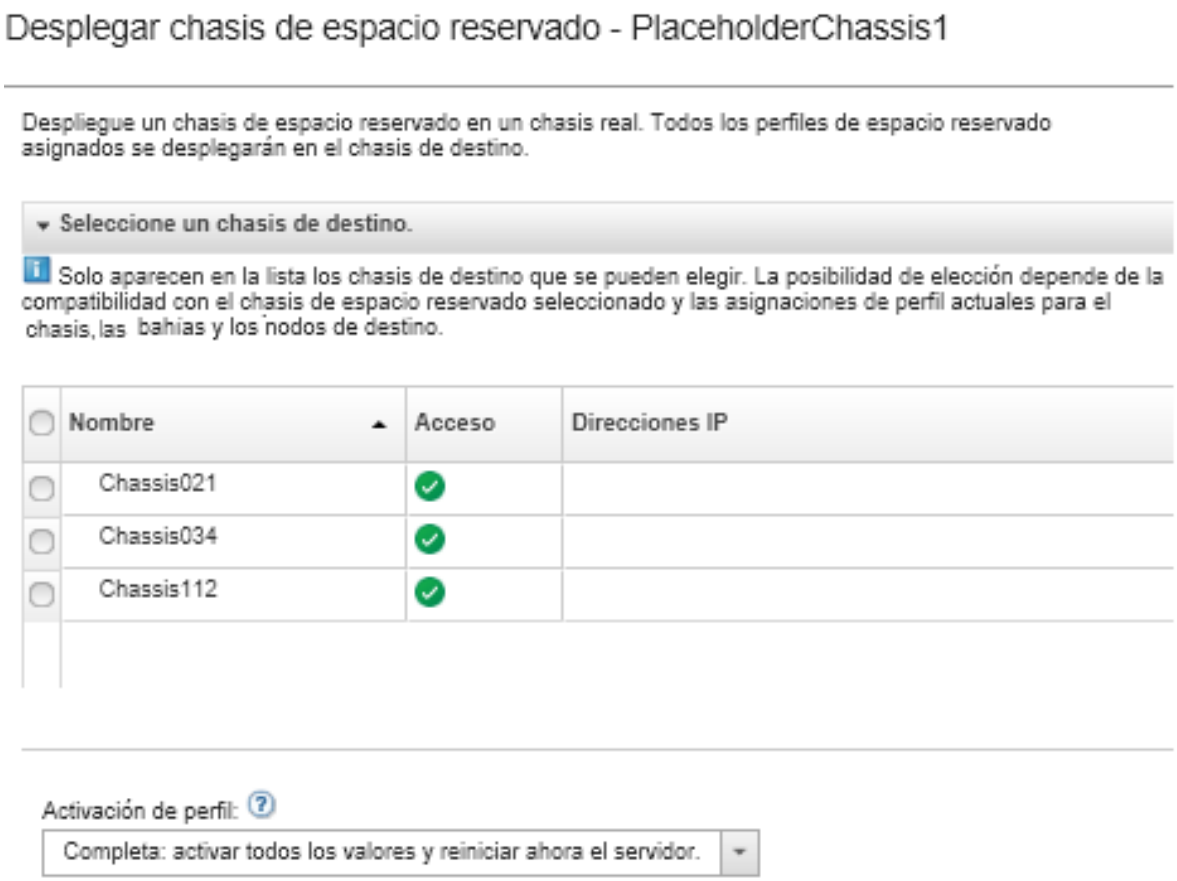
Lleve a cabo los pasos siguientes para desplegar un chasis de espacio reservado.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Aprovisionamiento → Patrones de configuración del servidor**. Se muestra la página Patrones de configuración de servidor.

Paso 2. Haga clic en la pestaña **Chasis de espacio reservado**.

Paso 3. Seleccione la pestaña vertical del chasis de espacio reservado que desee desplegar.

Paso 4. Haga clic en el icono **Desplegar chasis de espacio reservado** ( ) para mostrar el cuadro de diálogo Desplegar chasis de espacio reservado.



Paso 5. Elija cuándo se activan las configuraciones:

Nota: Los valores de red de los puertos internos del conmutador relativo se introducen en el conmutador inmediatamente después del despliegue, sea cual sea la configuración de activación.

- **Completa**. Enciende inmediatamente el servidor para activar las configuraciones del servidor, del controlador de gestión de la placa base y de Unified Extensible Firmware Interface (UEFI).
- **Parcial**. (predeterminado) Activa inmediatamente las configuraciones del controlador de gestión, pero aplaza la activación de las configuraciones del servidor y de UEFI hasta el siguiente reinicio del servidor. El servidor debe encenderse o reiniciarse manualmente antes para que el perfil esté completamente activado.

  Nota: Al desplegar patrones de servidor que incluían solo los valores de IMM (incluida la información del sistema, la interfaz de gestión y los patrones de categorías extendidos de BMC), no es necesario reiniciar el servidor.

Paso 6. Haga clic en **Activar**.

Restablecer adaptadores de almacenamiento a los valores predeterminados

Puede restablecer los adaptadores de almacenamiento local a sus valores de fábrica predeterminados en uno o varios servidores.

Acerca de esta tarea

Atención: Esta acción borra todos los datos de los adaptadores del almacenamiento local.

Si el servidor está apagado y admite el enlace RAID, el servidor se arranca a la configuración del sistema para restablecer los adaptadores de HDD y SSD locales.

Procedimiento

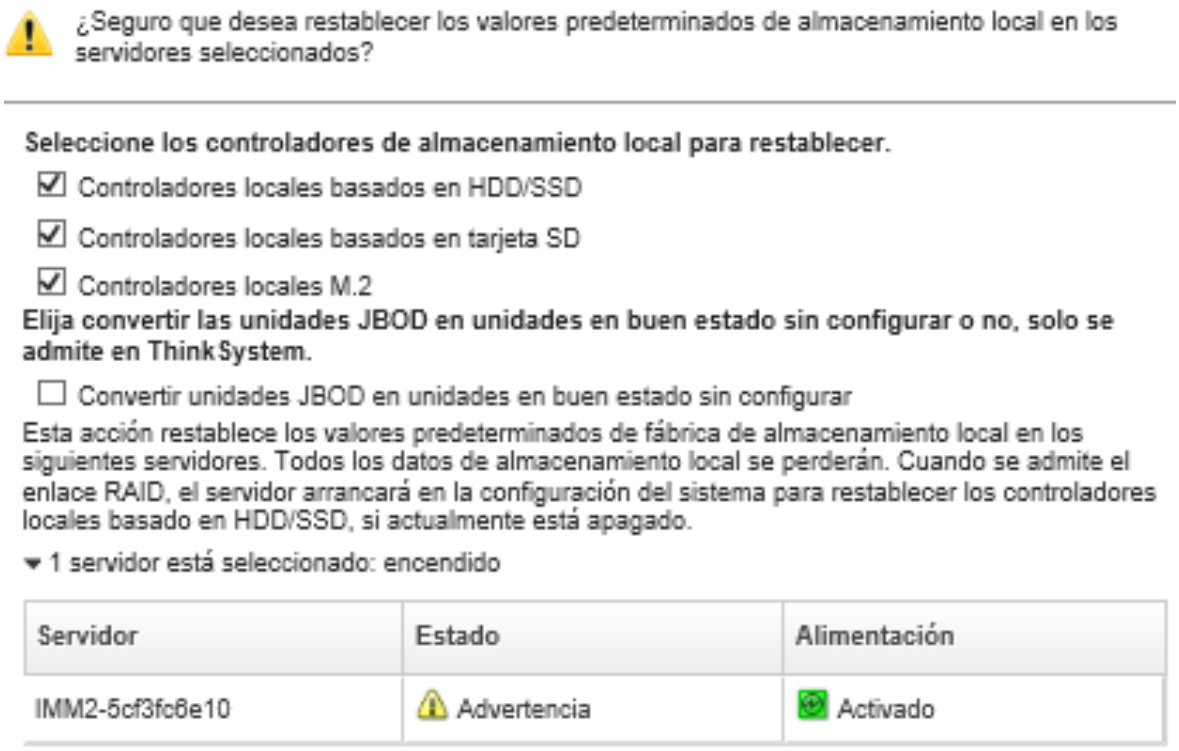
Complete estos pasos para eliminar la configuración de RAID para uno o más servidores.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Hardware → Servidores**. Se muestra la página Servidores con una vista de tabla de todos los servidores gestionados (servidores de bastidor y nodos de cálculo).

Puede ordenar las columnas de la tabla para que sea más fácil encontrar el servidor que desea gestionar. Además, puede seleccionar un tipo de servidor en la lista desplegable **Todos los sistemas** e introducir texto (como un nombre o una dirección IP) en el campo **Filtro** para filtrar mejor los servidores que se muestran.

Paso 2. Seleccione uno o más servidores

Paso 3. Seleccione **Todas las acciones → Servicio → Restablecer valores predeterminados de almacenamiento local**. Aparece un cuadro de diálogo que solicita información adicional.



Paso 4. Seleccione los adaptadores de almacenamiento local para restablecerlo.

Paso 5. : (solo servidores ThinkSystem) selecciónelo para convertir unidades JBOD al estado en buen estado sin configurar.

Paso 6. Haga clic en **Restablecer almacenamiento**.

Configuración de memoria

Puede cifrar y descifrar memoria persistente para DIMM de memoria persistente de Intel® Optane™ DC.

Procedimiento

Lleve a cabo el siguiente procedimiento para cifrar y descifrar memoria persistente.

Paso 1. En el menú de XClarity Administrator, haga clic en **Hardware → Servidores**. Se muestra la página Servidores con una vista de tabla de todos los servidores gestionados (servidores de bastidor y nodos de cálculo).

Paso 2. Seleccione uno o más servidores que desee configurar.

Paso 3. Haga clic en **Todas las acciones → Seguridad → Operación de PMEM de Intel Optane** para mostrar el cuadro de diálogo Operación de PMEM de Intel Optane.

Paso 4. Seleccione la operación de seguridad que desea realizar.

- **Habilitar seguridad**. Los datos que se escriben en el área de memoria persistente se cifran usando la frase de contraseña especificada.

  Importante: Registre la frase de paso de cifrado. La frase de contraseña es necesaria para autorizar la deshabilitación de la seguridad o borrar la frase de contraseña de cifrado.

- **Deshabilitar seguridad** Los datos que se escriben en el área de memoria persistente se cifran.

  Los datos que ya se encuentran almacenados en el área de memoria persistente permanecen cifrados y aún están accesibles.

Nota: Esta acción solo está disponible cuando se habilita la seguridad y se establece la frase de contraseña. Debe autorizar esta operación usando la frase de contraseña actual. Puede deshabilitar la seguridad para varias DIMM en el dispositivo solo si todos los DIMM comparten la misma frase de contraseña.

- **Borrado seguro**. Borra la frase de contraseña de cifrado que se utiliza para cifrar los datos que se encuentran almacenados en el área de memoria persistente para asegurarse de que los datos estén irrecuperables.

  Nota: Esta acción solo está disponible cuando se habilita la seguridad y se establece la frase de contraseña. Debe autorizar esta operación usando la frase de contraseña actual.

- **Borrado seguro sin frase de paso**. Borre de forma segura todos los datos almacenados en la memoria persistente de los DIMM especificados en el dispositivo. Después de realizar el borrado seguro, todos los datos son irrecuperables.

  Nota: Esta acción solo está disponible cuando se deshabilita la seguridad y no se requiere la frase de paso.

Paso 5. Si es necesario, especifique y confirme la frase de paso.

Paso 6. Haga clic en **Aceptar**.

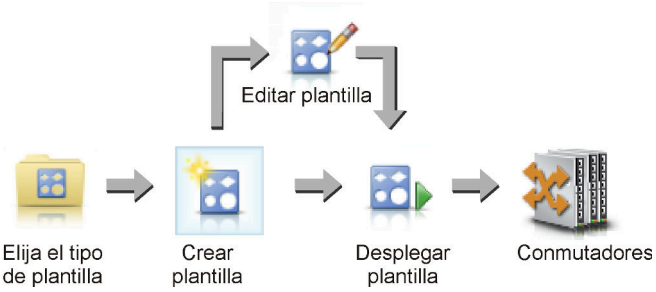
Capítulo 12. Configuración de conmutadores mediante el uso de plantillas de configuración

Puede utilizar plantillas para aprovisionar rápidamente varios conmutadores de bastidor CNOS desde un solo conjunto de valores de configuración definidos.

Acerca de esta tarea

Puede utilizar la plantilla de configuración del conmutador de XClarity Administrator para configurar los valores globales, canales de puerto, LAN virtuales, grupos de agregación de enlaces virtuales y topologías spine-leaf en conmutadores gestionados. Actualmente, solo los conmutadores de bastidor ejecutando CNOS son compatibles.

En la siguiente figura se ilustra el flujo de trabajo para configurar conmutadores de bastidor gestionados.



1. **Elija un tipo de plantilla.**

   Un *plantilla de configuración del conmutador* agrupa valores de conmutador relacionados. También puede crear los siguientes tipos de plantillas de configuración del conmutador.
   - **Global**. Configura los valores globales, como propiedad del sistema, etiquetas VLAN nativas e interfaces L2.
   - **Canal de puerto**. Configura los valores de puerto de canal básicos y avanzados y quita puertos de y elimina un canal de puerto.
   - **Spine-leaf**. Despliega una configuración spine-leaf en una topología existente.
   - **LAN virtual (VLAN)**. Configura los valores y las propiedades de VLAN y eliminar una VLAN.
   - **Grupo de agregación de enlace virtual (VLAG)**. Configura valores VLAG básicos, avanzados y de par y crea y elimina una instancia VLAG.
2. **Crear una plantilla.**

   Puede crear varias plantillas de configuración de conmutador para representar las distintas configuraciones que se utilizan en su centro de datos. Utiliza plantillas de configuración del conmutador para controlar una configuración de conmutador común desde un solo lugar.

   Para obtener más información acerca de crear plantillas de configuración de conmutador, consulte Creación de una plantilla de configuración del conmutador.
3. **Desplegar la plantilla en uno o más conmutadores.**

   Puede desplegar un patrón de servidor en uno o más conmutadores de bastidor individuales ejecutando CNOS.

   Para obtener más información sobre el despliegue de una configuración de conmutador, consulte Despliegue de plantillas de configuración del conmutador en un conmutador de destino.
4. **Editar una plantilla.**

Editar una plantilla de configuración de conmutador no despliega automáticamente la configuración actualizada a todos los conmutadores en los que se desplegó la plantilla inicial. Debe volver a desplegar manualmente las plantillas cambiadas. La página historial realiza un seguimiento de los valores para cada despliegue.

Configuración de las preferencias de configuración del servidor predeterminado

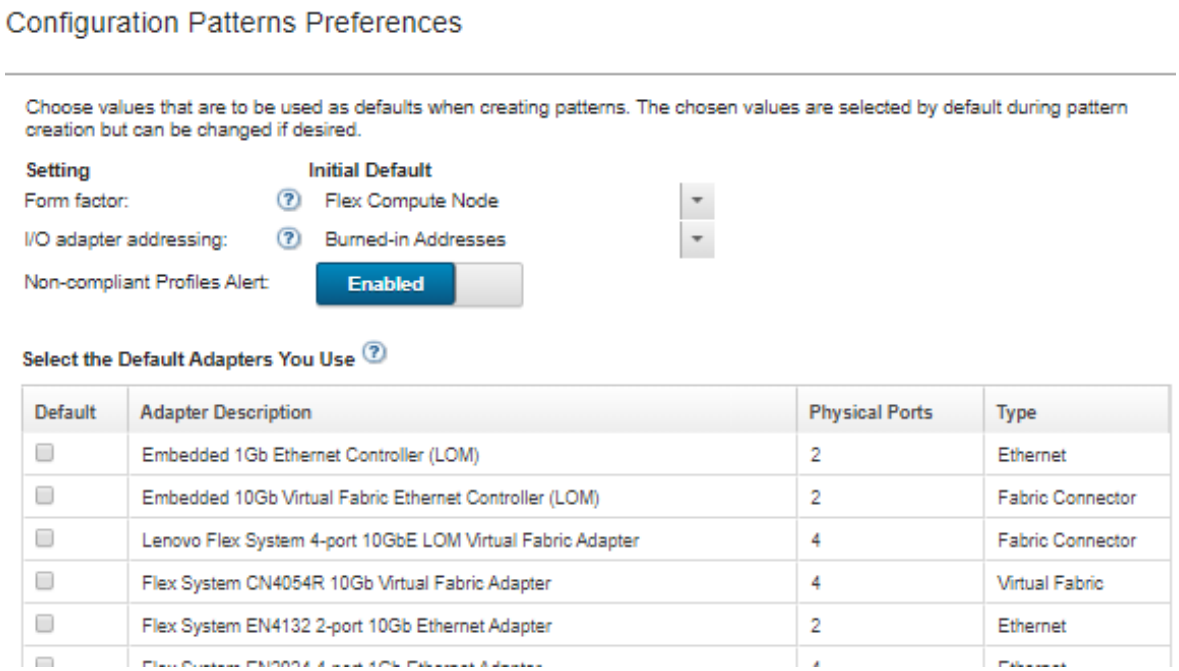
Puede definir los valores que se van a seleccionar de manera predeterminada cuando se crean patrones de configuración de servidor. Los valores se pueden cambiar durante la creación de los patrones de servidor.

Procedimiento

Lleve a cabo los pasos siguientes para establecer los valores predeterminados de la configuración del servidor.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Aprovisionamiento** y luego haga clic en el icono de ayuda (?) situado después de **Patrones de configuración** para mostrar la página Patrones de configuración: Introducción.

Paso 2. Haga clic en **Definir preferencias de patrones de configuración** para mostrar el cuadro de diálogo Preferencia de patrón de configuración.



Paso 3. Seleccione el factor de forma de servidor predeterminado.

Paso 4. Seleccione el modo predeterminado de direccionamiento de los adaptadores de E/S.

- **Grabado**. Utilice las direcciones World Wide Name (WWN) y Media Access Control (MAC) que se proporcionan de fábrica con el adaptador.
- **Virtual**. Utilice el direccionamiento de adaptador de E/S virtual para simplificar la gestión de las conexiones LAN y SAN. La virtualización de direcciones de E/S reasigna las direcciones de hardware grabadas con direcciones de fibra WWN y Ethernet MAC virtualizadas, lo que puede acelerar el despliegue preconfigurando la calidad de miembro de la zona SAN, así como facilitar la conmutación por error eliminando la necesidad de volver a configurar las zonas SAN y las asignaciones de enmascaramiento LUN al sustituir el hardware.

Cuando se habilita el direccionamiento virtual, tanto las direcciones de Ethernet como las de Fibre Channel se asignan de manera predeterminada independientemente de los adaptadores definidos. Puede elegir el grupo desde el cual se asignan las direcciones de Ethernet y las de Fibre Channel.

También puede editar los valores de las direcciones virtuales haciendo clic en el icono **Editar** () que se encuentra situado junto a los modos de dirección.

Restricción: UI direccionamiento virtual solo se admite para los servidores del chasis de Flex System. No se admiten los servidores de bastidor y de torre.

Paso 5. Elija si habilitar o deshabilitar que se genere una alerta cuando los valores de configuración de un servidor no coincidan con el perfil de configuración del servidor asignado.

Las alertas se generan solo para el incumplimiento de un perfil activo (en el estado ASSIGNED o ERROR_ACTIVATING).

Cuando la configuración del servidor pasa a ser en cumplimiento, o si el perfil de servidor no está asignado, se elimina la alerta de perfil no en cumplimiento.

Paso 6. Seleccione uno o varios adaptadores de E/S predeterminados que desee utilizar como adaptadores preferidos en las listas de selección.

Paso 7. Haga clic en **Guardar**.

Creación de una plantilla de configuración del conmutador

Cuando cree una plantilla de configuración de conmutador, defina los valores para un tipo de configuración específica.

Antes de empezar

Antes de crear una plantilla de configuración de conmutador, tenga en cuenta las siguientes sugerencias:

- Identifique los grupos de conmutadores que tengan las mismas opciones de hardware y que desee configurar del mismo modo. Puede utilizar una plantilla de configuración de conmutador para aplicar los mismos valores de configuración de varios conmutadores y, por tanto, controlar una configuración común desde un solo lugar.
- Identifique los aspectos de la configuración que desee personalizar (por ejemplo, global, puerto de canal o valores de VLAN).

Procedimiento

Lleve a cabo los pasos siguientes para crear una plantilla de configuración del conmutador.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Plantillas de configuración de conmutador**. Se muestra la página Plantillas de configuración de conmutador.

Paso 2. Seleccione el tipo de plantilla que desea crear en la barra de navegación a la izquierda.

Paso 3. Pulse el icono de **Crear** ( ) para mostrar el cuadro de diálogo Crear nueva plantilla.

Los campos que aparecen en este cuadro de diálogo varían según el tipo de plantilla.

Paso 4. Haga clic en **Guardar** para guardar la plantilla o haga clic en **Guardar y desplegar** para guardar y desplegar inmediatamente la plantilla en uno o más servidores

Para obtener información acerca del despliegue de una plantilla, consulte Despliegue de plantillas de configuración del conmutador en un conmutador de destino.

Después de finalizar

Si hizo clic en **Guardar y desplegar**, se muestra la página Desplegar plantilla de conmutador. Desde esta página, puede desplegar la plantilla de configuración de conmutador a conmutadores específicos.

Si hizo clic en **Guardar**, la plantilla de configuración del conmutador se guarda en la página Plantillas de configuración del conmutador. Desde esta página puede realizar las acciones siguientes en los patrones de servidor seleccionados:

- Ver los detalles acerca de la plantilla haciendo clic en el nombre de la plantilla en la columna Name (Nombre).
- Vea una lista agregada de todas las plantillas, haga clic en **Otros → Todas las plantillas**.
- Desplegar la plantilla (consulte Despliegue de plantillas de configuración del conmutador en un conmutador de destino).
- Para copiar y modificar una plantilla, haga clic en el ícono **Copia** ( ).
- Para editar la plantilla, haga clic en el ícono **Editar** ( ).

Nota: Los cambios realizados en la plantilla *no se vuelven* a desplegar automáticamente en los conmutadores en los que se desplegó la plantilla original.

- Cambiar el nombre del patrón haciendo clic en el icono **Cambiar nombre** ().
- Eliminar el patrón haciendo clic en el icono **Eliminar** ().

Definición de valores de pertenencia de puerto VLAN

Puede agregar puertos físicos y canales de puerto a una o varias VLAN (para troncal) utilizando la plantilla de configuración de membresía de puerto de VLAN.

Procedimiento

Lleve a cabo los siguientes pasos para crear una plantilla de configuración de membresía de puerto.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Plantillas de configuración de conmutador**. Se muestra la página Plantillas de configuración de conmutador.

Paso 2. Haga clic en **VLAN → Configuración de pertenencia de puerto** en el panel de navegación a la izquierda y haga clic en el ícono **Crear** ().

Paso 3. En el cuadro de diálogo Crear nueva plantilla, especifique la siguiente información.

Importante: Debe especificar una o más interfaces L2 físicas o Id. de canal de puerto.

- Introduzca el nombre y la descripción de la plantilla.
- Especifique una o más interfaces L2 físicas válidas. Puede especificar una lista de interfaces separadas por una coma, un rango de Id., separados por un guion o una combinación de ambos, por ejemplo:
  - Ethernet1/10
  - Ethernet1/3,5,7,9
  - Ethernet1/5-10,21-32
  - Ethernet2/2-5,7,9,11-13
- Especifique uno o varios Id. de canal de puerto válidos (interfaces del agregador de puertos). Puede especificar una lista de números separados por una coma, un rango de números, separados por un guion o una combinación de ambos. Los valores e intervalos pueden ser números de 1 a 4096, por ejemplo:
  - 10
  - 3,5,7,9
  - 5-10,21-32
  - 2-5,7,9,11-13
- Elija si el puerto acepta tráfico etiquetado o no etiquetado. Puede presentar uno de los valores siguientes.
  - **acceso**. El puerto transporta tráfico para una sola VLAN.
  - **entroncamiento**. (predeterminado) El puerto transporta tráfico de todas las VLAN accesibles por el conmutador.
- Especifique uno o más Id. de VLAN para agregar a la lista de suscripciones VLAN del puerto. Puede especificar una lista de números separados por una coma, un rango de números, separados por un guion o una combinación de ambos. Los valores e intervalos pueden ser números de 1 a 4096, por ejemplo:
  - 10
  - 3,5,7,9
  - 5-10,21-32
  - 2-5,7,9,11-13

Notas:

- Si el modo de puerto se establece en “acceso”, solo se usa el primer Id. de VLAN. Por ejemplo, en el rango `2-4,5,10-20`, solo se utiliza `2`.
- CNOS reserva los Id. de VLAN 4000-4095 de manera predeterminada. El uso de Id. de VLAN reservados (bien por CNOS u otro usuario) puede provocar un error en el despliegue de la configuración del conmutador.

- Especifique un Id. de VLAN nativo con el que se etiqueta el tráfico no etiquetado. Este puede ser un número comprendido entre 1 y 4096.

  Notas:
  - Este campo es válido solo cuando el modo de puerto está establecido en “entroncamiento.”
  - Si no se especifica, o si el Id. está fuera del VLAN de estado final en un puerto, el puerto no permitirá el tráfico no etiquetado de manera efectiva.

- Seleccione **Crear VLAN** para crear el Id. de VLAN que falta actualmente en el conmutador de destino.

  Si un puerto pertenece a una VLAN que no se ha creado, el puerto continúa siendo un miembro de esa VLAN, pero el tráfico que está etiquetado con ese Id. de VLAN y alcanza el puerto, no puede pasar.

Paso 4. Haga clic en **Crear** para guardar la plantilla o haga clic en **Crear y desplegar** para guardar y desplegar inmediatamente la plantilla en uno o más servidores.

Para obtener información acerca del despliegue de una plantilla, consulte Despliegue de plantillas de configuración del conmutador en un conmutador de destino

Definir propiedades VLAN

Puede configurar las propiedades de VLAN avanzadas mediante la plantilla de configuración de propiedades de VLAN.

Procedimiento

Lleve a cabo los siguientes pasos para crear una plantilla de configuración de propiedades de VLAN.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Plantillas de configuración de conmutador**. Se muestra la página Plantillas de configuración de conmutador.

Paso 2. Haga clic en **VLAN → Configuración de propiedades VLAN** en el panel de navegación a la izquierda y haga clic en el ícono **Crear** ( ).

Paso 3. En el cuadro de diálogo Crear nueva plantilla, especifique la siguiente información.

- Introduzca el nombre y la descripción de la plantilla.
- Especifique un Id. de VLAN en el que aplicar los cambios. Este puede ser un número comprendido entre 1 y 4095.

  Nota: CNOS reserva los Id. de VLAN 4000-4095 de manera predeterminada. El uso de Id. de VLAN reservados (bien por CNOS u otro usuario) puede provocar un error en el despliegue de la configuración del conmutador.

- Especifique un nombre personalizado para VLAN.
- Elija si la VLAN está activa (habilitada) o suspendida (deshabilitada).
- Elija si el flujo de multidifusión IP (IPMC) en la VLAN de destino está controlada (habilitada) en interfaces IPv4 o IPv6. Puede presentar uno de los valores siguientes.
  - **Deshabilitar**. IPv4 e IPv6 están deshabilitadas.
  - **Habilitar**. IPv4 e IPv6 están habilitadas.

- **Deshabilitar IPv4**
- **Habilitar IPv4**
- **Deshabilitar IPv6**
- **Habilitar IPv6**

  Esta acción es aditiva, lo que significa que la función “Habilitar IPv4” se desplegó en la parte superior de los resultados de “Deshabilitar” en “Habilitar IPv4”, pero el despliegue en la parte superior de los resultados de “Habilitar IPv6” en “Habilitar.” Lo contrario también es verdad para las opciones de deshabilitar.

Paso 4. Haga clic en **Crear** para guardar la plantilla o haga clic en **Crear y desplegar** para guardar y desplegar inmediatamente la plantilla en uno o más servidores.

Para obtener información acerca del despliegue de una plantilla, consulte Despliegue de plantillas de configuración del conmutador en un conmutador de destino

Extracción de los valores de VLAN

Puede quitar interfaces de VLAN utilizando la plantilla de extracción de VLAN.

Procedimiento

Lleve a cabo los pasos siguientes para crear una plantilla de Extracción de VLAN.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Plantillas de configuración de conmutador**. Se muestra la página Plantillas de configuración de conmutador.

Paso 2. Haga clic en **VLAN → Eliminar VLAN** en el panel de navegación a la izquierdo y haga clic en el ícono **Crear** ( ).

Paso 3. En el cuadro de diálogo Crear nueva plantilla, especifique la siguiente información.

Importante: Debe especificar una o más interfaces L2 físicas o Id. de canal de puerto.

- Introduzca el nombre y la descripción de la plantilla.
- Especifique una o más interfaces L2 físicas válidas. Puede especificar una lista de interfaces separadas por una coma, un rango de Id., separados por un guion o una combinación de ambos, por ejemplo:
  - Ethernet1/10
  - Ethernet1/1,3,5,7
  - Ethernet1/1-10,21-30
  - Ethernet2/1-5,7,9,11-13
- Especifique uno o varios Id. de canal de puerto válidos (interfaces del agregador de puertos). Puede especificar una lista de números separados por una coma, un rango de números, separados por un guion o una combinación de ambos. Los valores e intervalos pueden ser números de 1 a 4096, por ejemplo:
  - 10
  - 1.3,5,7
  - 1-10,21-32
  - 1-5,7,9,11-13
- Especifique uno o más Id. de VLAN para eliminar de la lista de suscripciones VLAN del puerto. Puede especificar una lista de números separados por una coma, un rango de números, separados por un guion o una combinación de ambos. Los valores e intervalos pueden ser números de 1 a 4096, por ejemplo:
  - 10
  - 1.3,5,7

- 1-10,21-32
- 1-5,7,9,11-13

Nota: Si el modo de puerto está configurado en “Acceso”, la extracción de la VLAN hace que el puerto vaya a VLAN 1.

Paso 4. Haga clic en **Crear** para guardar la plantilla o haga clic en **Crear y desplegar** para guardar y desplegar inmediatamente la plantilla en uno o más servidores.

Para obtener información acerca del despliegue de una plantilla, consulte Despliegue de plantillas de configuración del conmutador en un conmutador de destino

Eliminar VLAN

Puede eliminar configuraciones VLAN del conmutador utilizando la plantilla de Eliminación de VLAN.

Procedimiento

Lleve a cabo los pasos siguientes para crear una plantilla de Eliminación de VLAN.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Plantillas de configuración de conmutador**. Se muestra la página Plantillas de configuración de conmutador.

Paso 2. Haga clic en **VLAN → Eliminación de VLAN** en el panel de navegación a la izquierdo y haga clic en el ícono **Crear** ( ).

Paso 3. En el cuadro de diálogo Crear nueva plantilla, especifique la siguiente información.

- Introduzca el nombre y la descripción de la plantilla.
- Especifique uno o más Id. de VLAN para eliminar de la lista de suscripciones VLAN del puerto. Puede especificar una lista de números separados por una coma, un rango de números, separados por un guion o una combinación de ambos. Los valores e intervalos pueden ser números de 1 a 4096, por ejemplo:
  - 10
  - 3,5,7,9
  - 5-10,21-32
  - 2-5,7,9,11-13

  Nota: No se pueden eliminar los Id. de VLAN reservados.

Paso 4. Haga clic en **Crear** para guardar la plantilla o haga clic en **Crear y desplegar** para guardar y desplegar inmediatamente la plantilla en uno o más servidores.

Para obtener información acerca del despliegue de una plantilla, consulte Despliegue de plantillas de configuración del conmutador en un conmutador de destino

Definición de la configuración básica del puerto de canal

Puede crear agregadores de puertos y agregar puertos a los agregadores utilizando una plantilla de configuración básica de canal de puerto.

Si el canal del puerto contiene puertos y algunos de esos puertos forman parte de la plantilla, sus propiedades (prioridad de puerto, modo y tiempo de espera) se actualizan con los valores de la plantilla al desplegar la plantilla.

Procedimiento

Lleve a cabo los pasos siguientes para crear una plantilla de canal de puerto básico.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Plantillas de configuración de conmutador**. Se muestra la página Plantillas de configuración de conmutador.

Paso 2. Haga clic en **Canal de puerto → Configuración básica** en el panel de navegación izquierdo y luego pulse el ícono **Crear** ( ).

Paso 3. En el cuadro de diálogo Crear nueva plantilla, especifique la siguiente información.

- Introduzca el nombre y la descripción de la plantilla.
- Especifique una o más interfaces L2 físicas válidas. Puede especificar una lista de interfaces separadas por una coma, un rango de Id., separados por un guion o una combinación de ambos, por ejemplo:
  - Ethernet1/10
  - Ethernet1/3,5,7,9
  - Ethernet1/5-10,21-32
  - Ethernet2/2-5,7,9,11-13
- Especifique el Id. de canal de puerto (interface del agregador de puertos) a crear o actualizar. Este puede ser un número comprendido entre 1 y 4095.
- Especifique el modo de puerto de protocolo de Control de agregación de enlace (LACP). Puede presentar uno de los valores siguientes.
  - **Activo**. (predeterminado) Habilita LACP sin condiciones
  - **Pasivo**. Habilita LACP solamente cuando se detecta un dispositivo LCAP.
  - **Static**. Deshabilita LCAP.

  Nota: Activo y pasivo se pueden mezclar en el mismo agregador, pero Estático no lo hace.
- Especifique el orden de prioridad del puerto LACP. Este puede ser un número comprendido entre 1 y 65535.

  Nota: La prioridad del puerto LACP se utiliza con el número de puerto en el Id. de puerto LACP.
- Especifique el modo de tiempo de espera LACP antes de que LCAP pase al modo individual. Puede presentar uno de los valores siguientes.
  - **Largo**. (predeterminado) 90 segundos
  - **Corto**. 3 segundos

Paso 4. Haga clic en **Crear** para guardar la plantilla o haga clic en **Crear y desplegar** para guardar y desplegar inmediatamente la plantilla en uno o más servidores.

Para obtener información acerca del despliegue de una plantilla, consulte Despliegue de plantillas de configuración del conmutador en un conmutador de destino

Definición de la configuración avanzada de puerto de canal

Puede configurar las propiedades de canal de puerto avanzadas usando la plantilla de Configuración avanzada de canal de puerto.

Procedimiento

Lleve a cabo los siguientes pasos para crear una plantilla de Configuración avanzada de canal de puerto.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Plantillas de configuración de conmutador**. Se muestra la página Plantillas de configuración de conmutador.

Paso 2. Haga clic en **Canal de puerto → Configuración avanzada** en el panel de navegación izquierdo y luego pulse el ícono **Crear** ( ).

Paso 3. En el cuadro de diálogo Crear nueva plantilla, especifique la siguiente información.

- Introduzca el nombre y la descripción de la plantilla.

- Especifique el Id. de canal de puerto (interface del agregador de puertos) a actualizar. Este puede ser un número comprendido entre 1 y 4095.
- Elija si los puertos individuales permanecen activos cuando se produce un error en LACP. Puede presentar uno de los valores siguientes.
  - **Activo**. (predeterminado) Habilita LACP sin condiciones.
  - **Suspendido**. Deshabilita LACP.
- Especifique el número mínimo de enlaces que deben estar activos para el canal de puerto se considere activo. Este puede ser un número comprendido entre 1 y 32.

Paso 4. Haga clic en **Crear** para guardar la plantilla o haga clic en **Crear y desplegar** para guardar y desplegar inmediatamente la plantilla en uno o más servidores.

Para obtener información acerca del despliegue de una plantilla, consulte Despliegue de plantillas de configuración del conmutador en un conmutador de destino

Eliminación de canales de puerto

Puede quitar los canales de puerto del conmutador utilizando la plantilla de Eliminación de canal de puerto.

Procedimiento

Lleve a cabo los siguientes pasos para crear una plantilla de Eliminación de canal de puerto.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Plantillas de configuración de conmutador**. Se muestra la página Plantillas de configuración de conmutador.

Paso 2. Haga clic en **Canal de puerto → Eliminar canal de puerto** en el panel de navegación izquierdo y luego pulse el ícono **Crear** ( ).

Paso 3. En el cuadro de diálogo Crear nueva plantilla, especifique la siguiente información.

- Introduzca el nombre y la descripción de la plantilla.
- Especifique uno o varios Id. de canal de puerto (interfaces del agregador de puertos) para eliminar. Puede especificar una lista de números separados por una coma, un rango de números, separados por una coma o una combinación de ambos. Los valores e intervalos pueden ser números de 1 a 4096, por ejemplo:
  - 10
  - 3,5,7,9
  - 5-10,21-32
  - 2-5,7,9,11-13

Paso 4. Haga clic en **Crear** para guardar la plantilla o haga clic en **Crear y desplegar** para guardar y desplegar inmediatamente la plantilla en uno o más servidores.

Para obtener información acerca del despliegue de una plantilla, consulte Despliegue de plantillas de configuración del conmutador en un conmutador de destino

Definición de los valores generales de conmutador

Puede configurar las propiedades generales del conmutador utilizando la plantilla de configuración genérica global.

Procedimiento

Lleve a cabo los pasos siguientes para crear una plantilla de configuración genérica global del conmutador.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Plantillas de configuración de conmutador**. Se muestra la página Plantillas de configuración de conmutador.

Paso 2. Haga clic en **Global → Configuración genérica** en el panel de navegación a la izquierda y haga clic en el ícono **Crear** ( ).

Paso 3. En el cuadro de diálogo Crear nueva plantilla, especifique la siguiente información.

- Introduzca el nombre y la descripción de la plantilla.
- Especifique la prioridad del sistema LACP que se utiliza para generar el Id. del sistema LACP. Este puede ser un número comprendido entre 1 y 65535.
- Elija dónde habilitar el etiquetado VLAN nativo. Puede presentar uno de los valores siguientes.
  - **Entrada y salida**
  - **Solo salida**

  Nota: Esta propiedad es admitida por CNOS 10.10.1 y posterior.

Paso 4. Haga clic en **Crear** para guardar la plantilla o haga clic en **Crear y desplegar** para guardar y desplegar inmediatamente la plantilla en uno o más servidores.

Para obtener información acerca del despliegue de una plantilla, consulte Despliegue de plantillas de configuración del conmutador en un conmutador de destino

Definición de los valores de la interfaz global de nivel 2

Puede configurar las propiedades de etiquetado de VLAN en interfaces L2 utilizando la plantilla de configuración de la interfaz L2.

Procedimiento

Lleve a cabo los pasos siguientes para crear una plantilla de configuración de interfaz de nivel 2.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Plantillas de configuración de conmutador**. Se muestra la página Plantillas de configuración de conmutador.

Paso 2. Haga clic en **Global → Configuración de interfaz L2** el panel de navegación a la izquierda y haga clic en el ícono **Crear** ( ).

Paso 3. En el cuadro de diálogo Crear nueva plantilla, especifique la siguiente información.

- Introduzca el nombre y la descripción de la plantilla.
- Especifique una o más interfaces L2 físicas válidas. Puede especificar una lista de interfaces separadas por una coma, un rango de Id., separados por un guion o una combinación de ambos, por ejemplo:
  - Ethernet1/10
  - Ethernet1/3,5,7,9
  - Ethernet1/5-10,21-32
  - Ethernet2/2-5,7,9,11-13
- Elija dónde habilitar el etiquetado VLAN nativo. Puede presentar uno de los valores siguientes.
  - **Entrada y salida**
  - **Solo salida**

  Nota: Esta propiedad es admitida por CNOS 10.10.1 y posterior.
- Elija si desea habilitar o deshabilitar el soporte de tunelización (QinQ).

  Nota: Esta propiedad es admitida por CNOS 10.10.1 y posterior.

Paso 4. Haga clic en **Crear** para guardar la plantilla o haga clic en **Crear y desplegar** para guardar y desplegar inmediatamente la plantilla en uno o más servidores.

Para obtener información acerca del despliegue de una plantilla, consulte Despliegue de plantillas de configuración del conmutador en un conmutador de destino

Definición de los valores de VLAG par

Puede configurar pares VLAG mediante la plantilla de configuración de pares VLAG.

Procedimiento

Lleve a cabo los pasos siguientes para crear una plantilla de configuración de pares VLAG.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Plantillas de configuración de conmutador**. Se muestra la página Plantillas de configuración de conmutador.

Paso 2. Haga clic en **VLAG → Configuración de pares** en el panel de navegación a la izquierda y haga clic en el ícono **Crear** ( ).

Paso 3. En el cuadro de diálogo Crear nueva plantilla, especifique la siguiente información.

- Introduzca el nombre y la descripción de la plantilla.
- Elija si desea habilitar o deshabilitar el VLAG.
- Para el Par 1 y Par 2, llene los siguientes campos. Se deben rellenar los campos para ambos pares.
  - Especifique la dirección IPv4 o IPv6 del par VLAG que se va a utilizar para la comprobación de estado.
  - Especifique el Id. del canal del puerto que se usa entre los dos pares. Este puede ser un número comprendido entre 1 y 4095.
  - Especifique el VRF que se utiliza para la comprobación del estado (por ejemplo, gestión, valores predeterminados o customVRF).

Paso 4. Haga clic en **Crear** para guardar la plantilla o haga clic en **Crear y desplegar** para guardar y desplegar inmediatamente la plantilla en uno o más servidores.

Para obtener información acerca del despliegue de una plantilla, consulte Despliegue de plantillas de configuración del conmutador en un conmutador de destino

Definición de los valores de VLAG

Puede crear o actualizar una instancia de VLAG utilizando la plantilla de configuración de instancia de VLAG. Una instancia de VLAG es un dispositivo que está conectado a ambos conmutadores (generalmente a través de una agregación de puertos) en la que el VLAG aparece como un solo dispositivo.

Procedimiento

Lleve a cabo los siguientes pasos para crear una plantilla de Configuración de instancia de VLAG.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Plantillas de configuración de conmutador**. Se muestra la página Plantillas de configuración de conmutador.

Paso 2. Haga clic en **VLAG → Configuración de instancia** en el panel de navegación a la izquierdo y haga clic en el ícono **Crear** ( ).

Paso 3. En el cuadro de diálogo Crear nueva plantilla, especifique la siguiente información.

- Introduzca el nombre y la descripción de la plantilla.
- Especifique el Id. de VLAG. Este puede ser un número comprendido entre 1 y 64.
- Especifique el Id. del canal de puerto que está conectado al par 1 y par 2. Puede ser un número entre 1 y 4095.

- Elija si desea habilitar o deshabilitar la instancia de VLAG.

Paso 4. Haga clic en **Crear** para guardar la plantilla o haga clic en **Crear y desplegar** para guardar y desplegar inmediatamente la plantilla en uno o más servidores.

Para obtener información acerca del despliegue de una plantilla, consulte Despliegue de plantillas de configuración del conmutador en un conmutador de destino

Definición de los valores avanzados de VLAG

Puede configurar las propiedades de VLAG avanzadas mediante la plantilla de configuración avanzada de VLAG.

Procedimiento

Lleve a cabo los siguientes pasos para crear una plantilla de configuración avanzada de VLAG.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Plantillas de configuración de conmutador**. Se muestra la página Plantillas de configuración de conmutador.

Paso 2. Haga clic en **VLAG → Configuración avanzada** en la configuración a la izquierda y haga clic en el ícono **Crear** ( ).

Paso 3. En el cuadro de diálogo Crear nueva plantilla, especifique la siguiente información.

- Introduzca el nombre y la descripción de la plantilla.
- Especifique el orden de prioridad que se utilizar para controlar cuál parte es la principal. Este puede ser un número comprendido entre 1 y 65535.

  Si no se especifica, se utiliza la prioridad predeterminada del conmutador. Para CNOS, el valor predeterminado es 0.
- Especifique el periodo de gracia, en segundos, para que el VLAG se conecte después de un reinicio simultáneo. Este puede ser un número comprendido entre 240 y 3600.

  Si no se especifica, se utiliza el valor predeterminado. Para CNOS, el valor predeterminado es 300.
- Especifique el Id. de nivel que se utiliza para diferenciar las configuraciones de VLAG en la misma red. Este puede ser un número comprendido entre 1 y 512.
- Especifique el intervalo de retraso de inicio de vLAG, en segundos, que se utiliza para retrasar la descarga de puertos después de que se vuelva a cargar el par. Este puede ser un número comprendido entre 0 y 3600.

  Si no se especifica, se utiliza el valor predeterminado. Para CNOS, el valor predeterminado es 120.
- Especifique el número de intentos de mantenimiento de conexiones de VLAG (mensajes de saludo no respondidos) antes de que se produzca un error en el VLAG. Este puede ser un número comprendido entre 1 y 24.

  Si no se especifica, se utiliza el valor predeterminado. Para CNOS, el valor predeterminado es 3.
- Especifique el intervalo, en segundos, entre los intentos de mantenimiento de VLAG. Este puede ser un número comprendido entre 2 y 300.

  Si no se especifica, se utiliza el valor predeterminado. Para CNOS, el valor predeterminado es 5.
- Especifique el intervalo, en segundos, entre los reintentos de mantenimiento de VLAG. Este puede ser un número comprendido entre 1 y 300.

  Si no se especifica, se utiliza el valor predeterminado. Para CNOS, el valor predeterminado es 30.

Paso 4. Haga clic en **Crear** para guardar la plantilla o haga clic en **Crear y desplegar** para guardar y desplegar inmediatamente la plantilla en uno o más servidores.

Para obtener información acerca del despliegue de una plantilla, consulte Despliegue de plantillas de configuración del conmutador en un conmutador de destino

Eliminación de una instancia de VLAG

Puede eliminar una instancia VLAG mediante la plantilla de eliminación de instancia VLAG.

Procedimiento

Lleve a cabo los pasos siguientes para crear una plantilla de eliminación de instancia de VLAG.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Plantillas de configuración de conmutador**. Se muestra la página Plantillas de configuración de conmutador.

Paso 2. Haga clic en **VLAG → Eliminación de instancia** en el panel de navegación a la izquierdo y haga clic en el ícono **Crear** ( ).

Paso 3. En el cuadro de diálogo Crear nueva plantilla, especifique la siguiente información.

- Introduzca el nombre y la descripción de la plantilla.
- Especifique el Id. único de la instancia de VLAG. Este puede ser un número comprendido entre 1 y 64.

Paso 4. Haga clic en **Crear** para guardar la plantilla o haga clic en **Crear y desplegar** para guardar y desplegar inmediatamente la plantilla en uno o más servidores.

Para obtener información acerca del despliegue de una plantilla, consulte Despliegue de plantillas de configuración del conmutador en un conmutador de destino

Definición de una topología spine-leaf

Puede verificar la topología física y desplegar una configuración de SpineLeaf (entramado L3) en los conmutadores gestionados utilizando la plantilla del asistente de topología de Spine-Leaf.

Procedimiento

Lleve a cabo los pasos siguientes para crear una plantilla de Asistente de topología Spine-Leaf.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Plantillas de configuración de conmutador**. Se muestra la página Plantillas de configuración de conmutador.

Paso 2. Haga clic en **Spine-Leaf → Asistente de topología** en el panel de navegación a la izquierda y haga clic en el ícono **Crear** ( ).

Paso 3. En el cuadro de diálogo Crear nueva plantilla, especifique la siguiente información.

- Introduzca el nombre y la descripción de la plantilla.
- Especifique el número del sistema autónomo (AS) para el Protocolo de puerta de enlace de borde (BGP) que se está ejecutando en el conmutador. Este puede ser un número comprendido entre 1 y 4294967295.

  Nota: Esto es admitido por CNOS 10.9.3 y posterior.
- Elija si desea permitir vínculos únicos entre los conmutadores.

  Normalmente, el despliegue produce un error si no hay al menos dos enlaces entre cualquier conmutador de Spine y Leaf.

Paso 4. Haga clic en **Crear** para guardar la plantilla o haga clic en **Crear y desplegar** para guardar y desplegar inmediatamente la plantilla en uno o más servidores.

Para obtener información acerca del despliegue de una plantilla, consulte Despliegue de plantillas de configuración del conmutador en un conmutador de destino

Despliegue de plantillas de configuración del conmutador en un conmutador de destino

Puede definir los valores de puerto VLAN mediante la creación de una plantilla de configuración de puerto VLAN.

Acerca de esta tarea

Existen tres tipos de despliegues:

- **Normal**. Despliega valores de configuración del conmutador a uno o varios conmutadores de bastidor en una arquitectura de capas básica.
- **VLAG**. Despliega valores de configuración de conmutador a exactamente dos conmutadores que admiten una arquitectura de enlace virtual de grupo de agregación (VLAG). Los conmutadores deben ser del mismo modelo y versión de software.
- **Spine-Leaf**. Plantillas de implementación para uno o varios conmutadores de spine y conmutadores de leaf.

Procedimiento

Para desplegar una plantilla de configuración de conmutador en uno o varios conmutadores gestionados, lleve a cabo los pasos siguientes.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Plantillas de configuración de conmutador**. Se muestra la página Plantillas de configuración de conmutador.

Paso 2. Seleccione una o más plantillas de configuración de conmutadores para desplegar.

Paso 3. Haga clic en el icono **Desplegar** ( ) para mostrar el cuadro de diálogo Desplegar plantilla.

Paso 4. Seleccione uno o más conmutadores a los que desea desplegar las plantillas.

Solo se muestran los conmutadores que son compatibles con las plantillas seleccionadas.

Paso 5. Haga clic en **Desplegar**. Se muestra un cuadro de diálogo con el estado de despliegue de cada conmutador seleccionado.

Paso 6. Haga clic en **Desplegar** de nuevo para iniciar el proceso de despliegue.

Nota: El despliegue puede tardar en completarse varios minutos.

Después de finalizar

Puede ver el historial de despliegue (consulte Visualización del historial de despliegue de la configuración del conmutador).

Visualización del historial de despliegue de la configuración del conmutador

Puede ver información acerca de plantillas de configuración del conmutador que se desplegaron a los conmutadores gestionados, incluidos el nombre de la plantilla, el tipo de plantilla, indicación de hora y los

conmutadores en el que se despliegan. Cada despliegue contiene una instantánea de la plantilla como estaba cuando se desplegó.

Procedimiento

Realice los siguientes pasos para ver el historial de despliegue de configuración del conmutador.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Plantillas de configuración de conmutador**. Se muestra la página Plantillas de configuración de conmutador.

Paso 2. Expanda **Despliegue** y haga clic en **Historial** en el panel de navegación izquierdo para mostrar una tabla de plantillas desplegadas.

La columna **Estado** indica si el despliegue de configuración se realizó correctamente. Puede ser uno de los siguientes estados:

- **Exitoso**. El despliegue de configuración en todos los conmutadores de destino se completó correctamente.
- **Advertencia**. El despliegue de la configuración en uno o varios conmutadores de destino se completaron con advertencias.
- **Con error**. El despliegue de la configuración en uno o varios conmutadores de destino presentaron errores.

Después de finalizar

- Ver la información acerca de cada plantilla desplegada, incluido lo que se desplegó y lo que se realizó correctamente o con errores, haciendo clic en el nombre de la plantilla en la tabla.
- Elimine el historial de despliegue seleccionando un despliegue y haga clic en el ícono **Eliminar** ( ).

Capítulo 13. Actualización de firmware en dispositivos gestionados

Desde la interfaz web de Lenovo XClarity Administrator, puede descargar, instalar y gestionar las actualizaciones de firmware para los dispositivos gestionados, incluidos chasis, servidores, sistemas de almacenamiento y conmutadores. Puede asignar políticas de cumplimiento de firmware a los dispositivos gestionados para asegurarse de que el firmware en esos dispositivos se mantiene conforme. También puede crear y editar políticas de cumplimiento de firmware si los niveles de firmware validados no coinciden con las políticas predefinidas sugeridas.

Más información:
- XClarity Administrator: Aumento de la eficiencia al actualizar firmware
- Prácticas recomendadas para las actualizaciones de firmware y de controladores de Lenovo ThinkSystem
- XClarity Administrator: implementación básica a clúster
- XClarity Administrator: actualización de firmware
- XClarity Administrator: aprovisionamiento de actualizaciones de seguridad de firmware

Antes de empezar

La actualización del firmware y de los controladores de dispositivo son procesos independientes en XClarity Administrator; no existe una conexión entre estos procesos. XClarity Administrator no mantiene la conformidad entre el firmware y los controladores de dispositivos en dispositivos gestionados, aunque se recomienda actualizar los controladores de dispositivo al mismo tiempo que el firmware.

Acerca de esta tarea

Nota: Un sistema operativo no tiene la obligación de actualizar el firmware. En servidores sin sistema operativo, asegúrese de que el servidor esté apagado antes de actualizar el firmware.

Puede gestionar y aplicar las actualizaciones de firmware de los siguientes dispositivos gestionados.
- **Chasis**. Actualizaciones de CMM
- **ThinkAgile, ThinkSystem, System x, Converged, Flex System y servidores NeXtScale**. Actualizaciones del controlador de gestión de la placa base, UEFI, DSA, entretapa y adaptador
- **Conmutadores RackSwitch y Flex System**
- **Dispositivos de almacenamiento Lenovo Storage y ThinkSystem DM Storage**
- **Dispositivos de la biblioteca de cintas IBM TS4300**

El firmware de los siguientes dispositivos no se puede actualizar mediante XClarity Administrator.

- **Servidores ThinkServer**. Consulte la documentación que se le proporcionó con el servidor para obtener información sobre cómo actualizar el firmware.
- **Nodos de cálculo de Flex Power Systems**. Existen varios métodos para actualizar el firmware de los nodos de cálculo de Flex Power Systems. Para obtener más información, consulte el apartado Documentación en línea de nodos de cálculo p260/p460 IBM Flex System. El proceso para otros nodos de cálculo de Flex Power Systems es similar.
- **Los conmutadores Flex que se encuentran en el modo apilado o el modo protegido**. *No puede* actualizar firmware en conmutadores apilados. La actualización de firmware está deshabilitada para todos los conmutadores que están apilados.
- **Conmutadores Flex**. Si está utilizando el siguiente conmutador, consulte la documentación que se le proporcionó con el conmutador para obtener información sobre cómo actualizar el firmware.

– Cisco Nexus B22 Fabric Extender

Procedimiento

En la siguiente figura se muestra el flujo de trabajo para actualizar el firmware en los dispositivos gestionados.

Paso 1. **Gestione el repositorio de actualizaciones de firmware.**

El *repositorio de actualizaciones de firmware* contiene un catálogo de las actualizaciones disponibles y los paquetes de actualización que se pueden aplicar a los dispositivos gestionados.

El *catálogo* contiene información acerca de las actualizaciones de firmware que se encuentran disponibles en la actualidad para todos los dispositivos compatibles con XClarity Administrator. El catálogo organiza las actualizaciones de firmware por tipo de dispositivo. Cuando actualiza el catálogo, XClarity Administrator recupera información acerca de las últimas actualizaciones de firmware disponibles en el sitio web de Lenovo (incluidos los archivos metadata.xml o .json y readme.txt) y almacena la información en el repositorio de actualizaciones de firmware. No se descarga el archivo de carga útil (.exe). Para obtener más información sobre actualizar el catálogo, consulte Actualización del catálogo de productos.

Si hay nuevas actualizaciones de firmware disponibles, debe descargar los paquetes de actualización antes de poder actualizar dicho firmware en los dispositivos gestionados. La actualización del catálogo no descarga automáticamente los paquetes de actualizaciones. La tabla de **Catálogo de productos** en la página del Repositorio de actualizaciones de firmware identifica qué paquetes de actualización se descargan y cuáles están disponibles para descargarse.

Puede descargar las actualizaciones de firmware de varias maneras distintas:

- **Paquetes del repositorio de actualizaciones de firmware**

  Los paquetes del repositorio de actualización de firmware son colecciones de las actualizaciones de firmware más recientes que están disponibles al mismo tiempo que la versión XClarity Administrator para la mayoría de los dispositivos compatibles y una política de cumplimiento de firmware actualizada predeterminada. Estos paquetes del repositorio se importan y luego se aplican desde la página Actualizar servidor de gestión. Cuando aplica un paquete del repositorio de actualización de firmware, cada paquete de actualización del paquete se agrega en el repositorio de actualizaciones de firmware y una política de cumplimiento de firmware predeterminada se crea automáticamente para todos los dispositivos gestionables. También puede copiar esta política predefinida, pero no se puede cambiar.

  Los siguientes paquetes de repositorio están disponibles.

  – **lnvgy_sw_lxca_cmmswitchrepo***x-x.x.x*_**anyos_noarch**. Contiene las actualizaciones de firmware para todos los CMM y conmutadores Flex System.
  – **lnvgy_sw_lxca_storagerackswitchrepo***x-x.x.x*_**anyos_noarch**. Contiene las actualizaciones de firmware para todos los conmutadores RackSwitch y dispositivos Lenovo Storage.
  – **lnvgy_sw_lxca_systemxrepo***x-x.x.x*_**anyos_noarch**. Contiene las actualizaciones de firmware para todos los servidores serie Converged HX, Flex System, NeXtScale y System x.

- **lnvgy_sw_thinksystemrepo***x-x.x.x*_**anyos_noarch**. Contiene actualizaciones de firmware para todos los servidores ThinkAgile y ThinkSystem.
- **lnvgy_sw_lxca_thinksystemv2repo***x-x.x.x*_**anyos_noarch**. Contiene actualizaciones de firmware para todos los servidores ThinkAgile y ThinkSystem V2.
- **lnvgy_sw_lxca_thinksystemv3repo***x-x.x.x*_**anyos_noarch**. Contiene actualizaciones de firmware para todos los servidores ThinkAgile y ThinkSystem V3.

Puede determinar si los paquetes del repositorio de actualizaciones de firmware deben almacenarse en el repositorio desde la columna **Estado de descarga** de la página Actualizar servidor de gestión. Esta columna contiene los siguientes valores:

- **Descargado**. El paquete del repositorio de actualizaciones de firmware se almacena en el repositorio.
- **No descargado**. El paquete del repositorio de actualizaciones de firmware está disponible, pero no se almacena en el repositorio.

- **UpdateXpress System Packs (UXSPs)**

  Nota: Para los servidores con XCC2, estos paquetes se conocen como paquetes de firmware. El *paquete* se utiliza en los nombres de los paquetes y en los nombres de las políticas predefinidas.

  UXSP contiene las últimas actualizaciones de firmware y controlador de dispositivo disponibles, organizadas por sistema operativo. Cuando descargue UXSP, XClarity Administrator descarga el UXSP en función de la versión enumerada en el catálogo y almacena los paquetes de actualizaciones en el repositorio de actualizaciones de firmware. Cuando descarga un UXSP, cada actualización de firmware del UXSP se añade al repositorio de actualizaciones de firmware y se enumera en la pestaña **Actualizaciones individuales**, y se crea automáticamente una política de cumplimiento de firmware predeterminada para todos los dispositivos gestionables que utilizan los nombres siguientes. También puede copiar esta política predefinida, pero no se puede cambiar.
  - *{uxsp-version}-{date}-{server-short-name}***-UXSP** (por ejemplo, `v1.50-2017-11-22- SD530-UXSP`)
  - *{uxsp-version}-{buildnumber}-{server-short-name}***-bundle** (por ejemplo, `22a.0-kaj92va-SR650V3-bundle`)

  Nota: Cuando descarga o importa UXSP desde la página Actualizaciones de firmware: Repositorio, solo se descargan las actualizaciones de firmware y se almacenan en el repositorio. Se descartan actualizaciones del controlador de dispositivo. Para obtener información acerca de cómo descargar o importar actualizaciones de controladores de dispositivos de Windows mediante UXSP, consulte Gestión del repositorio de controladores de dispositivos del SO.

  Puede determinar si los UXSP están almacenados en el repositorio de actualizaciones de firmware desde la columna **Estado de descarga** en la pestaña **Actualizaciones individuales** en la página Actualizaciones de firmware: Repositorio. Esta columna contiene los siguientes valores:

  - **Descargado**. El paquete de actualizaciones completo o cada actualización de firmware se almacenan en el repositorio.
  - *x* **de** *y* **descargado**. Algunas de las actualizaciones de firmware del paquete de actualización se almacenan en el repositorio, pero no todas. Los números entre paréntesis indican el número de actualizaciones disponibles y el número de actualizaciones almacenadas, o no hay actualizaciones para el tipo de dispositivo específico.
  - **No descargado**. El paquete de actualización completo o la actualización de firmware individual no se almacenan en el repositorio.

- **Actualizaciones de firmware individuales**

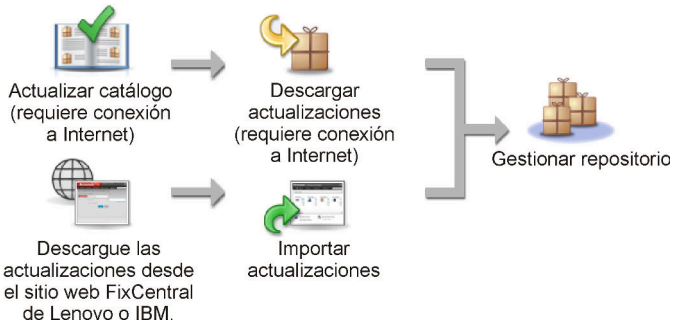
Puede descargar paquetes de actualización de firmware individuales, uno detrás de otro. Cuando descargue paquetes de actualización de firmware, XClarity Administrator descarga la actualización en función de la versión enumerada en el catálogo y almacena los paquetes de actualizaciones en el repositorio de actualizaciones de firmware. A continuación, puede crear políticas de cumplimiento de firmware utilizando dichos paquetes de actualización para cada uno de sus dispositivos gestionados.

Nota: Las actualizaciones de firmware principales (como el controlador de gestión, UEFI y pDSA) no dependen del sistema operativo. Los paquetes de actualización de firmware para los sistemas operativos RHEL 6 o SLES 11 se utilizan para actualizar nodos de cálculo y servidores de bastidor. Para obtener más información acerca de los paquetes de actualización de firmware que deben utilizarse para sus servidores gestionados, consulte Descarga de actualizaciones de firmware.

Puede determinar si hay *actualizaciones de firmware* específicas almacenadas en el repositorio de actualizaciones de firmware desde la columna **Estado de descarga** en la pestaña **Actualizaciones individuales** en la página Actualizaciones de firmware: Repositorio. Esta columna contiene los siguientes valores.

- **Descargado**. El paquete de actualizaciones completo o cada actualización de firmware se almacenan en el repositorio.
- *x* **de** *y* **descargado**. Algunas de las actualizaciones de firmware del paquete de actualización se almacenan en el repositorio, pero no todas. Los números entre paréntesis indican el número de actualizaciones disponibles y el número de actualizaciones almacenadas, o no hay actualizaciones para el tipo de dispositivo específico.
- **No descargado**. El paquete de actualización completo o la actualización de firmware individual no se almacenan en el repositorio.

XClarity Administrator debe estar conectado a Internet para actualizar el catálogo y descargar las actualizaciones de firmware. Si no está conectado a Internet, puede descargar manualmente los archivos en una estación de trabajo que tenga acceso de red al host de XClarity Administrator utilizando un navegador web y luego importar los archivos al repositorio de actualizaciones de firmware.



Cuando importa manualmente las actualizaciones de firmware en XClarity Administrator, debe incluir los siguientes archivos obligatorios: carga útil (imagen y MIB), metadatos, historial de cambios y archivo léame. Por ejemplo:

- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.tgz
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.xml
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.chg
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.txt

Atención:

- Solo importe estos archivos necesarios. No importe otros archivos que puedan encontrarse en los sitios web de descarga de firmware.
- Si no incluye el archivo XML en el paquete de actualizaciones, la actualización no se importa.
- Si no incluye todos los archivos requeridos que están asociados a la actualización, el repositorio muestra que la actualización no se descarga, lo que significa que se importa parcialmente. Posteriormente, puede incorporar los archivos que falten seleccionándolos e importándolos.
- Las actualizaciones de firmware principales (como el controlador de gestión, UEFI y pDSA) no dependen del sistema operativo. Los paquetes de actualización de firmware para los sistemas operativos RHEL 6 o SLES 11 se utilizan para actualizar nodos de cálculo y servidores de bastidor. Para obtener más información acerca de los paquetes de actualización de firmware que deben utilizarse para sus servidores gestionados, consulte Descarga de actualizaciones de firmware.

Para obtener más información sobre las actualizaciones de firmware, consulte Gestión del repositorio de actualizaciones de firmware.

Paso 2. **(Opcional) Creación y asignación de políticas de cumplimiento de firmware**

Las Políticas de cumplimiento de firmware garantizan que el firmware de determinados dispositivos gestionados se encuentra en el nivel actual o especificado marcando los dispositivos que necesitan atención. Cada política de cumplimiento de firmware identifica qué dispositivos se supervisan y qué nivel de firmware se debe instalar a fin de mantener la conformidad de los dispositivos. Puede establecer la conformidad en el nivel del dispositivo o del componente de firmware. XClarity Administrator luego utiliza estas políticas para comprobar el estado de los dispositivos gestionados e identificar los dispositivos que están fuera de conformidad.

Cuando cree una política de cumplimiento de firmware, puede elegir que XClarity Administrator distinga un dispositivo cuando:
- El firmware del dispositivo sea de un nivel inferior
- El firmware del dispositivo no coincide con la versión del destino de cumplimiento

XClarity Administrator viene con una política de cumplimiento de firmware predefinida con el nombre de **firmware más reciente en el repositorio**. Cuando se descargan o se importan nuevos firmware en el repositorio, esta política se actualiza a fin de incluir las versiones de firmware más recientes disponibles en el repositorio.

Después de asignar una política de cumplimiento de firmware a un dispositivo, XClarity Administrator comprueba el estado de cumplimiento de cada dispositivo cambia el inventario del dispositivo o el repositorio de actualizaciones de firmware. Cuando el firmware de un dispositivo no está en cumplimiento con la política asignada, XClarity Administrator identifica ese dispositivo como no en cumplimiento en la página Actualizaciones de firmware: aplicar/activar, en función de la regla que ha especificado en la política de cumplimiento de firmware

Por ejemplo, puede crear una política de cumplimiento de firmware que defina el nivel de línea base para el firmware que está instalado en todos los dispositivos ThinkSystem SR850 y, a continuación, asignar esa política de cumplimiento de firmware a todos los dispositivos

ThinkSystem SR850. Cuando el repositorio de actualizaciones de firmware se actualiza y se agrega una nueva actualización de firmware, esos nodos de cálculo podrían estar fuera de conformidad. Si esto ocurre, XClarity Administrator actualiza la página Actualizaciones de firmware: Aplicar/Activar para mostrar los dispositivos que no son conformes y genera una alerta.

Nota: Puede elegir mostrar u ocultar las alertas de los dispositivos que no cumplen con los requisitos de las políticas de cumplimiento de firmware asignadas (consulte Configuración de los valores globales de actualización de firmware). De forma predeterminada, las alertas están ocultas.

Para obtener más información sobre las políticas de conformidad de firmware, consulte Creación y asignación de políticas de cumplimiento de firmware.

Paso 3. **Aplicación y activación de actualizaciones**

XClarity Administrator no aplica automáticamente las actualizaciones de firmware a los dispositivos gestionados. Para actualizar el firmware, debe aplicar y activar manualmente la actualización en los dispositivos seleccionados. Puede aplicar el firmware mediante uno de los métodos siguientes.

- **Aplique actualizaciones de firmware del paquete con políticas de cumplimiento**

  Puede aplicar actualizaciones de firmware a *todos* los componentes de los dispositivos seleccionados de acuerdo con la política de cumplimiento de firmware asignada mediante una imagen del paquete que contenga los paquetes de actualización de firmware aplicables.

  El proceso de actualización del paquete actualiza primero el controlador de gestión de la placa base y la UEFI fuera de banda. Una vez completadas estas actualizaciones, el proceso crea una imagen del paquete del firmware restante de la política de cumplimiento según el tipo de equipo. A continuación, el proceso monta la imagen en el dispositivo seleccionado y reinicia el dispositivo para arrancar la imagen. La imagen se ejecuta automáticamente para realizar el resto de actualizaciones.

  Atención: Los dispositivos seleccionados se apagan antes de iniciar el proceso de actualización. Asegúrese de que todas las cargas de trabajo en ejecución se hayan detenido o, si está trabajando en un entorno virtualizado, se hayan desplazado a otro servidor. Si hay trabajos en ejecución, el trabajo de actualización queda en cola hasta que se completen todos los otros trabajos. Para ver una lista de los trabajos activos, pulse **Supervisión → Trabajos**.

  Notas:

  - La aplicación de actualizaciones de firmware del paquete solo es compatible con los servidores ThinkSystem SR635 y SR655.
  - La aplicación de actualizaciones de firmware del paquete solo es compatible con las direcciones IPv4. No se admiten las direcciones IPv6.
  - Asegúrese de que cada dispositivo de destino se haya arrancado en el SO al menos una vez para recuperar la información completa del inventario.
  - Se requiere el firmware v2.94 o posterior del controlador de gestión de la placa base para utilizar la función de actualización del paquete.
  - Solo se utilizan actualizaciones de firmware de paquetes de repositorios o actualizaciones de firmware individuales. No se admiten UpdateXpress System Packs (UXSPs).
  - Solo se aplican las actualizaciones de firmware descargadas. Actualice el catálogo de productos y descargue las actualizaciones de firmware adecuadas (consulte Actualización del catálogo de productos y Descarga de actualizaciones de firmware).

    Nota: Cuando XClarity Administrator se instala por primera vez, el catálogo de productos y el repositorio están vacíos.

- La comprobación de conformidad solo es compatible con el controlador de gestión de la placa base y la UEFI en los servidores ThinkSystem SR635 y SR655; sin embargo, XClarity Administrator intenta aplicar actualizaciones de firmware a todos los componentes de hardware disponibles.
- Las actualizaciones se aplican de acuerdo con la política de cumplimiento de firmware asignada. No puede optar por actualizar un subconjunto de componentes.
- Se requiere XClarity Administrator v3.2 o posterior para aplicar actualizaciones de firmware para Lenovo XClarity Provisioning Manager (LXPM), controladores Windows LXPM o controladores Linux LXPM a servidores ThinkSystem SR635 y SR655.
- Las actualizaciones del controlador de gestión de la placa base y de la UEFI se omiten si la versión instalada en el momento es mayor que la política de cumplimiento asignada.
- Las políticas de cumplimiento de firmware se deben crear y asignar a los dispositivos en los que tenga previsto aplicar las actualizaciones de firmware. Para obtener más información, consulte el apartado Creación y asignación de políticas de cumplimiento de firmware.
- Los dispositivos seleccionados se apagan antes de iniciar el proceso de actualización. Asegúrese de que todas las cargas de trabajo en ejecución se hayan detenido o, si está trabajando en un entorno virtualizado, se hayan desplazado a otro servidor.

- **Aplique las actualizaciones de firmware seleccionadas con o sin utilizar políticas de cumplimiento**

  Puede aplicar actualizaciones de firmware a componentes y dispositivos seleccionados de acuerdo con la política de cumplimiento de firmware asignada mediante paquetes de actualización de firmware aplicables. También puede optar por aplicar actualizaciones de firmware posteriores al firmware instalado actualmente en componentes y dispositivos seleccionados sin usar políticas de cumplimiento.

  Puede optar por aplicar las actualizaciones para todos los componentes en un dispositivo específico. También puede elegir optar por actualizar solo un subconjunto de componentes en los dispositivos seleccionados, como el controlador de gestión de la placa base o la UEFI.

  Para activar las actualizaciones de firmware, los dispositivos se deben reiniciar. Tenga en cuenta que el reinicio de un dispositivo provoca una interrupción. Puede elegir si reinicia los dispositivos como parte del proceso de actualización (lo que se denomina *activación inmediata*) o si espera a que una ventana de mantenimiento esté disponible para reiniciar los dispositivos (lo que se denomina *activación con retardo*). En este caso, tiene que reiniciar manualmente el dispositivo para que la actualización surta efecto.

  Si elige actualizar el firmware de un dispositivo gestionado, se producen los pasos siguientes.

  1. XClarity Administrator envía actualizaciones de firmware (por ejemplo, para el controlador de gestión, UEFI y DSA) al dispositivo.
  2. Cuando se reinicia el dispositivo, las actualizaciones de firmware se activan en el dispositivo.
  3. En el caso de servidores, XClarity Administrator envía actualizaciones para los dispositivos opcionales, como el adaptador de red y la unidad de disco duro. XClarity Administrator aplica estas actualizaciones y el servidor se reinicia.
  4. Si reinicia el dispositivo o elige la activación inmediata, se activan las actualizaciones de los dispositivos opcionales.

  Notas:

  - Cuando se aplican actualizaciones mediante políticas de cumplimiento, se debe crear una política de cumplimiento de firmware y asignarla a cada dispositivo de destino. Para obtener más información, consulte el apartado Creación y asignación de políticas de cumplimiento de firmware.

- Si elige instalar un paquete de actualización de firmware que contiene actualizaciones para varios componentes, se actualizan todos los componentes a los que se aplica dicho paquete de actualización.
- Las actualizaciones realizadas en los CMM y conmutadores Flex se activan siempre de forma inmediata, incluso si selecciona la activación con retardo.

Cuando realiza actualizaciones en un conjunto de dispositivos, XClarity Administrator realiza las actualizaciones en el orden siguiente.

- CMM del chasis
- Conmutadores RackSwitch y Flex System
- Nodos de cálculo Flex y servidores de bastidor y de torre
- Dispositivos Lenovo Storage

Atención: Antes de intentar aplicar las actualizaciones de firmware en los dispositivos gestionados, asegúrese de realizar las acciones siguientes.

- Antes de actualizar el firmware en los dispositivos gestionados, lea las consideraciones sobre la actualización de firmware (consulte Consideraciones sobre la actualización de firmware).
- Inicialmente, los dispositivos que no admiten actualizaciones se ocultan en la vista. No se puede seleccionar los dispositivos que no se admiten actualizaciones.
- De manera predeterminada, todos los componentes detectados se muestran como disponibles para aplicar actualizaciones; no obstante, un firmware de nivel inferior puede impedir que un componentes aparezca en el inventario o presente la información completa de la versión. Para mostrar todos los paquetes basados en políticas que están disponibles para aplicar actualizaciones, haga clic en **Todas las acciones → Valores globales** y, a continuación, seleccione **Compatibilidad mejorada para dispositivos de nivel inferior**. Si esta opción está seleccionada, aparece “Otro software disponible” en la columna Installed Version (Versión instalada) de los dispositivos no detectados. Para obtener más información, consulte el apartado Configuración de los valores globales de actualización de firmware.

  Notas:

  - Los valores globales no se pueden cambiar cuando las actualizaciones en los dispositivos gestionados están en curso.
  - Las opciones adicionales tardan unos minutos en generarse. Después de unos instantes, puede que tenga que hacer clic en icono **Actualizar** () para actualizar la tabla.
- Asegúrese de que no haya trabajos que se encuentren en ejecución en la actualidad en el servidor de destino. Si hay trabajos en ejecución, el trabajo de actualización queda en cola hasta que se completen todos los otros trabajos. Para ver una lista de los trabajos activos, haga clic en **Supervisión → Trabajos**.
- Asegúrese de que el repositorio de actualizaciones de firmware contiene los paquetes de firmware que desea desplegar. En caso contrario, actualice el catálogo de productos y descargue las actualizaciones de firmware adecuadas (consulte Actualización del catálogo de productos y Descarga de actualizaciones de firmware).

  Nota: Cuando XClarity Administrator se instala por primera vez, el catálogo de productos y el repositorio están vacíos.

  Si tiene intención de instalar el firmware de requisito previo, asegúrese de que este también se descargue en el repositorio.

  En algunos casos, se pueden necesitar varias versiones para actualizar el firmware y todas las versiones se deberán descargar en el repositorio. Por ejemplo, para actualizar el conmutador escalable SAN de IBM FC5022 v7.4.0a a v8.2.0a, primero debe instalar v8.0.1-pha, v8.1.1 y

luego v8.2.0a. Las tres versiones deben estar en el repositorio para actualizar el conmutador para v8.2.0a.

- Por lo general, los dispositivos deben reiniciarse para activar la actualización de firmware. Si elige reiniciar el dispositivo durante el proceso de actualización (*activación inmediata*), asegúrese de que las cargas de trabajo en ejecución se hayan detenido o, si está trabajando en un entorno virtualizado, se hayan desplazado a otro servidor.

Para obtener más información sobre cómo instalar actualizaciones, consulte Aplicación y activación de actualizaciones de firmware.

Consideraciones sobre la actualización de firmware

Antes de empezar a actualizar el firmware para los dispositivos gestionados utilizando Lenovo XClarity Administrator, tenga en cuenta las siguientes consideraciones importantes.

- Consideraciones generales
- Consideraciones acerca de CMM
- Consideraciones del controlador de gestión de la placa base
- Consideraciones de dispositivo ThinkSystem
- Consideraciones de dispositivo Flex System
- Consideraciones de almacenamiento

Consideraciones generales

- **Niveles de firmware mínimos que se requieren.**

  Asegúrese de que el firmware que está instalado en cada dispositivo gestionado esté en el nivel mínimo necesario antes de utilizar XClarity Administrator para actualizar el firmware en esos dispositivos. 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.

  Nota: Para obtener información acerca del soporte y las limitaciones conocidas de los dispositivos de E/S, consulte Soporte de XClarity Administrator: página web de compatibilidad.

- **Actualice todos los componentes en el nivel que está incluido en el repositorio de actualizaciones de firmware.**

  Puesto que las actualizaciones de firmware de componentes de Flex System se prueban y se lanzan conjuntamente, se recomienda que mantenga el mismo nivel de firmware en todos los componentes de un chasis de Flex System. Por lo tanto, es importante actualizar el firmware en todos los componentes del chasis en la misma ventana de mantenimiento. XClarity Administrator aplica automáticamente las actualizaciones seleccionadas en la secuencia correcta.

- **No se incluyen los controladores Linux LXPM y los controladores Windows LXPM cuando se descargan UXSP**

  Los controladores de Linux y Windows de Lenovo XClarity Provisioning Manager (LXPM) no se incluyen en UpdateXpress System Packs (UXSPs). Para aplicar estos paquetes de actualización a sus dispositivos, descargue los paquetes del repositorio de actualizaciones de firmware más recientes o descargue manualmente los paquetes individuales y cree una política de cumplimiento de firmware que incluya estos paquetes.

- **Algunas actualizaciones de firmware son codependientes en un nivel mínimo de controlador de dispositivo.**

Antes de aplicar las actualizaciones de firmware de E/S y adaptador en un servidor, puede que tenga que actualizar el controlador de dispositivo a un nivel mínimo. En general, las actualizaciones de firmware no dependen de niveles específicos de controladores de dispositivo. Consulte el archivo readme de la actualización de firmware para conocer las codependencias mencionadas y actualice los controladores de dispositivo de su sistema operativo antes de actualizar el firmware. XClarity Administrator no actualiza los controladores de dispositivo del sistema operativo.

- **Reinicie XClarity Administrator antes de actualizar el firmware**

  Si los intentos anteriores de actualizar el firmware fallan, reinicie XClarity Administrator antes de actualizar el firmware. Si se reinicia el servidor de gestión, se garantiza que la cuenta reservada del sistema que se utiliza para actualizar el firmware se sincroniza en los dispositivos gestionados.

- **Las actualizaciones de firmware conllevan una interrupción y requieren que las cargas de trabajo estén inactivas en los dispositivos.**

  Llevar a cabo actualizaciones de firmware en dispositivos gestionados supone una interrupción si opta por activar inmediatamente la actualización. Debe desactivar los dispositivos antes de actualizar el firmware mediante la activación inmediata.

  Cuando actualiza el firmware en los servidores, los servidores se apagan y se colocan en un sistema operativo de mantenimiento a fin de actualizar los controladores de dispositivo para los adaptadores, las unidades de disco y las unidades de estado sólido.

  Conmutadores Flex en un chasis determinado se actualizan secuencialmente y se reinician durante el proceso de actualización de firmware. La implementación de rutas de datos redundantes disminuye las interrupciones, pero todavía puede haber una breve interrupción en la conectividad de la red durante la actualización de firmware.

- **No utilice XClarity Administrator para actualizar el firmware del servidor en el que XClarity Administrator se encuentra en ejecución.**

  Si XClarity Administrator se ejecuta en un host hipervisor que se ejecuta en un servidor que gestiona, no utilice XClarity Administrator para actualizar el firmware en ese servidor. Cuando las actualizaciones de firmware se aplican con la activación inmediata, XClarity Administrator fuerza un reinicio del servidor de destino, lo que reinicia también el host hipervisor y XClarity Administrator. Cuando se aplica con la activación diferida, solo se aplica determinado firmware hasta que se reinicia el sistema de destino

Consideraciones acerca de CMM

- **Reubique virtualmente CMM antes de actualizar el firmware.**

  Si está actualizando CMM que están ejecutando el nivel de firmware con versión de la pila 1.3.2.1 2PET12K a 2PET12Q y estos han estado en ejecución durante más de tres semanas y se encuentran en una configuración de CMM dual, debe reubicar virtualmente el CMM principal y el CMM en espera antes de actualizar el firmware (consulte Reubicación virtual de un CMM).

Consideraciones del controlador de gestión de la placa base

- **Niveles mínimos de BMC necesarios para el estado de activación pendiente**

  Para ver el estado pendiente activación, la versión de firmware siguiente debe instalarse en el controlador de gestión de placa base principal en el servidor.
  - **IMM2**: TCOO46F, TCOO46E o una versión posterior (según la plataforma)
  - **XCC**: CDI328M, PSI316N, TEI334I o una versión posterior (según la plataforma)

- **Las actualizaciones aplicadas a las particiones principales de firmware del controlador de gestión y de la UEFI.**

  Las actualizaciones del controlador de gestión de la placa base (BMC) y de UEFI se pueden aplicar a las particiones principales y de copia de seguridad de firmware para el controlador de gestión y la UEFI de forma independiente.

También puede aplicar las actualizaciones del controlador de gestión y de la UEFI solo a las particiones principales en el servidor. De manera predeterminada, el controlador de gestión está configurado para sincronizar la partición de copia de seguridad del controlador de gestión con la partición principal del controlador de gestión, una vez que el controlador de gestión principal ha estado ejecutándose correctamente y el nuevo nivel está listo para promover la copia de seguridad. Sin embargo, el controlador de gestión no está configurado de manera predeterminada para sincronizar la partición de copia de seguridad de la UEFI. Por tanto, debe utilizar una de las siguientes opciones en el controlador de gestión:

– Habilitar la sincronización automática de la partición de seguridad de UEFI.

  De este modo se garantiza que tanto la partición principal como la de seguridad se ejecutan en el mismo nivel de firmware (y que el firmware de la UEFI es compatible con el firmware del controlador de gestión).

– Deshabilitar la sincronización automática de la partición de la copia de seguridad del controlador de gestión.

  Aunque no se recomienda, esto proporciona el control completo sobre los niveles de firmware del controlador de gestión y de la UEFI. Sin embargo, debe actualizar manualmente el firmware del controlador de gestión y de la UEFI en ambas particiones.

Las políticas de cumplimiento de firmware se utilizan para determinar qué actualizaciones se aplican a cada dispositivo. Para obtener más información sobre las políticas de conformidad de firmware, consulte Creación y asignación de políticas de cumplimiento de firmware.

Nota: Si el controlador de gestión y la UEFI se configuran para sincronizar automáticamente el firmware de copia de seguridad a partir del principal, XClarity Administrator no tiene que actualizar los bancos de copia de seguridad. Si esto ocurre, puede borrar las actualizaciones del banco de copia de seguridad al aplicar actualizaciones a un servidor, o bien quitar los bancos de copia de seguridad de la política de cumplimiento de firmware.

- **Cabe la posibilidad de que se produzca un error en el sistema de VMware vSphere ESXi (pantalla de diagnóstico del host en morado) al restablecer el controlador de gestión.**

  Si ejecuta VMware vSphere ESXi en cualquier servidor, asegúrese de que estén instalados los siguientes niveles mínimos de VMware ESXi antes de actualizar el firmware en el nodo de cálculo:

  – Si está ejecutando VMware vSphere ESXi 5.0, instale un nivel mínimo de 5.0u2 (actualización 2).
  – Si está ejecutando VMware vSphere ESXi 5.1, instale un nivel mínimo de 5.1u1 (actualización 1).

  Si no instala estos niveles mínimos, se puede producir un error del sistema de VMware vSphere ESXi (pantalla de diagnóstico morada de host) cuando se restablezca el controlador de gestión, incluso cuando se aplica y activa el firmware del controlador de gestión.

  Nota: Este problema no afecta a ESXi versión 5.5.

Consideraciones de dispositivo ThinkSystem

- **Para los servidores ThinkSystem SE350 que ejecutan una versión de firmware XCC anterior a 20A, el acceso de IPMI sobre KCS se debe habilitar manualmente en el controlador de gestión de la placa base para garantizar que el controlador de gestión se pueda comunicar con XClarity Administrator.**

  Para los servidores ThinkSystem SE350, IPMI sobre KCS está deshabilitado de manera predeterminada. Para los servidores ThinkSystem SE350 que ejecutan la versión 20A o posterior del firmware XCC, XClarity Administrator habilita automáticamente IPMI sobre KCS durante una actualización de firmware y luego lo deshabilita una vez que se completa la actualización de firmware. Sin embargo, para los servidores ThinkSystem SE350 que ejecutan una versión de firmware XCC anterior a 20A, debe habilitar

esta opción manualmente en la interfaz de usuario de Lenovo XClarity Controller. Para ello, haga clic en **Configuración de BMC → Seguridad → Acceso de IPMI sobre KCS**.

- Para los servidores ThinkSystem SR635 y SR655, se aplican las siguientes limitaciones.
  - Solo se admite la activación inmediata. La activación con retraso y la activación prioritaria no se admiten.
  - Para XClarity Administrator v3.1.1 y posterior, puede utilizar la función de actualización del paquete para actualizar todos los componentes de los servidores ThinkSystem SR635 y SR655, incluidos el controlador de gestión de la placa base, la UEFI, las unidades de disco y las opciones de E/S.

    Atención: Los dispositivos seleccionados se apagan antes de iniciar el proceso de actualización. Asegúrese de que todas las cargas de trabajo en ejecución se hayan detenido o, si está trabajando en un entorno virtualizado, se hayan desplazado a otro servidor. Si hay trabajos en ejecución, el trabajo de actualización queda en cola hasta que se completen todos los otros trabajos. Para ver una lista de los trabajos activos, pulse **Supervisión → Trabajos**.

    Notas:

    - La aplicación de actualizaciones de firmware del paquete solo es compatible con los servidores ThinkSystem SR635 y SR655.
    - La aplicación de actualizaciones de firmware del paquete solo es compatible con las direcciones IPv4. No se admiten las direcciones IPv6.
    - Asegúrese de que cada dispositivo de destino se haya arrancado en el SO al menos una vez para recuperar la información completa del inventario.
    - Se requiere el firmware v2.94 o posterior del controlador de gestión de la placa base para utilizar la función de actualización del paquete.
    - Solo se utilizan actualizaciones de firmware de paquetes de repositorios o actualizaciones de firmware individuales. No se admiten UpdateXpress System Packs (UXSPs).
    - Solo se aplican las actualizaciones de firmware descargadas. Actualice el catálogo de productos y descargue las actualizaciones de firmware adecuadas (consulte Actualización del catálogo de productos y Descarga de actualizaciones de firmware).

      Nota: Cuando XClarity Administrator se instala por primera vez, el catálogo de productos y el repositorio están vacíos.
    - La comprobación de conformidad solo es compatible con el controlador de gestión de la placa base y la UEFI en los servidores ThinkSystem SR635 y SR655; sin embargo, XClarity Administrator intenta aplicar actualizaciones de firmware a todos los componentes de hardware disponibles.
    - Las actualizaciones se aplican de acuerdo con la política de cumplimiento de firmware asignada. No puede optar por actualizar un subconjunto de componentes.
    - Se requiere XClarity Administrator v3.2 o posterior para aplicar actualizaciones de firmware para Lenovo XClarity Provisioning Manager (LXPM), controladores Windows LXPM o controladores Linux LXPM a servidores ThinkSystem SR635 y SR655.
    - Las actualizaciones del controlador de gestión de la placa base y de la UEFI se omiten si la versión instalada en el momento es mayor que la política de cumplimiento asignada.
    - Las políticas de cumplimiento de firmware se deben crear y asignar a los dispositivos en los que tenga previsto aplicar las actualizaciones de firmware. Para obtener más información, consulte el apartado Creación y asignación de políticas de cumplimiento de firmware.
    - Los dispositivos seleccionados se apagan antes de iniciar el proceso de actualización. Asegúrese de que todas las cargas de trabajo en ejecución se hayan detenido o, si está trabajando en un entorno virtualizado, se hayan desplazado a otro servidor.

También puede utilizar la función de actualización tradicional para aplicar las actualizaciones de hardware únicamente al controlador de gestión de la placa base y la UEFI.

  - Para XClarity Administrator v3.0:
    - Los datos de gestión no se actualizan correctamente al actualizar el firmware de 20A a 20B o 20C. Para solucionar este problema, anule la gestión y, a continuación, vuelva a gestionar el dispositivo, o bien reinicie XClarity Administrator.
    - No se admiten actualizaciones de firmware a versiones anteriores.

- **Las actualizaciones de firmware no se admiten en servidores ThinkSystem que utilizan DHCPv6 o direcciones IPv6 asignadas estáticamente**

  Al utilizar el direccionamiento IPv6 en servidores ThinkSystem, las actualizaciones de firmware solo se admiten en la dirección de vínculo local (LLA) IPv6 y las direcciones sin estado.

- **Al actualizar el firmware a la versión 20D, debe actualizar tanto UEFI como XCC juntos.**

  La UEFI y Lenovo XClarity Controller (XCC) deben actualizarse a la vez para la versión 20D. La actualización de XCC y no UEFI, y viceversa, causará problemas.

Consideraciones de dispositivo Flex System

- **Asegúrese de que los conmutadores Flex que se están actualizando estén encendidos,**
- **Seleccione la opción Activación inmediata al actualizar los nodos de cálculo que tengan niveles de firmware del controlador de gestión anteriores a Flex System 1.3.2.**

  Si aplica Flex System 1.3.2, versión del ciclo de vida del 2º trimestre, a un nodo de cálculo, debe elegir *Activación inmediata* para actualizar el nodo de cálculo. La activación inmediata fuerza el reinicio del nodo de cálculo durante el proceso de actualización.

- **Los Conmutadores Flex deben estar configurados con una dirección IP a la que se pueda acceder desde XClarity Administrator.**

  El Conmutador Flex de destino debe tener asignada una dirección IP que pueda comunicarse con XClarity Administrator, de forma que XClarity Administrator pueda descargar y aplicar la actualización de firmware.

- **Compatibilidad de actualizaciones en complejos escalables como los nodos x480 X6 y x880 X6.**

  La compatibilidad de actualización en nodos escalables, como los nodos de cálculo Flex System x480 X6 y x880 X6, está limitada a configuraciones en las que el complejo está configurado como una *única partición* que incluye todos los nodos de cálculo que forman parte del complejo de varios nodos. No puede utilizar XClarity Administrator para actualizar un complejo que conste de varias particiones.

  Si asigna una política de cumplimiento de firmware a una partición que incluye varios servidores en un complejo escalable (como nodos de cálculo Flex System x480 X6 y x880 X6), XClarity Administrator actualiza el firmware en todos los controladores de gestión y UEFI para cada servidor en la partición de forma predeterminada. Sin embargo, si selecciona un subconjunto de componentes dentro de la partición, XClarity Administrator actualiza el firmware únicamente en los componentes seleccionados en la partición.

- **Antes de actualizar el CMM2 a la versión 1.30 (1AON06C) o posterior, los conmutadores Flex deben estar ejecutando la versión nivel 3 de Enhanced Configuration and Management (EHCM L3)**

  CMM2 y los conmutadores Flex se comunican utilizando el protocolo EHCM. Este protocolo se requiere para que XClarity Administrator actualice los conmutadores Flex. Cuando actualiza un CMM2 a la versión 1.30 (1AON06C) o posterior, XClarity Administrator verifique que los conmutadores Flex estén ejecutando EHCM L3 y, de lo contrario, cancela la actualización de CMM con una advertencia que los conmutadores Flex primero se deben actualizar a una versión que soporte EHCM-L3. Puede invalidar esta verificación seleccionando **Intentar actualizar los componentes que ya cumplen los requisitos** al actualizar el firmware de CMM.

Atención: Actualmente no hay un versión de firmware para los conmutadores Flex System EN6131 Ethernet e IB6131 InfiniBand que admita EHCM L3. Esto significa que después de actualizar el CMM2 al firmware versión 1.30 (1AON06C) o posterior, ya no puede utilizar XClarity Administrator para actualizar esos conmutadores. La solución es utilizar la interfaz web del controlador de gestión o la interfaz de la línea de comandos del chasis para actualizar el conmutador.

Conmutador Flex System	Versión	Fecha de publicación
CN4093	7.8.4.0	Junio de 2014
EN4023	6.0.0	Abril de 2015
EN4093	7.8.4.0	Junio de 2014
EN4093R	7.8.4.0	Junio de 2014
EN6132	No disponible	No disponible
FC3171	9.1.3.02.00	Junio de 2014
FC5022	7.4.0b1	Marzo de 2016
IB6132	No disponible	No disponible
SI4091	7.8.4.0	Junio de 2014
SI4093	7.8.4.0	Junio de 2014

Nota: El conmutador escalable Ethernet EN2092 de 1 Gb no requiere EHCM L3 y no tiene esta restricción.

Consideraciones de almacenamiento

- **Consideraciones de los dispositivos de almacenamiento de DM ThinkSystem**

  Para actualizar el firmware en dispositivos de almacenamiento ThinkSystem DM, los dispositivos deben ejecutar v9.7 o posterior.

  La degradación solo es compatible con las versiones menores. Por ejemplo, puede degradar 9.7P11 a 9.7P9; sin embargo no se puede degradar de 9.8 a 9.7.

  Para descargar el firmware para los dispositivos de almacenamiento ThinkSystem serie DM:

  - Uno o varios dispositivos de almacenamiento de ThinkSystem serie DM se deben gestionar mediante XClarity Administrator.
  - Cada dispositivo de almacenamiento de ThinkSystem serie DM debe tener derecho al servicio y soporte de hardware.
  - Debe especificar el país donde están ubicados los dispositivos de almacenamiento de ThinkSystem serie DM en la página Actualizaciones de firmware: Repositorio. Solo se puede descargar firmware cifrado para dispositivos de los siguientes países: Armenia, Bielorrusia, China, Cuba, Irán, Kazajstán, Kirguizistán, Corea del Norte, Rusia, Sudán, Siria.
- **Las unidades de disco deben encontrarse en el estado JBOD, en línea, preparado o no configurado (bueno).**

  Para actualizar firmware en unidades de disco, el estado RAID debe encontrarse en el estado JBOD, en línea, preparado o no configurado (bueno). No se admiten otros estados. Para determinar el estado RAID de una unidad de disco, vaya a la página de inventario para el dispositivo, expanda la sección **Unidades** y compruebe la columna **Estado RAID** para esa unidad de disco (consulte Visualización de los detalles de un servidor gestionado).
- **La versión de firmware no se detecta para unidades de disco y unidades de estado sólido.**

XClarity Administrator detecta solo la versión de firmware instalada y realiza una comprobación de conformidad para unidades de disco y unidades de estado sólido (SSD) que están conectadas a un adaptador MegaRAID o un adaptador NVMe. Es posible que otras unidades conectadas tengan un nivel de firmware no compatible o que no admitan la notificación de la versión de firmware. No obstante, las actualizaciones de firmware se aplican a dichas unidades cuando se seleccionan.

- **El firmware NVMe se aplica aunque no esté identificado con un componente de destino**

  En la página Aplicar/Activar, se muestra la versión de firmware de NVMe para las unidades de estado sólido (SSD). Debido a que no se identifica ninguna actualización de firmware para los dispositivos NVMe descubiertos, se muestra un mensaje de advertencia cuando intente actualizar el sistema de destino. Sin embargo, la actualización de HDD/SSD se aplica incluso si no se identifica con un componente de destino, así que el firmware NVMe aún se actualiza.

- **La aplicación del paquete de actualización de ServeRAID M5115 PSoC3 desde XClarity Administrator requiere que se haya instalado como mínimo el nivel 68.**

  La actualización de ServeRAID M5115 PSoC3 (sistema en el chip programable) desde una versión anterior a la 68 se debe realizar de una forma controlada.

  Consejo: puede ver la versión del código de ServeRAID M5115 PSoC3 iniciando sesión en la interfaz web del CMM y seleccionando la pestaña **Firmware** correspondiente al nodo de cálculo de destino. A continuación, seleccione la tarjeta de expansión para el adaptador ServeRAID M5115. La versión del código de PSoc3 es el tipo de firmware GENÉRICO.

  Si la versión instalada es anterior a la 68, no es posible realizar la actualización utilizando XClarity Administrator. En su lugar, tiene que llevar a cabo los siguientes pasos desde la interfaz web del Chassis Management Module (CMM) o a través de la interfaz de la línea de comandos (CLI).

  – **Utilización de la interfaz web de CMM:**
    1. Inicie sesión en la interfaz web del Chassis Management Module (CMM).
    2. En el menú principal, haga clic en **Servicio y soporte → Avanzado**.
    3. Haga clic en la pestaña **Restablecer servicio**.
    4. Seleccione el nodo de cálculo adecuado pulsando su botón de selección.
    5. En la lista desplegable **Restablecer**, seleccione **Reubicación virtual**.
    6. Haga clic en **Aceptar** para confirmar.
  – **Utilización de CLI de CMM**:
    – Inicie sesión en la interfaz de shell seguro (SSH) del CMM.
    – Introduzca el siguiente comando para realizar una reubicación virtual:
      `'service -vr -T blade[x]`

      donde *x* es el número de bahía del nodo de cálculo que se va a reubicar.

  Una vez encendido de nuevo el sistema, arranque en el sistema operativo y actualice ServeRAID M5115 PSoC3 mediante el paquete de actualización integrado extraído. Lleve a cabo los siguientes pasos para extraer el paquete integrado.

  – **Uso de Microsoft Windows:**

    Abra el paquete de actualización (lnvgy_fw_psoc3_m5115-70_windows_32-64.exe) y, a continuación, seleccione Extraer en el disco duro. A continuación, seleccione la ruta en la que se extraerá el paquete integrado.
  – **Uso de Linux:**

    Ejecute el siguiente comando:

    `lnvgy_fw_psoc3_m5115-70_linux_32-64.bin -x`

donde *x* es la ubicación en la que debe extraerse el paquete integrado.

Gestión del repositorio de actualizaciones de firmware

El *repositorio de actualizaciones de firmware* contiene un catálogo de las actualizaciones disponibles y los paquetes de actualización que se pueden aplicar a los dispositivos gestionados.

Acerca de esta tarea

El *catálogo* contiene información acerca de las actualizaciones de firmware que se encuentran disponibles en la actualidad para todos los dispositivos compatibles con XClarity Administrator. El catálogo organiza las actualizaciones de firmware por tipo de dispositivo. Cuando actualiza el catálogo, XClarity Administrator recupera información acerca de las últimas actualizaciones de firmware disponibles en el sitio web de Lenovo (incluidos los archivos metadata.xml o .json y readme.txt) y almacena la información en el repositorio de actualizaciones de firmware. No se descarga el archivo de carga útil (.exe). Para obtener más información sobre actualizar el catálogo, consulte Actualización del catálogo de productos.

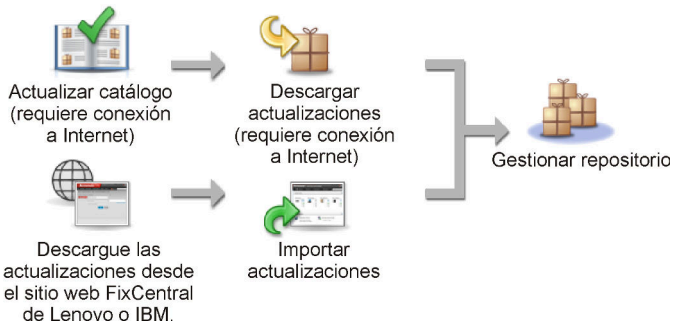
Si hay nuevas actualizaciones de firmware disponibles, debe descargar los paquetes de actualización antes de poder actualizar dicho firmware en los dispositivos gestionados. La actualización del catálogo no descarga automáticamente los paquetes de actualizaciones. La tabla de **Catálogo de productos** en la página del Repositorio de actualizaciones de firmware identifica qué paquetes de actualización se descargan y cuáles están disponibles para descargarse.

Puede descargar las actualizaciones de firmware de varias maneras distintas:

- **Paquetes del repositorio de actualizaciones de firmware**. Los paquetes de repositorio contienen las más recientes actualizaciones de firmware disponibles para todos los dispositivos admitidos y una política de cumplimiento de firmware actualizada predeterminada. Estos paquetes del repositorio se importan y luego se aplican desde la página Actualizar servidor de gestión.
- **UpdateXpress System Packs (UXSP)**. UXSP contiene las últimas actualizaciones de firmware y controlador de dispositivo disponibles, organizadas por sistema operativo. Cuando descarga UXSP en la página Actualizaciones de firmware: Repositorio, solo se descargan las actualizaciones de firmware y se almacenan en el repositorio. Se excluyen actualizaciones del controlador de dispositivo.

  Nota: Para los servidores con XCC2, estos paquetes se conocen como *paquetes* de firmware.
- **Actualizaciones de firmware individuales**. Puede descargar paquetes de actualización de firmware individuales, uno a la vez, según la versión que aparece en el catálogo.

XClarity Administrator debe estar conectado a Internet para actualizar el catálogo y descargar las actualizaciones de firmware. Si no está conectado a Internet, puede descargar manualmente los archivos en una estación de trabajo que tenga acceso de red al host de XClarity Administrator utilizando un navegador web y luego importar los archivos al repositorio de actualizaciones de firmware.



Cuando importa manualmente las actualizaciones de firmware en XClarity Administrator, debe incluir los siguientes archivos obligatorios: carga útil (imagen y MIB), metadatos, historial de cambios y archivo léame. Por ejemplo:
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.tgz
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.xml
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.chg
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.txt

Atención:

- Solo importe estos archivos necesarios. No importe otros archivos que puedan encontrarse en los sitios web de descarga de firmware.
- Si no incluye el archivo XML en el paquete de actualizaciones, la actualización no se importa.
- Si no incluye todos los archivos requeridos que están asociados a la actualización, el repositorio muestra que la actualización no se descarga, lo que significa que se importa parcialmente. Posteriormente, puede incorporar los archivos que falten seleccionándolos e importándolos.
- Las actualizaciones de firmware principales (como el controlador de gestión, UEFI y pDSA) no dependen del sistema operativo. Los paquetes de actualización de firmware para los sistemas operativos RHEL 6 o SLES 11 se utilizan para actualizar nodos de cálculo y servidores de bastidor. Para obtener más información acerca de los paquetes de actualización de firmware que deben utilizarse para sus servidores gestionados, consulte Descarga de actualizaciones de firmware.

Después de que se descarguen los paquetes en el repositorio, se entrega información sobre cada actualización, incluida la fecha, tamaño, uso de política y gravedad de la versión. La gravedad indica el impacto y la necesidad de aplicar la actualización para ayudarle a evaluar en qué se puede ver afectado su entorno.
- **Versión inicial**. Esta es la primera versión del firmware.
- **Crítico**. La versión de firmware contiene arreglos urgentes para la corrupción de datos, la seguridad o el problema de estabilidad.
- **Sugerido**. La versión del firmware contiene arreglos importantes para problemas que posiblemente encuentre.
- **No crítico**. La versión del firmware contiene arreglos menores, mejoras de rendimiento y cambios textuales.

Notas:

- La gravedad es relativa a la versión anterior de la actualización. Por ejemplo, si el firmware instalado es v1.01 y la actualización v1.02 es crítica y se recomienda la actualización v1.03, esto significa que se recomienda la actualización desde 1.02 a 1.03, pero que la actualización de v1.01 a v1.03 es crítica porque es acumulativa (v1.03 incluye problemas críticos de v1.02).
- Pueden surgir casos especiales en los que una actualización puede ser únicamente crítica o recomendada para un tipo de equipo o sistema operativo específico. Para obtener más información, consulte las Notas de la versión.

Procedimiento

Para ver las actualizaciones de firmware que están disponibles en el catálogo de productos, lleve a cabo los pasos siguientes.

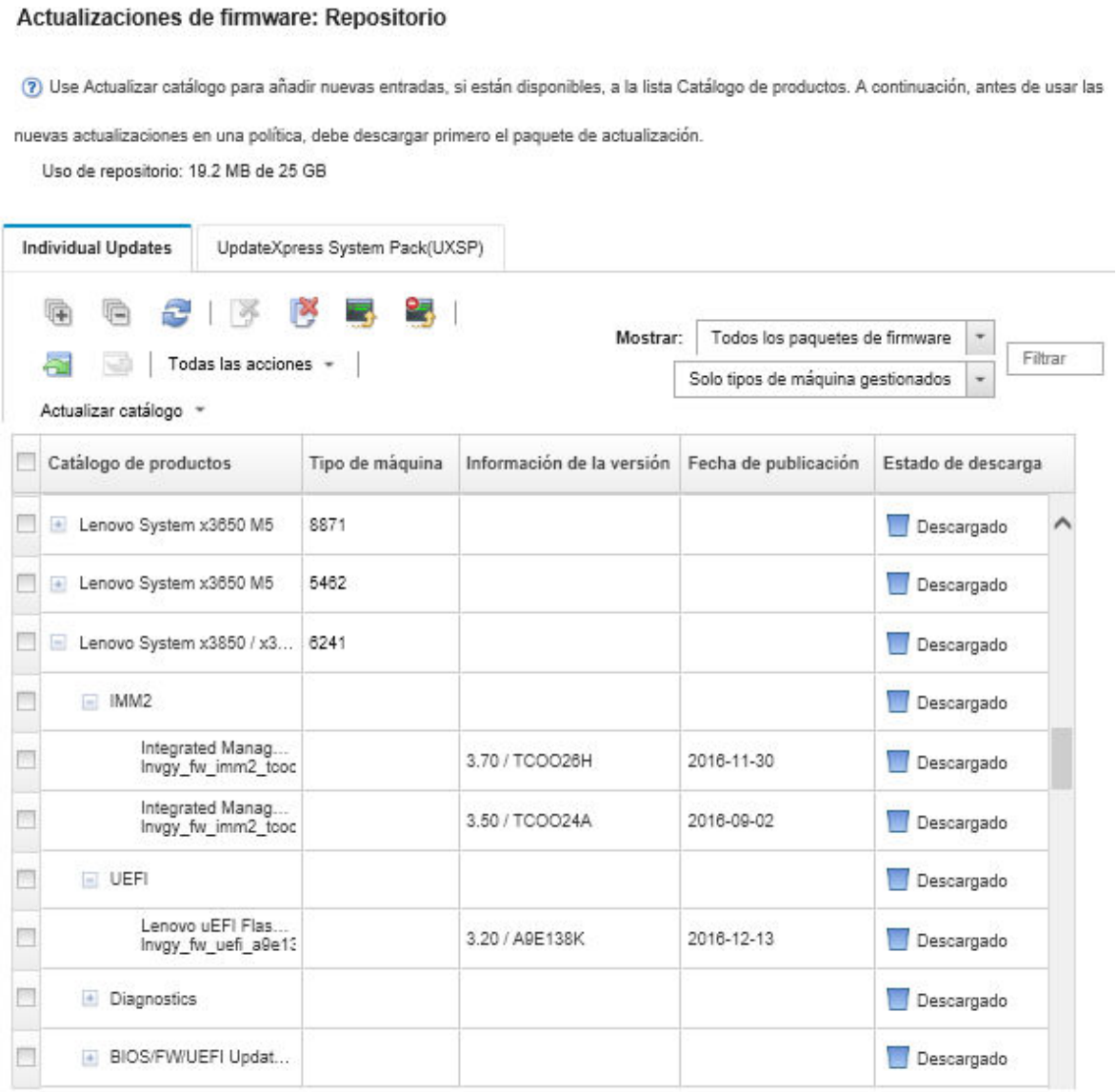
Paso 1. En la barra de menús de XClarity Administrator , haga clic en **Aprovisionamiento → Repositorio**. Se muestra la página Repositorio de actualizaciones de firmware con una lista de los paquetes de actualización de firmware disponibles, organizados por tipo de dispositivo.

Paso 2. Haga clic en la pestaña **Actualizaciones individuales** para ver información acerca de los paquetes de actualización de firmware disponibles, o bien haga clic en la pestaña **UpdateXpress System Packs (UXSP)** para ver información sobre los UXSP disponibles.

Paso 3. Expanda un dispositivo y sus componentes para ver la lista de paquetes de actualización y de actualizaciones de firmware para dicho dispositivo.

Puede ordenar las columnas de la tabla y hacer clic en el icono **Expandir todo** ( ) y el icono **Contraer todo** ( ) para facilitar la búsqueda de actualizaciones de firmware específicas. Además, puede filtrar la lista de actualizaciones de dispositivos y firmware que se muestran al seleccionar una opción en el menú **Mostrar** de modo que se enumeren solo las actualizaciones de firmware de una específica edad, las actualizaciones de firmware para todos los tipos de servidor o solo aquellos de tipo servidor gestionado o aquello que se ingrese como texto en el campo **Filtro**. Tenga en cuenta que si busca dispositivos específicos, solo se muestran los dispositivos; las actualizaciones de firmware no se muestran en el nombre del dispositivo.

Nota: Para los servidores, hay disponibles paquetes de actualizaciones específicos en función del tipo de servidor. Por ejemplo, si expande un servidor, como Nodo de cálculo Flex System x240, se muestran los paquetes de actualizaciones que están disponibles específicamente para ese nodo de cálculo.



Resultados

Desde esta página puede llevar a cabo las siguientes acciones:

- Para actualizar esta página con la información más reciente de las actualizaciones de firmware del catálogo, haga clic en el icono **Actualizar** ().
- Para recuperar la información más reciente sobre las actualizaciones disponibles, haga clic en **Actualizar catálogo**.La recuperación de esta información puede tardar varios minutos. Para obtener más información, consulte el apartado Actualización del catálogo de productos.
- Para agregar las actualizaciones de firmware al repositorio, seleccione uno o varios paquetes de actualización del catálogo de productos y, a continuación, haga clic en el icono **Descargar** (). Cuando las actualizaciones de firmware se hayan descargado y agregado al repositorio, el estado cambia a "Descargado."

  Nota: XClarity Administrator debe estar conectado a Internet para adquirir actualizaciones a través de la interfaz de usuario de XClarity Administrator. Si no está conectado a Internet, podrá importar las actualizaciones que haya descargado previamente.

  Para obtener más información sobre cómo descargar actualizaciones, consulte Descarga de actualizaciones de firmware.
- Para importar las actualizaciones de firmware que ha descargado manualmente a una estación que tenga acceso de red a XClarity Administrator, seleccione una o varias actualizaciones y, a continuación, haga clic en el icono **Importar** ().Para obtener más información sobre cómo importar actualizaciones, consulte Descarga de actualizaciones de firmware.
- Para detener las descargas que actualmente están en curso, seleccione uno o varios paquetes de actualización y, a continuación, haga clic en el icono **Cancelar descargas** ().Al cancelar las descargas, se cancelan *todas* las descargas de firmware que están en curso. Puede supervisar el progreso detallado de y detener una descarga específica de firmware desde el registro de trabajos (consulte Supervisión de trabajos).
- Eliminar paquetes de actualización o actualizaciones individuales desde el repositorio (consulte Eliminación de actualizaciones de firmware).
- Exporte actualizaciones de firmware que existen en el repositorio de actualizaciones de firmware a un sistema local (consulte Exportación e importación de actualizaciones de firmware).

Uso de un repositorio remoto para actualizaciones de firmware

De forma predeterminada, Lenovo XClarity Administrator utiliza un repositorio local (interno) para almacenar actualizaciones de firmware. Puede liberar espacio en el disco que está disponible para el repositorio local de XClarity Administrator usando una unidad compartida remota sobre sistema de archivos SSH (SSHFS) montada como repositorio remoto. A continuación, puede utilizar los archivos de actualización de firmware directamente desde el repositorio remoto para mantener el cumplimiento del firmware en sus dispositivos.

Antes de empezar

Solo las actualizaciones de firmware pueden almacenarse en la carpeta remota. Los controladores de dispositivos y las actualizaciones de XClarity Administrator solo se pueden almacenar en el repositorio de actualizaciones local.

Asegúrese de que el servicio SFTP del puerto 22 esté abierto en el servidor de uso compartido remoto. Los controladores de gestión de la placa base deben tener acceso a este puerto.

La unidad compartida remota se utiliza como servidor SFTP cuando se utiliza como repositorio de firmware. Asegúrese de no deshabilitar SFTP al actualizar la configuración de SSHD.

Acerca de esta tarea

Cuando cambie la ubicación de repositorio de actualizaciones de firmware, puede elegir copiar todas las actualizaciones de firmware desde el repositorio original en el nuevo repositorio.

Los archivos de actualización de firmware del repositorio original *no* se limpian automáticamente después de cambiar de ubicación.

Si XClarity Administrator tiene permisos de lectura/escritura en el repositorio remoto, el comportamiento es el mismo que al usar el repositorio local. No obstante, si XClarity Administrator dispone de permisos de solo lectura, no podrá actualizar el catálogo ni descargar o importar actualizaciones al repositorio.

El mismo repositorio remoto puede compartirse con varias instancias de XClarity Administrator; sin embargo, si una instancia de XClarity Administrator cambia el repositorio, las otras instancias de XClarity Administrator no se notifican automáticamente. Debe actualizar el repositorio para obtener los detalles más recientes. Para actualizar el repositorio, haga clic en **Todas las acciones → Actualizar repositorio** desde la página Actualizaciones de firmware: Repositorio.

Nota: Tenga cuidado al eliminar actualizaciones de firmware y UXSP si el repositorio de actualizaciones de firmware se encuentra en una carpeta compartida remota que se encuentra en varias instancias de XClarity Administrator.

Procedimiento

Para usar un repositorio de actualizaciones de firmware remoto, complete los siguientes pasos.

Paso 1. Añada una acción compartido remota XClarity Administrator (consulte Gestión de remote shares).

Paso 2. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Actualizaciones de firmware: Repositorio** . Se muestra la página del repositorio de actualizaciones de firmware.

Paso 3. Haga clic en **Todas las acciones → Cambiar ubicación de repositorio** para mostrar el cuadro de diálogo Ubicación de repositorio de intercambio.

Paso 4. Seleccione la carpeta compartida remota que acaba de crear en la lista desplegable **Ubicación de repositorio**.

Paso 5. Opcionalmente, seleccione **Limpieza del repositorio actual** para eliminar los archivos de actualización de firmware de la ubicación actual del repositorio.

Paso 6. Opcionalmente, seleccione **Copiar paquetes de actualización desde el repositorio actual en el nuevo repositorio** para copiar los archivos de actualización de firmware en la nueva ubicación de repositorio antes de cambiar la ubicación de repositorio.

De forma predeterminada, los archivos de actualización de firmware que existen en la nueva ubicación no se copian (se omiten). Opcionalmente, puede optar por sobrescribir cualquier archivo existente o sobrescribir únicamente el archivo existente con un tamaño diferente o la fecha de modificación en la lista desplegable **Sobrescribir reglas**.

Paso 7. Haga clic en **Aceptar**.

Se crea un trabajo para copiar los paquetes de actualización de firmware en el nuevo repositorio. Puede supervisar el progreso del trabajo haciendo clic en **Supervisión → Trabajos** en la barra de menús de XClarity Administrator.

Actualización del catálogo de productos

El catálogo de productos contiene información acerca de las actualizaciones de firmware que están disponibles para todos los dispositivos admitidos por Lenovo XClarity Administrator, incluidos los chasis, los servidores y Conmutadores Flex.

Antes de empezar

Se requiere una conexión a Internet para actualizar el catálogo de productos.

La actualización del catálogo puede tardar varios minutos en finalizar.

Acerca de esta tarea

Cuando actualiza el catálogo, XClarity Administrator recupera información sobre las últimas actualizaciones de firmware disponibles desde Sitio web de soporte de Lenovo XClarity y almacena la información en el repositorio de actualizaciones de firmware.

La actualización del catálogo solo agrega al repositorio información sobre las actualizaciones de firmware disponibles. No descarga los paquetes de actualización. Debe descargar las actualizaciones de firmware para que las actualizaciones estén disponibles para la instalación. Para obtener más información sobre cómo descargar actualizaciones, consulte Descarga de actualizaciones de firmware.

Procedimiento

Para actualizar el catálogo de productos, lleve a cabo los pasos siguientes.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Actualizaciones de firmware: Repositorio** . Se muestra la página Repositorio de actualizaciones de firmware.

Paso 2. Haga clic en la pestaña **Actualizaciones individuales** para obtener información acerca de los paquetes de actualización de firmware individuales, o bien haga clic en la pestaña **UpdateXpress System Pack (UXSP)** para ver información sobre los UXSP disponibles.

Paso 3. Haga clic en **Actualizar catálogo** y, a continuación, haga clic en una de las siguientes opciones para obtener información sobre las últimas actualizaciones de firmware disponibles.

- **Actualizar selección - Solo reciente**. Permite recuperar información acerca de la versión más actual de las actualizaciones de firmware que están disponibles solo para los dispositivos seleccionados.
- **Actualizar todo - Solo reciente**. Permite recuperar información acerca de la versión más reciente de todas las actualizaciones de firmware para todos los dispositivos compatibles.
- **Actualizar selección**. Permite recuperar información acerca de todas las versiones de actualizaciones de firmware que están disponibles solo para los dispositivos seleccionados.
- **Actualizar todo**. Permite recuperar información acerca de todas las versiones de todas las actualizaciones de firmware que están disponibles para todos los dispositivos compatibles.

Consejo: puede actualizar el catálogo de productos y descargar el firmware más reciente en un solo paso haciendo clic en **Todas las acciones → actualizar y descargar la versión más reciente de todos los dispositivos gestionados** o **Todas las acciones → Actualizar y descargar la versión más reciente para los dispositivos seleccionados**.

Descarga de actualizaciones de firmware

Puede descargar o importar actualizaciones de firmware en el repositorio de actualizaciones de firmware, dependiendo de su acceso a Internet. Las actualizaciones de firmware deben estar disponibles en el repositorio de actualizaciones de firmware antes de poder actualizar el firmware en dispositivos de gestión.

Antes de empezar

Asegúrese de que todos los puertos y direcciones de Internet requeridos por Lenovo XClarity Administrator estén disponibles antes de intentar descargar firmware. Para obtener más información acerca de los puertos, consulte Disponibilidad de puertos y Firewall y servidores proxy en la documentación en línea de XClarity Administrator.

Si un tipo de dispositivo no aparece en el repositorio de actualizaciones de firmware, debe gestionar un dispositivo de ese tipo antes de descargar o importar actualizaciones de firmware individuales para dicho tipo de dispositivo.

Importante:

- Para XClarity Administrator v1.1.1 y anterior, debe descargar manualmente e importar las actualizaciones de firmware para el hardware de Lenovo desde Sitio web del Soporte del Centro de Datos de Lenovo.
- XClarity Administrator no puede descargar actualizaciones para los conmutadores RackSwitch y los dispositivos Lenovo Storage serie DE, DX y SS desde el sitio web de Lenovo al repositorio de actualizaciones de firmware; en su lugar, debe descargar e importar estas actualizaciones desde el sitio web de Lenovo a una estación de trabajo que tenga acceso de red al host de XClarity Administrator, o descargar y aplicar manualmente los *paquetes del repositorio de actualización de firmware*, que contienen todas las actualizaciones de firmware disponibles.
- Los navegadores web Internet Explorer y Microsoft Edge tienen un límite de carga de 4 GB. Si el archivo que desea importar es mayor a 4 GB, considere usar otro navegador web (por ejemplo, Chrome o Firefox).
- Para descargar el firmware para los dispositivos de almacenamiento ThinkSystem serie DM:
  - Uno o varios dispositivos de almacenamiento de ThinkSystem serie DM se deben gestionar mediante XClarity Administrator.
  - Cada dispositivo de almacenamiento de ThinkSystem serie DM debe tener derecho al servicio y soporte de hardware.
  - Debe especificar el país donde están ubicados los dispositivos de almacenamiento de ThinkSystem serie DM en la página Actualizaciones de firmware: Repositorio. Solo se puede descargar firmware cifrado para dispositivos de los siguientes países: Armenia, Bielorrusia, China, Cuba, Irán, Kazajstán, Kirguizistán, Corea del Norte, Rusia, Sudán, Siria.

Acerca de esta tarea

Puede descargar las actualizaciones de firmware de varias maneras distintas:

- **Paquetes del repositorio de actualizaciones de firmware**

  Los paquetes del repositorio de actualización de firmware son colecciones de las actualizaciones de firmware más recientes que están disponibles al mismo tiempo que la versión XClarity Administrator para la mayoría de los dispositivos compatibles y una política de cumplimiento de firmware actualizada predeterminada. Estos paquetes del repositorio se importan y luego se aplican desde la página Actualizar servidor de gestión. Cuando aplica un paquete del repositorio de actualización de firmware, cada paquete de actualización del paquete se agrega en el repositorio de actualizaciones de firmware y una política de cumplimiento de firmware predeterminada se crea automáticamente para todos los dispositivos gestionables. También puede copiar esta política predefinida, pero no se puede cambiar.

Los siguientes paquetes de repositorio están disponibles.

- **lnvgy_sw_lxca_cmmswitchrepo***x-x.x.x*_**anyos_noarch**. Contiene las actualizaciones de firmware para todos los CMM y conmutadores Flex System.
- **lnvgy_sw_lxca_storagerackswitchrepo***x-x.x.x*_**anyos_noarch**. Contiene las actualizaciones de firmware para todos los conmutadores RackSwitch y dispositivos Lenovo Storage.
- **lnvgy_sw_lxca_systemxrepo***x-x.x.x*_**anyos_noarch**. Contiene las actualizaciones de firmware para todos los servidores serie Converged HX, Flex System, NeXtScale y System x.
- **lnvgy_sw_thinksystemrepo***x-x.x.x*_**anyos_noarch**. Contiene actualizaciones de firmware para todos los servidores ThinkAgile y ThinkSystem.
- **lnvgy_sw_lxca_thinksystemv2repo***x-x.x.x*_**anyos_noarch**. Contiene actualizaciones de firmware para todos los servidores ThinkAgile y ThinkSystem V2.
- **lnvgy_sw_lxca_thinksystemv3repo***x-x.x.x*_**anyos_noarch**. Contiene actualizaciones de firmware para todos los servidores ThinkAgile y ThinkSystem V3.

Puede determinar si los paquetes del repositorio de actualizaciones de firmware deben almacenarse en el repositorio desde la columna **Estado de descarga** de la página Actualizar servidor de gestión. Esta columna contiene los siguientes valores:

- **Descargado**. El paquete del repositorio de actualizaciones de firmware se almacena en el repositorio.
- **No descargado**. El paquete del repositorio de actualizaciones de firmware está disponible, pero no se almacena en el repositorio.

- **UpdateXpress System Packs (UXSPs)**

  Nota: Para los servidores con XCC2, estos paquetes se conocen como paquetes de firmware. El *paquete* se utiliza en los nombres de los paquetes y en los nombres de las políticas predefinidas.

  UXSP contiene las últimas actualizaciones de firmware y controlador de dispositivo disponibles, organizadas por sistema operativo. Cuando descargue UXSP, XClarity Administrator descarga el UXSP en función de la versión enumerada en el catálogo y almacena los paquetes de actualizaciones en el repositorio de actualizaciones de firmware. Cuando descarga un UXSP, cada actualización de firmware del UXSP se añade al repositorio de actualizaciones de firmware y se enumera en la pestaña **Actualizaciones individuales**, y se crea automáticamente una política de cumplimiento de firmware predeterminada para todos los dispositivos gestionables que utilizan los nombres siguientes. También puede copiar esta política predefinida, pero no se puede cambiar.
  - *{uxsp-version}-{date}-{server-short-name}***-UXSP** (por ejemplo, `v1.50-2017-11-22- SD530-UXSP`)
  - *{uxsp-version}-{buildnumber}-{server-short-name}***-bundle** (por ejemplo, `22a.0-kaj92va-SR650V3-bundle`)

  Nota: Cuando descarga o importa UXSP desde la página Actualizaciones de firmware: Repositorio, solo se descargan las actualizaciones de firmware y se almacenan en el repositorio. Se descartan actualizaciones del controlador de dispositivo. Para obtener información acerca de cómo descargar o importar actualizaciones de controladores de dispositivos de Windows mediante UXSP, consulte Gestión del repositorio de controladores de dispositivos del SO.

  Puede determinar si los UXSP están almacenados en el repositorio de actualizaciones de firmware desde la columna **Estado de descarga** en la pestaña **Actualizaciones individuales** en la página Actualizaciones de firmware: Repositorio. Esta columna contiene los siguientes valores:

  - **Descargado**. El paquete de actualizaciones completo o cada actualización de firmware se almacenan en el repositorio.
  - *x* **de** *y* **descargado**. Algunas de las actualizaciones de firmware del paquete de actualización se almacenan en el repositorio, pero no todas. Los números entre paréntesis indican el número de

actualizaciones disponibles y el número de actualizaciones almacenadas, o no hay actualizaciones para el tipo de dispositivo específico.

– **No descargado**. El paquete de actualización completo o la actualización de firmware individual no se almacenan en el repositorio.

- **Actualizaciones de firmware individuales**

  Puede descargar paquetes de actualización de firmware individuales, uno detrás de otro. Cuando descargue paquetes de actualización de firmware, XClarity Administrator descarga la actualización en función de la versión enumerada en el catálogo y almacena los paquetes de actualizaciones en el repositorio de actualizaciones de firmware. A continuación, puede crear políticas de cumplimiento de firmware utilizando dichos paquetes de actualización para cada uno de sus dispositivos gestionados.

  Nota: Las actualizaciones de firmware principales (como el controlador de gestión, UEFI y pDSA) no dependen del sistema operativo. Los paquetes de actualización de firmware para los sistemas operativos RHEL 6 o SLES 11 se utilizan para actualizar nodos de cálculo y servidores de bastidor. Para obtener más información acerca de los paquetes de actualización de firmware que deben utilizarse para sus servidores gestionados, consulte Descarga de actualizaciones de firmware.

  Puede determinar si hay *actualizaciones de firmware* específicas almacenadas en el repositorio de actualizaciones de firmware desde la columna **Estado de descarga** en la pestaña **Actualizaciones individuales** en la página Actualizaciones de firmware: Repositorio. Esta columna contiene los siguientes valores.

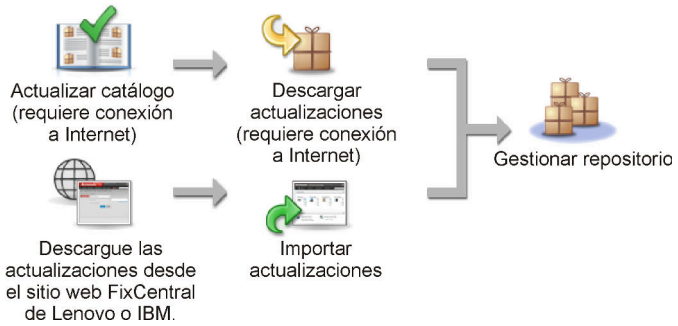
  – **Descargado**. El paquete de actualizaciones completo o cada actualización de firmware se almacenan en el repositorio.

  – *x* **de** *y* **descargado**. Algunas de las actualizaciones de firmware del paquete de actualización se almacenan en el repositorio, pero no todas. Los números entre paréntesis indican el número de actualizaciones disponibles y el número de actualizaciones almacenadas, o no hay actualizaciones para el tipo de dispositivo específico.

  – **No descargado**. El paquete de actualización completo o la actualización de firmware individual no se almacenan en el repositorio.

Cuando instala XClarity Administrator o actualiza a una nueva versión, se recomienda descargar el paquete de repositorio más reciente para asegurarse de que cuenta con las actualizaciones de firmware más recientes. Luego puede programar un trabajo recurrente para actualizar el catálogo con el fin de buscar las actualizaciones individuales que se publicaron en la web desde el último paquete del repositorio y luego descargar las actualizaciones electrónicamente, una a la vez.

XClarity Administrator debe estar conectado a Internet para actualizar el catálogo y descargar las actualizaciones de firmware. Si no está conectado a Internet, puede descargar manualmente los archivos en una estación de trabajo que tenga acceso de red al host de XClarity Administrator utilizando un navegador web y luego importar los archivos al repositorio de actualizaciones de firmware.



Cuando importa manualmente las actualizaciones de firmware en XClarity Administrator, debe incluir los siguientes archivos obligatorios: carga útil (imagen y MIB), metadatos, historial de cambios y archivo léame. Por ejemplo:

- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.tgz
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.xml
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.chg
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.txt

Nota: Las actualizaciones de firmware principales (como el controlador de gestión, UEFI y pDSA) no dependen del sistema operativo. Los paquetes de actualización de firmware para los sistemas operativos RHEL 6 o SLES 11 se utilizan para actualizar nodos de cálculo y servidores de bastidor.

Se muestra un mensaje en la página cuando la capacidad de uso del repositorio está sobre el 50 por ciento. Se muestra otro mensaje en la página cuando la capacidad de uso del repositorio está sobre el 85 por ciento. Para reducir el espacio utilizado en el repositorio, puede eliminar los archivos de imágenes y las políticas no utilizados. Puede eliminar políticas de cumplimiento de firmware no utilizadas y los paquetes de firmware asociados, haciendo clic en **Aprovisionamiento → Políticas de cumplimiento**, seleccionando una o más políticas que desee eliminar y luego haciendo clic en **Acciones → Eliminar cualquier política y paquete de firmware**.

En la tabla siguiente se resumen las diferencias entre adquirir paquetes del repositorio de actualizaciones de firmware, UXSPs y paquetes de actualización de firmware individuales.

Paquete de actualización	Página de la interfaz de usuario (IU) para descargar e importar archivos	Página web para descargar archivos manualmente	¿Se ha actualizado el repositorio de actualiza-ciones de firmware?	¿Se ha actualizado la política de cumplimiento de firmware de forma automática?
Paquetes del repositorio de actualizaciones de firmware	Página Actualizar servidor de gestión **Nota:** Debe importar y luego aplicar el paquete del repositorio.	Página web de descarga de XClarity Administrator	Sí	Sí
UpdateXpress System Packs	Actualizaciones de firmware: página de repositorio, pestaña **UpdateXpress System Packs (UXSPs)**	Página web de Lenovo XClarity Essentials UpdateXpress	Sí	Sí
Actualizaciones de firmware	Actualizaciones de firmware: página Repositorio, pestaña **Actualizaciones individuales**	Sitio web del Soporte del Centro de Datos de Lenovo **Notas:** Utilice Sitio web de Fix Central para los dispositivos siguientes: • Flex System x220 tipo 2585, 7906 • Flex System x222 Compute Nod tipo 2589, 7916 • Flex System x240 tipo 7863, 8737, 8738, 8956 • Flex System x280 / x480 / x880 X6 tipo 4259, 7903 • Flex System x440 tipo 2584, 7917	Sí	No

Procedimiento

Para descargar una o varias actualizaciones de firmware, lleve a cabo los pasos siguientes.

- Para importar uno o varios *paquetes del repositorio de actualizaciones de firmware*:
  1. En la barra de menús de XClarity Administrator, haga clic en **Administración → Actualizar servidor de gestión** para mostrar la página Actualización del servidor de gestión.
  2. Descargue los paquetes del repositorio más recientes:
     - Si XClarity Administrator está conectado a Internet:
       a. Para recuperar información acerca de las actualizaciones más recientes, haga clic en **Actualizar catálogo → Actualizar todos los gestionados: solo los más recientes**. Las nuevas actualizaciones del servidor de gestión y los paquetes del repositorio de actualizaciones de firmware se incluyen en la tabla de la página “Actualización del servidor de gestión”.

          La actualización del repositorio puede tardar varios minutos en finalizar.

Nota: La actualización del repositorio no descarga automáticamente los archivo de carga útil. Solo se descargan los metadatos y los archivos léame.

b. Seleccione los paquetes del repositorio de actualizaciones de firmware que desee descargar.

Consejo: Asegúrese de que los paquetes que seleccione muestran “Paquete suplementario” en la columna **Tipo**.

c. Haga clic en el icono **Descargar selección** (). Cuando la descarga se haya completado, el área **Estado de descarga** de dicha actualización de software cambia a “Descargado”.

– Si XClarity Administrator no está conectado a Internet:

a. Descargue los paquetes del repositorio de actualizaciones de firmware desde la Página web de descarga de XClarity Administrator en una estación de trabajo que tenga conexión de red con el host de XClarity Administrator.

b. En la página Actualización del servidor de gestión, haga clic en el icono **Importar** ().

c. Haga clic en **Seleccionar archivos** y desplácese hasta la ubicación de los paquetes del repositorio de actualizaciones de firmware en la estación de trabajo.

d. Seleccione todos los archivos del paquete y, a continuación, haga clic en **Abrir**.

Debe importar el archivo de metadatos (.xml o .json), así como la imagen o el archivo de carga útil (.zip, .bin, .uxz, o .tgz), el archivo de historial de cambios (.chg) y el archivo léame (.txt) para la actualización. Todos los archivos seleccionados, pero no especificados en el archivo de metadatos, se descartan. Si no incluye el archivo de metadatos, la actualización no se importa.

e. Haga clic en **Importar**.

Una vez completada la importación, los paquetes del repositorio de actualizaciones de firmware se muestras en la tabla de la página Actualización del servidor de gestión y en el área **Estado de descarga** de dicha actualización aparece “Descargado”.

3. Seleccione los paquetes del repositorio de actualizaciones de firmware que desee instalar en el repositorio de actualizaciones de firmware.

Nota: Asegúrese de que en el área **Estado de descarga** se muestre “Descargado” y de que en el área **Tipo** se muestre “Parche”.

4. Haga clic en el icono **Realizar actualización** () y agregue los paquetes de actualización de firmware al repositorio.
5. Espere unos minutos para que finalice la actualización y XClarity Administrator se reinicie.
6. Para determinar si la actualización ha finalizado, actualice el navegador web.

Una vez completada la operación, aparece la página Actualización del servidor de gestión, mientras que la columna **Estado aplicado** cambia a “Aplicado”.

7. Borre la caché del navegador web.

- Para descargar uno o más *UXSP*.

1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Actualizaciones de firmware: Repositorio** para mostrar la página Repositorio de actualizaciones de firmware.
2. Haga clic en la pestaña **UpdateXpress System Packs (UXSP)**.
3. Descargue los últimos UXSP:

– Si XClarity Administrator está conectado a Internet:

Para actualizar el catálogo y descargar la versión más reciente de UXSP para todos los dispositivos gestionados, haga clic en **Todas las acciones → Actualizar y descargar la versión más reciente de todos los dispositivos gestionados**.

Para actualizar el catálogo y descargar la versión más reciente de UXSP, solo para los dispositivos seleccionados:

a. Expanda el dispositivo para mostrar la lista de actualizaciones de UXSP.

b. Seleccione uno o más UXSP que desee descargar.

c. Haga clic en **Todas las acciones → Actualizar y descargar la versión más reciente para los dispositivos seleccionados**.

Una vez completada la descarga, el área **Estado de descarga** para los UXSP cambia a "Descargado."

– Si XClarity Administrator no está conectado a Internet:

a. Descargue los UXSP desde Página web de Lenovo XClarity Essentials UpdateXpress en una estación de trabajo que tenga conexión de red con el host de XClarity Administrator.

b. Desde XClarity Administrator, haga clic en el icono **Importar** ().

c. Haga clic en **Seleccionar archivos** y desplácese hasta la ubicación del UXSP en la estación de trabajo.

d. Seleccione todos los archivos del paquete y, a continuación, haga clic en **Abrir**.

Debe importar el archivo de metadatos (.xml o .json), así como la imagen o el archivo de carga útil (.zip, .bin, .uxz, o .tgz), el archivo de historial de cambios (.chg) y el archivo léame (.txt) para la actualización. Todos los archivos seleccionados, pero no especificados en el archivo de metadatos, se descartan. Si no incluye el archivo de metadatos, la actualización no se importa.

e. Haga clic en **Importar**.

Una vez completada la importación, los paquetes del repositorio de actualizaciones de firmware se muestras en la tabla de la página Actualización del servidor de gestión y en el área Estado de descarga de dicha actualización aparece "Descargado."

- Para descargar uno o más *paquetes de actualizaciones de firmware* individuales.

1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Actualizaciones de firmware: Repositorio** para mostrar la página Repositorio de actualizaciones de firmware.
2. Si descarga firmware para dispositivos de almacenamiento de ThinkSystem serie DM, seleccione el país donde están ubicados los dispositivos de almacenamiento.
3. Haga clic en la pestaña **Actualizaciones individuales**.
4. Descargue las actualizaciones de firmware individuales más recientes:

– Si XClarity Administrator está conectado a Internet:

Para actualizar el catálogo y descargar la versión más reciente del firmware para todos los dispositivos gestionados, haga clic en **Todas las acciones → Actualizar y descargar la versión más reciente de todos los dispositivos gestionados**.

Para actualizar el catálogo y descargar la versión más reciente del firmware, solo para los dispositivos seleccionados:

a. Expanda el dispositivo para mostrar la lista de actualizaciones de firmware disponibles.

b. Seleccione una o más actualizaciones de firmware que desee descargar.

Consejo: un paquete de actualización puede constar de varias actualizaciones de firmware. Cuando descargue una actualización de firmware, puede elegir si descarga el paquete de actualizaciones completo o solamente unas actualizaciones concretas. También puede optar por descargar varios paquetes a la vez.

c. Haga clic en **Todas las acciones → Actualizar y descargar la versión más reciente para los dispositivos seleccionados**.

Cuando la descarga se haya completado, el área **Estado de descarga** para la actualización de firmware seleccionada cambia a “Descargado”.

- Si XClarity Administrator no está conectado a Internet:
  a. Descargue los paquetes de actualización de firmware desde el Sitio web del Soporte del Centro de Datos de Lenovo en una estación de trabajo que tenga conexión de red con el host XClarity Administrator.

     En los siguientes servidores, descargue las actualizaciones de firmware para el sistema operativo SLES 11 desde el Sitio web de Fix Central:

     - Flex System x220 tipo 2585, 7906
     - Flex System x222 Compute Nod tipo 2589, 7916
     - Flex System x240 tipo 7863, 8737, 8738, 8956
     - Flex System x280 / x480 / x880 X6 tipo 4259, 7903
     - Flex System x440 tipo 2584, 7917

     Para los demás servidores, descargue las actualizaciones de firmware para el sistema operativo RHEL 6, desde el Sitio web de soporte de Lenovo XClarity.

  b. Desde XClarity Administrator, haga clic en el icono **Importar** ().
  c. Haga clic en **Seleccionar archivos** y desplácese hasta la ubicación de las actualizaciones de firmware en la estación de trabajo.
  d. Seleccione todos los archivos del paquete y, a continuación, haga clic en **Abrir**.

     Debe importar el archivo de metadatos (.xml o .json), así como la imagen o el archivo de carga útil (.zip, .bin, .uxz, o .tgz), el archivo de historial de cambios (.chg) y el archivo léame (.txt) para la actualización. Todos los archivos seleccionados, pero no especificados en el archivo de metadatos, se descartan.

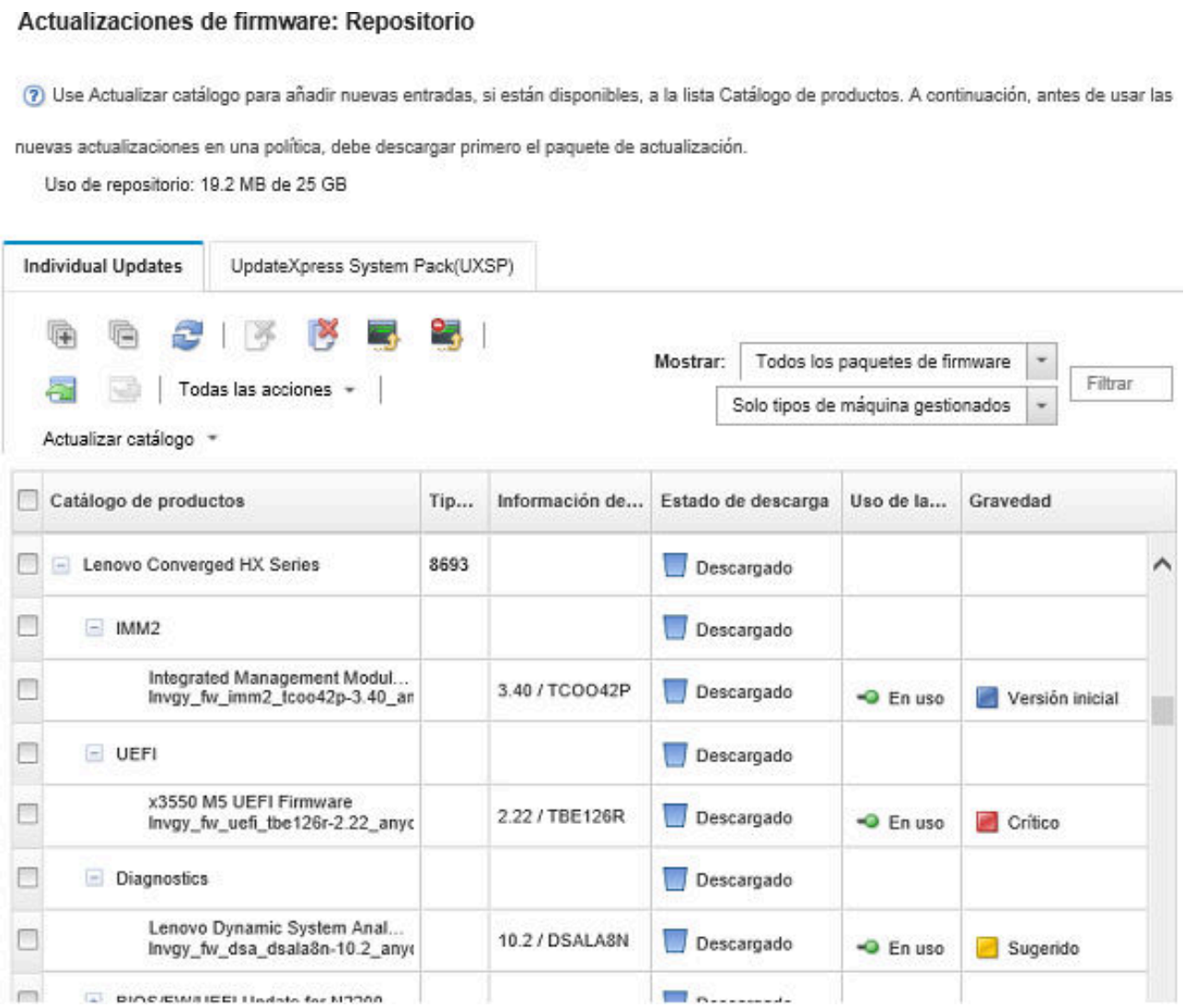
     Atención:

     - Solo importe estos archivos necesarios. No importe otros archivos que puedan encontrarse en los sitios web de descarga de firmware.
     - Si no incluye el archivo XML en el paquete de actualizaciones, la actualización no se importa.
     - Si no incluye todos los archivos requeridos que están asociados a la actualización, el repositorio muestra que la actualización no se descarga, lo que significa que se importa parcialmente. Posteriormente, puede incorporar los archivos que falten seleccionándolos e importándolos.
     - Las actualizaciones de firmware principales (como el controlador de gestión, UEFI y pDSA) no dependen del sistema operativo. Los paquetes de actualización de firmware para los sistemas operativos RHEL 6 o SLES 11 se utilizan para actualizar nodos de cálculo y servidores de bastidor. Para obtener más información acerca de los paquetes de actualización de firmware que deben utilizarse para sus servidores gestionados, consulte Descarga de actualizaciones de firmware.

  e. Haga clic en **Importar**.

La actualización del catálogo y la descarga de las actualizaciones de firmware pueden durar varios minutos. Cuando las actualizaciones se han descargado y almacenado en el repositorio, la fila del catálogo de productos se resalta y la columna **Estado de descarga** cambia a “Descargado”.

Nota: Puede que el tipo de equipo para algunos conmutadores se muestre como un número hexadecimal.



Después de finalizar

Puede configurar el tamaño máximo del repositorio de actualizaciones (que incluye firmware, controladores de dispositivos del SO y actualizaciones del servidor de gestión) en la página Repositorio de firmware, haciendo clic en **Todas las acciones → Valores globales**. El tamaño mínimo es de 50 GB. El tamaño máximo depende de la cantidad de espacio en el disco del sistema local.

Exportación e importación de actualizaciones de firmware

Puede exportar actualizaciones de firmware individuales y UpdateXpress System Packs (UXSP) que existen en el repositorio para el sistema local.

Acerca de esta tarea

Solo se exportan las actualizaciones de firmware que existen en el repositorio. Asegúrese de que el estado de descarga para las actualizaciones de firmware seleccionadas sea “Descargado.”

Todos los archivos que están asociados con la actualización de firmware se exportan, incluidos la imagen de actualización o el archivo de carga útil (.zip, .bin, .uxz o .tgz), el archivo de metadatos (.xml o .json), el archivo de historial de cambios (.chg) y el archivo léame (.txt).

Atención: No cambie el nombre de los archivos de actualización de firmware.

Procedimiento

- Para exportar actualizaciones de firmware:
  1. Haga clic en la pestaña **Actualizaciones individuales** o **UpdateXpress System Packs (UXSP)**.
  2. Seleccione una o varias actualizaciones de firmware.
  3. Haga clic en el icono **Export** Exportar (ícono  (Colapsar)).
- Para importar actualizaciones de firmware:

  Puede importar archivos manualmente exportado desde Lenovo XClarity Administrator y los archivos que descargó manualmente desde la web. Para obtener más información, consulte el apartado Descarga de actualizaciones de firmware.

Eliminación de actualizaciones de firmware

Puede eliminar las actualizaciones de firmware y los UpdateXpress System Packs (UXSP) desde el repositorio de actualizaciones de firmware.

Antes de empezar

Asegúrese de que todos los trabajos de actualización planificados o en ejecución que utilicen una política de conformidad de firmware que contenga actualizaciones de firmware que se han de eliminar, se hayan completado o cancelado (consulte Supervisión de trabajos).

Antes de eliminar la actualización, asegúrese de que la actualización no se esté utilizando en una política de cumplimiento de firmware. No es posible eliminar un paquete de actualización de firmware que se encuentre en uso en la actualidad en una o varias políticas de cumplimiento de firmware.

Eliminar un UXSP, también elimina la política de cumplimiento de firmware que se crea automáticamente para ese UXSP.

Nota: Tenga cuidado al eliminar actualizaciones de firmware y UXSP si el repositorio de actualizaciones de firmware se encuentra en una carpeta compartida remota que se usa en varias instancias de XClarity Administrator.

Procedimiento

Realice los pasos siguientes para eliminar una o varias actualizaciones de firmware del repositorio.

Paso 1. Anule la asignación de todas las políticas de cumplimiento de firmware que contienen actualizaciones de firmware que se han de eliminar de todos los dispositivos gestionados.

   a. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Aplicar/Activar**. Se muestra la página Actualizaciones de firmware: Aplicar/Activar.

   b. Seleccione “Sin asignación” o elija otra política de cumplimiento de firmware en la columna **Política asignada** para los dispositivos gestionados que utilicen la política de cumplimiento de firmware.

Paso 2. Elimine todas las políticas de cumplimiento de firmware definidas por el cliente que contengan las actualizaciones de firmware que se han de eliminar, o bien edite las políticas de cumplimiento de firmware para quitar las actualizaciones de firmware que se deben eliminar.

   a. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Políticas de cumplimiento**. Se muestra la página Actualizaciones de firmware: Políticas de cumplimiento.

b. Seleccione la política de cumplimiento de firmware y, a continuación, seleccione el icono **Eliminar** () para eliminar la política, o bien haga clic en el icono **Editar** () para quitar las actualizaciones de firmware de la política.

Paso 3. Elimine las actualizaciones de firmware.

- **Actualizaciones de firmware individuales**
  1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Actualizaciones de firmware: Repositorio** . Se muestra la página Repositorio de actualizaciones de firmware.
  2. Haga clic en la pestaña **Actualizaciones individuales**.
  3. Seleccione una o más actualizaciones de firmware a eliminar.
  4. Haga clic en el icono **Eliminar solo imágenes** () para eliminar solo la imagen o el archivo de carga útil (.zip, .bin, .uxz o .tgz). Información sobre la actualización, se conserva para que pueda descargar nuevamente la actualización con facilidad, si es necesario. O haga clic en el icono **Eliminar paquetes de actualización completos** () para eliminar los paquetes de actualización completos, lo que incluye la imagen o el archivo de carga útil, cambiar el archivo de historial (.chg), el archivo léame (.txt) y el archivo de metadatos (.xml o .json).

  Cuando elimina una actualización de firmware, también se eliminan los archivos de carga útil. Sin embargo, el archivo de metadatos, que contiene información sobre la actualización, se conserva para que pueda volver a descargarla fácilmente, si es necesario, y el **Estado de descarga** cambia a “No descargado”.
- **UXSP**
  1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Actualizaciones de firmware: Repositorio** . Se muestra la página Repositorio de actualizaciones de firmware.
  2. Haga clic en la pestaña **UpdateXpress System Pack (UXSP)**.
  3. Seleccione uno o más UXSP para eliminar.
  4. Haga clic en el icono **Eliminar UXSP y políticas asociadas** () para eliminar los UXSP completos, lo que incluye la imagen o el archivo de carga útil, cambiar el archivo de historial (.chg), el archivo léame (.txt) y el archivo de metadatos (.xml o .json) y todas las políticas de cumplimiento de firmware asociadas.

  Si los USXSP seleccionados están asociados con políticas que están en uso (asignadas a dispositivos), se muestra el cuadro de diálogo Eliminar UXSP, Política y Paquetes de actualización. Elija si eliminar la directivas asignadas además del UXSP y las políticas no asignadas y haga clic en **Aceptar**.

Creación y asignación de políticas de cumplimiento de firmware

Las Políticas de cumplimiento de firmware garantizan que el firmware de determinados dispositivos gestionados se encuentra en el nivel actual o especificado marcando los dispositivos que necesitan atención. Cada política de cumplimiento de firmware identifica qué dispositivos se supervisan y qué nivel de firmware se debe instalar a fin de mantener la conformidad de los dispositivos. Puede establecer la conformidad en el nivel del dispositivo o del componente de firmware. XClarity Administrator luego utiliza estas políticas para comprobar el estado de los dispositivos gestionados e identificar los dispositivos que están fuera de conformidad.

Antes de empezar

Al crear una política de cumplimiento de firmware, debe seleccionar la versión de actualización de destino que se va a aplicar a los dispositivos que se van a asignar a la política. Asegúrese de que las actualizaciones de firmware para la versión de destino estén en el repositorio de actualizaciones antes de crear la política (consulte Descarga de actualizaciones de firmware).

Si un tipo de dispositivo no aparece en el repositorio de actualizaciones de firmware, primero debe gestionar un dispositivo de ese tipo y, después, descargar o importar el conjunto completo de actualizaciones de firmware antes de crear políticas de cumplimiento para los dispositivos de ese tipo.

Acerca de esta tarea

Cuando cree una política de cumplimiento de firmware, puede elegir que XClarity Administrator distinga un dispositivo cuando:

- El firmware del dispositivo sea de un nivel inferior
- El firmware del dispositivo no coincide con la versión del destino de cumplimiento

XClarity Administrator viene con una política de cumplimiento de firmware predefinida con el nombre de **firmware más reciente en el repositorio**. Cuando se descargan o se importan nuevos firmware en el repositorio, esta política se actualiza a fin de incluir las versiones de firmware más recientes disponibles en el repositorio.

Después de asignar una política de cumplimiento de firmware a un dispositivo, XClarity Administrator comprueba el estado de cumplimiento de cada dispositivo cambia el inventario del dispositivo o el repositorio de actualizaciones de firmware. Cuando el firmware de un dispositivo no está en cumplimiento con la política asignada, XClarity Administrator identifica ese dispositivo como no en cumplimiento en la página Actualizaciones de firmware: aplicar/activar, en función de la regla que ha especificado en la política de cumplimiento de firmware

Por ejemplo, puede crear una política de cumplimiento de firmware que defina el nivel de línea base para el firmware que está instalado en todos los dispositivos ThinkSystem SR850 y, a continuación, asignar esa política de cumplimiento de firmware a todos los dispositivos ThinkSystem SR850. Cuando el repositorio de actualizaciones de firmware se actualiza y se agrega una nueva actualización de firmware, esos nodos de cálculo podrían estar fuera de conformidad. Si esto ocurre, XClarity Administrator actualiza la página Actualizaciones de firmware: Aplicar/Activar para mostrar los dispositivos que no son conformes y genera una alerta.

Nota: Puede elegir mostrar u ocultar las alertas de los dispositivos que no cumplen con los requisitos de las políticas de cumplimiento de firmware asignadas (consulte Configuración de los valores globales de actualización de firmware). De forma predeterminada, las alertas están ocultas.

Procedimiento

Para crear y asignar una política de cumplimiento de firmware, lleve a cabo los pasos siguientes.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Actualizaciones de firmware: políticas de cumplimiento**. Se muestra la página Política de cumplimiento con una lista de todas las políticas de cumplimiento de firmware existentes.

Paso 2. Cree una política de cumplimiento de firmware.

1. Haga clic en el icono **Crear** ( ) para abrir el cuadro de diálogo Crear una nueva política.

2. Rellene el nombre y la descripción de la política de cumplimiento de firmware.
3. Rellene la tabla según los criterios siguientes para cada dispositivo.
   - **Tipo de dispositivo**. Elija un tipo de dispositivo o componente al que se aplicará esta política.

     Consejo: Si elige un servidor, el nivel de cumplimiento se realiza en el nivel de UXSP. No obstante, también puede elegir expandir el servidor para establecer niveles específicos de firmware para cada componente, como el controlador de gestión de la placa base o el UEFI.
   - **Destino de cumplimiento**. Especifique el objetivo de cumplimiento para los dispositivos y subcomponentes aplicables.

     Para los servidores, puede elegir uno de los siguientes valores.

- **Predeterminado**. Cambia el objetivo de conformidad para cada uno al valor predeterminado (por ejemplo, el conjunto de firmware más reciente en el repositorio para ese dispositivo).
- **No actualizar**. Cambia el objetivo de cumplimiento para cada subcomponente a “No actualizar.”

Para los dispositivos sin subcomponentes (por ejemplo, CMM, conmutadores y dispositivos de almacenamiento) o para los subcomponentes en un servidor, puede elegir uno de los siguientes valores.

- *<firmware_level>*. Especifica el nivel de firmware base.
- **No actualizar**. Especifica que el firmware no se puede actualizar. Tenga en cuenta que el firmware en el controlador de gestión de respaldo no se actualiza de forma predeterminada.

Nota: Al cambiar los valores predeterminados para los subcomponentes en un servidor, se cambia el objetivo de conformidad para el servidor a **Personalizado**.

- **Regla de cumplimiento**. Especifique cuándo un dispositivo se debe marcar como no conforme en la columna **Versión instalada** en la página Actualizaciones de firmware: Aplicar/Activar.
  - **Marcar en caso de nivel inferior**. Si el nivel de firmware instalado en un dispositivo es anterior al nivel que se ha especificado en la política de cumplimiento de firmware, el dispositivo se marca como no conforme. Por ejemplo, si sustituye un adaptador de red en un nodo de cálculo y el firmware en dicho adaptador de red es anterior al nivel identificado en la política de cumplimiento de firmware, el nodo de cálculo se marca como no conforme.
  - **Marcar si no hay coincidencia exacta**. Si el nivel de firmware instalado en un dispositivo no coincide exactamente con la política de cumplimiento de firmware, el dispositivo se marca como no conforme. Por ejemplo, si sustituye un adaptador de red en un nodo de cálculo y el firmware en dicho adaptador de red es distinto del nivel identificado en la política de cumplimiento de firmware, el nodo de cálculo se marca como no conforme.
  - **No marcar**. Los dispositivos que no se ajustan a la conformidad no se marcan.

4. **Opcional:** Expanda el tipo de sistema para mostrar cada actualización del paquete y seleccione el nivel de firmware que se usará como destino de cumplimiento, o bien seleccione “No actualizar” para impedir que el firmware se actualice en dicho dispositivo.
5. Haga clic en **Crear**.

   La política de cumplimiento de firmware se enumera en la tabla en la página Actualizaciones de firmware: Política de cumplimiento. La tabla muestra el estado de uso, el origen de la política (si la ha definido el usuario o está predefinida) y la última fecha de modificación.

Paso 3. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Actualizaciones de firmware: Aplicar/Activar**. Se muestra la página Actualizaciones de firmware: Aplicar/Activar con una lista de los dispositivos gestionados.

Paso 4. Asigne la política de cumplimiento de firmware a dispositivos.

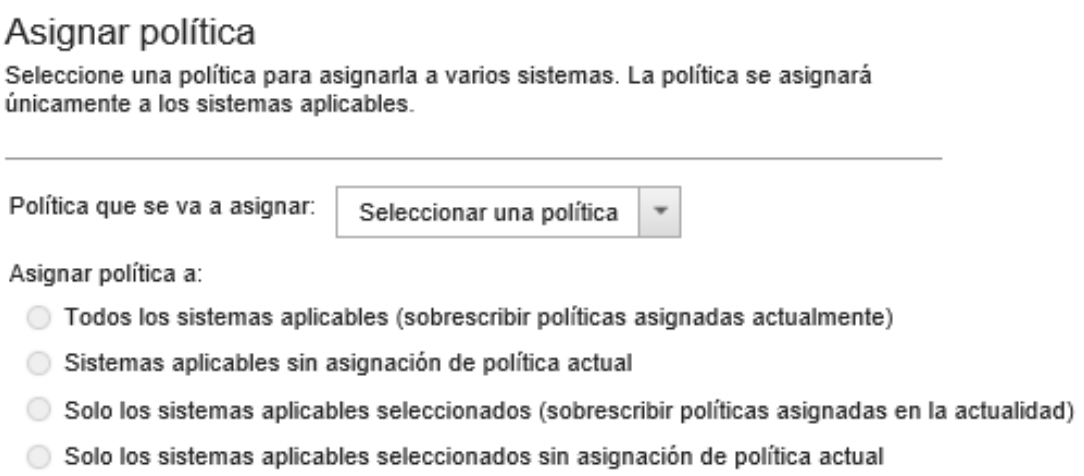
- **A un solo dispositivo**

  Para cada dispositivo, seleccione una política desde el menú desplegable en la columna **Política de cumplimiento asignada**.

  Puede seleccionar los valores de una lista de políticas de cumplimiento de firmware que son aplicables para cada dispositivo. Si una política no está actualmente asignada al dispositivo, la

política asignada se establece en **Sin asignación**. Si ninguna política es aplicable al dispositivo, la política asignada se establece en **No hay políticas aplicables**.

- **Para dispositivos múltiples**
  1. **Opcional:** seleccione uno o varios dispositivos a los que desee asignar una política de cumplimiento de firmware.
  2. Haga clic en el icono **Asignar política** ( ) para mostrar el cuadro de diálogo Asignar política.



  3. Seleccione una política de cumplimiento de firmware en el menú desplegable **Política para asignar**.

     Puede seleccionar los valores de una lista de políticas de cumplimiento de firmware que son para todos los dispositivos seleccionados. Si no se seleccionaron dispositivos antes de abrir el cuadro de diálogo, se enumeran todas las políticas.

     Para cancelar la asignación de una política, seleccione **Sin asignación**.
  4. Seleccione uno de los ámbitos siguientes para la asignación de la política.
     - **Todos los dispositivos aplicables que son...**
     - **Solo los dispositivos aplicables seleccionados que son...**
  5. Seleccione uno o varios criterios de dispositivos.
     - **Sin una política asignada**
     - **No conforme (sobrescriba la política asignada actual)**
     - **Conforme (sobrescriba la política asignada actual)**
     - **No supervisado (sobrescriba la política asignada actual)**
     - **Otro (sobrescriba la política asignada actual)**. Esto se aplica a dispositivos de otros estados, como Estado pendiente, con datos que faltan o que no son compatibles con las actualizaciones. Sitúe el cursor sobre el icono de ayuda ( ) para ver una lista de los dispositivos correspondientes.

     Nota: Los criterios **No supervisado** y **Otro** se enumeran solo cuando hay dispositivos en esos estados.
  6. Haga clic en **Aceptar**.

     La política que figura en la columna **Política asignada** en la página Actualizaciones de firmware: Repositorio cambia al nombre de la política de cumplimiento de firmware seleccionada.

Después de finalizar

Una vez creada la política de cumplimiento de firmware, puede realizar las acciones siguientes en una política de cumplimiento de firmware seleccionada:

- Vea los detalles de la política, incluida una lista de dispositivos asignados, haciendo clic en el nombre de la política en la tabla.
- Cree un duplicado de una política seleccionada haciendo clic en el icono **Copiar** ( ).
- Cambie el nombre o modifique una política seleccionada haciendo clic en el icono **Editar** ( ).No puede editar una política de cumplimiento de firmware predefinida o una política asignada a un dispositivo gestionado.

  Si modifica una política asignada de forma que ya no se aplique a ciertos dispositivos asignados, se cancela automáticamente la asignación de la política a dichos dispositivos.

  No puede cambiar el nombre ni modificar la política predefinida de **Firmware más reciente**.
- Elimine una política de cumplimiento de firmware seleccionada, al hacer clic en el icono **Eliminar política** ( ) o elimine la política de cumplimiento de firmware seleccionada y todas las actualizaciones de firmware asociadas que usa esa política, al hacer clic en el icono **Eliminar cualquier política y paquete de firmware** ( ).Puede optar por eliminar la política aunque esté asignada a un dispositivo.

  Cuando elimina una política que está asignada a un dispositivo, se elimina la asignación de política hasta que se borre.

  No puede eliminar la política de **Firmware más reciente** predefinida; no obstante, puede deshabilitar la política haciendo clic en el icono **Valores globales** ( ) y seleccionando a continuación **Deshabilitar la última política de firmware**. Cuando esta opción está seleccionada, la política de firmware más reciente no está asignada a los dispositivos gestionados y la política ya no se actualiza para incluir las versiones de firmware más recientes disponibles en el repositorio.
- Exporte una política seleccionada a un sistema local seleccionando las políticas y haciendo clic en el icono **Exportar** ( ). Luego podrá importar las políticas a otra instancia de XClarity Administrator pulsando el icono **Importar** ( ).

Después de crear una política de cumplimiento de firmware, puede asignar la política a un dispositivo específico (consulte Creación y asignación de políticas de cumplimiento de firmware) y aplicar y activar las actualizaciones para ese dispositivo (consulte Aplicación y activación de actualizaciones de firmware).

Identificación de dispositivos no conformes

Si una política de cumplimiento de firmware se ha asignado a un dispositivo gestionado, puede determinar si el firmware en ese dispositivo es conforme con dicha política.

Procedimiento

Para determinar si el firmware de un dispositivo es conforme con su política de cumplimiento de firmware asignada, haga clic en **Aprovisionamiento → Actualizaciones de firmware: Aplicar/Activar** en la Lenovo XClarity Administrator barra de menús para mostrar la página Actualización de firmware: Política de cumplimiento y consulte la columna **Versiones instaladas** correspondiente a ese dispositivo.

La columna **Versiones instaladas** contiene uno de los valores siguientes:

- **Versión de firmware**. La versión de firmware instalada en el dispositivo es conforme con la política asignada.

- **Conformidad**. El firmware instalado en el dispositivo es conforme con la política asignada.
- **No conforme**. El firmware instalado en el dispositivo no es conforme con la política asignada.
- **No se ha definido ninguna política de cumplimiento**. No hay una política de cumplimiento de firmware asignada al dispositivo.

Puede hacer clic en el icono **Actualizar** ( ) para actualizar el contenido de la columna **Versión instalada**.

Configuración de los valores globales de actualización de firmware

Valores globales se utilizan como valores predeterminados cuando se aplican las actualizaciones de firmware.

Acerca de esta tarea

En la página Valores globales, puede configurar los siguientes valores:
- Soporte mejorado para dispositivos de nivel inferior
- Alertas para dispositivos que no están en cumplimiento con sus políticas asignadas
- Asignación automática de una política de cumplimiento de firmware a un dispositivo que no tenga una política asignada
- Estado de no conformidad para dispositivos con un componente de firmware que no tiene ningún destino asociado en la política de cumplimiento de firmware

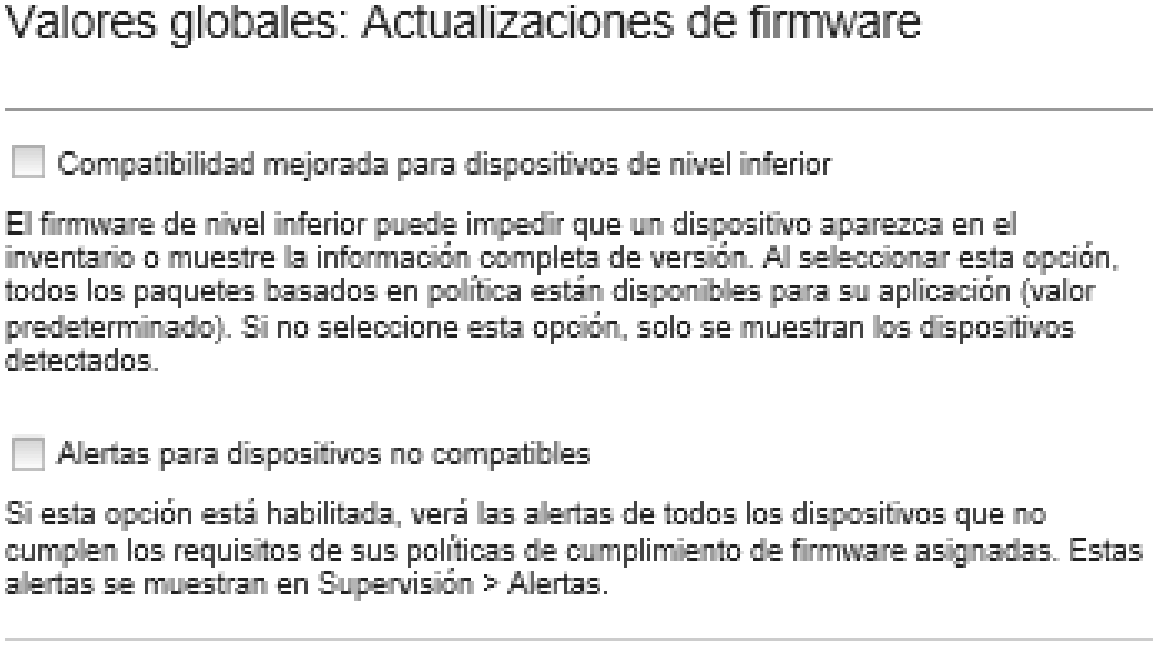
Procedimiento

Para configurar los valores globales que se utilizarán en todos los servidores, lleve a cabo los pasos siguientes.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Aprovisionamiento → Actualizaciones de firmware: Aplicar/Activar**. Se muestra la página Actualizaciones de firmware: Aplicar/Activar.

Paso 2. Haga clic en la pestaña **Actualizar con política** o **Actualizar sin política**.

Paso 3. Haga clic en **Todas las acciones → Valores globales** para mostrar el cuadro de diálogo Actualizaciones de firmware.



Paso 4. Opcionalmente, seleccione una de las siguientes opciones.

- Seleccione **Compatibilidad mejorada para dispositivos de nivel inferior** para mostrar el inventario y la información completa de la versión de todos los dispositivos, incluso si el firmware tiene un nivel inferior o si el dispositivo no está en el inventario.
- Seleccione **Alertas de los dispositivos no conformes** para mostrar alertas en la página Alertas para dispositivos que no cumplen con los requisitos de las políticas de cumplimiento de firmware asignadas. Las alertas están ocultas en la página Alertas de forma predeterminada. Para obtener más información, consulte Visualización de alertas activas.
- Seleccione **Deshabilitar la asignación automática de política** para deshabilitar la asignación automática de una política de cumplimiento de firmware a un dispositivo que no tenga una política asignada. Si esta opción no está seleccionada, las políticas de cumplimiento de firmware se asignan a los dispositivos sin una política cuando XClarity Administrator se reinicia o cuando gestiona un dispositivo nuevo.
- Seleccione **Informe de no conformidad para el firmware sin destino** para marcar los dispositivos como no conformes cuando un componente de firmware no tiene un destino asociado en la política de cumplimiento de firmware. Si esta opción no está seleccionada, los dispositivos sin destinos se marcan como conformes.

Paso 5. Haga clic en **Aceptar** para cerrar el cuadro de diálogo.

Aplicación y activación de actualizaciones de firmware

Lenovo XClarity Administrator no aplica automáticamente las actualizaciones de firmware a los dispositivos gestionados. Puede elegir aplicar actualizaciones de firmware con o sin políticas de conformidad.

Antes de empezar

Cuando utiliza políticas de cumplimiento, puede planificar actualizaciones en dispositivos múltiples al mismo tiempo. XClarity Administrator actualiza dispositivos en la secuencia correcta automáticamente. Primero se actualiza el CMM, seguido por los conmutadores, los servidores y luego los dispositivos de almacenamiento.

Solo se aplican las actualizaciones de firmware descargadas.

Cuando realiza una actualización de firmware, XClarity Administrator inicia uno o varios trabajos para realizar la actualización.

Mientras la actualización de firmware está en progreso, el dispositivo de destino permanece bloqueado. No puede iniciar otras tareas de gestión en el dispositivo de destino hasta que se complete el proceso de actualización.

Después de aplicar una actualización de firmware a un dispositivo, pueden ser necesarios uno o varios reinicios para activar completamente la actualización de firmware. Puede elegir si el dispositivo se reinicia inmediatamente o diferir la activación o priorizar la activación. Si elige reiniciar inmediatamente, XClarity Administrator reduce a un mínimo el número de reinicios necesarios. Si elige diferir la activación, las actualizaciones se activan la próxima vez que el dispositivo se reinicia. Si elige la activación priorizada, las actualizaciones se activan de inmediato en el controlador de gestión de placa base y todas las demás actualizaciones se activan la próxima vez que se reinicia el dispositivo.

Puede actualizar firmware seleccionado en un máximo de 50 dispositivos a la vez. Si elige actualizar el firmware seleccionado en más de 50 dispositivos, el resto de los dispositivos se ponen en la cola. Un dispositivo en cola se saca de la cola de “actualización de firmware seleccionado” cuando la activación se completa en un dispositivo actualizado o un dispositivo actualizado se coloca en el estado de modo de mantenimiento pendiente (si se requiere un reinicio en ese dispositivo). Cuando un dispositivo en el estado de modo de mantenimiento pendiente se reinicia, el dispositivo arranca en el modo de mantenimiento y

continúa con el proceso de actualización, incluso si el número máximo de actualizaciones de firmware ya está en curso.

Puede actualizar firmware del paquete en un máximo de 10 dispositivos a la vez. Si elige actualizar firmware del paquete en más de 10 dispositivos, el resto de los dispositivos se ponen en la cola. Un dispositivo en cola se saca de la cola de “actualización de firmware del paquete” cuando la activación se completa en un dispositivo en el que se realizó una actualización de firmware del paquete.

Atención: Para Red Hat® Enterprise Linux (RHEL) versión 7 y posterior, el reiniciar el sistema operativo desde un modo gráfico suspende el servidor de forma predeterminada. Antes de poder llevar a cabo las acciones **Reiniciar normalmente** o **Reiniciar inmediatamente** desde Lenovo XClarity Administrator, debe configurar manualmente el sistema operativo para cambiar el comportamiento del botón de encendido/apagado a apagado. Para obtener instrucciones, consulte Guía de migración de datos y de administración de Red Hat: cambiar el comportamiento al presionar el botón de encendido en modo de destino gráfico.

Nota: XClarity Administrator habilita automáticamente la interfaz LAN sobre USB.

Aplicación de actualizaciones de firmware del paquete con políticas de cumplimiento

Después de que Lenovo XClarity Administrator identifica un dispositivo gestionado como no conforme, puede aplicar manualmente actualizaciones de firmware para *todos* los componentes de los servidores ThinkSystem SR635 y SR655 seleccionados que no cumplen con la política de cumplimiento de firmware asignada mediante una imagen del paquete que contenga los paquetes de actualización de firmware aplicables. La *imagen del paquete* se crea durante el proceso de actualización al recopilar todos los paquetes de actualización de firmware de la política de cumplimiento.

Antes de empezar

- Antes de actualizar el firmware en los dispositivos gestionados, lea las consideraciones sobre la actualización de firmware (consulte Consideraciones sobre la actualización de firmware).
- Inicialmente, los dispositivos que no admiten actualizaciones se ocultan en la vista. No se puede seleccionar los dispositivos que no se admiten actualizaciones.
- De manera predeterminada, todos los componentes detectados se muestran como disponibles para aplicar actualizaciones; no obstante, un firmware de nivel inferior puede impedir que un componentes aparezca en el inventario o presente la información completa de la versión. Para mostrar todos los paquetes basados en políticas que están disponibles para aplicar actualizaciones, haga clic en **Todas las acciones → Valores globales** y, a continuación, seleccione **Compatibilidad mejorada para dispositivos de nivel inferior**. Si esta opción está seleccionada, aparece “Otro software disponible” en la columna Installed Version (Versión instalada) de los dispositivos no detectados. Para obtener más información, consulte el apartado Configuración de los valores globales de actualización de firmware.

  Notas:

  – Los valores globales no se pueden cambiar cuando las actualizaciones en los dispositivos gestionados están en curso.

  – Las opciones adicionales tardan unos minutos en generarse. Después de unos instantes, puede que tenga que hacer clic en icono **Actualizar** () para actualizar la tabla.
- Asegúrese de que no haya trabajos que se encuentren en ejecución en la actualidad en el servidor de destino. Si hay trabajos en ejecución, el trabajo de actualización queda en cola hasta que se completen todos los otros trabajos. Para ver una lista de los trabajos activos, haga clic en **Supervisión → Trabajos**.
- La aplicación de actualizaciones de firmware del paquete solo es compatible con los servidores ThinkSystem SR635 y SR655.

- La aplicación de actualizaciones de firmware del paquete solo es compatible con las direcciones IPv4. No se admiten las direcciones IPv6.
- Asegúrese de que cada dispositivo de destino se haya arrancado en el SO al menos una vez para recuperar la información completa del inventario.
- Se requiere el firmware v2.94 o posterior del controlador de gestión de la placa base para utilizar la función de actualización del paquete.
- Solo se utilizan actualizaciones de firmware de paquetes de repositorios o actualizaciones de firmware individuales. No se admiten UpdateXpress System Packs (UXSPs).
- Solo se aplican las actualizaciones de firmware descargadas. Actualice el catálogo de productos y descargue las actualizaciones de firmware adecuadas (consulte Actualización del catálogo de productos y Descarga de actualizaciones de firmware).

  Nota: Cuando XClarity Administrator se instala por primera vez, el catálogo de productos y el repositorio están vacíos.
- La comprobación de conformidad solo es compatible con el controlador de gestión de la placa base y la UEFI en los servidores ThinkSystem SR635 y SR655; sin embargo, XClarity Administrator intenta aplicar actualizaciones de firmware a todos los componentes de hardware disponibles.
- Las actualizaciones se aplican de acuerdo con la política de cumplimiento de firmware asignada. No puede optar por actualizar un subconjunto de componentes.
- Se requiere XClarity Administrator v3.2 o posterior para aplicar actualizaciones de firmware para Lenovo XClarity Provisioning Manager (LXPM), controladores Windows LXPM o controladores Linux LXPM a servidores ThinkSystem SR635 y SR655.
- Las actualizaciones del controlador de gestión de la placa base y de la UEFI se omiten si la versión instalada en el momento es mayor que la política de cumplimiento asignada.
- Las políticas de cumplimiento de firmware se deben crear y asignar a los dispositivos en los que tenga previsto aplicar las actualizaciones de firmware. Para obtener más información, consulte el apartado Creación y asignación de políticas de cumplimiento de firmware.
- Los dispositivos seleccionados se apagan antes de iniciar el proceso de actualización. Asegúrese de que todas las cargas de trabajo en ejecución se hayan detenido o, si está trabajando en un entorno virtualizado, se hayan desplazado a otro servidor.

Atención: Los dispositivos seleccionados se apagan antes de iniciar el proceso de actualización. Asegúrese de que todas las cargas de trabajo en ejecución se hayan detenido o, si está trabajando en un entorno virtualizado, se hayan desplazado a otro servidor. Si hay trabajos en ejecución, el trabajo de actualización queda en cola hasta que se completen todos los otros trabajos. Para ver una lista de los trabajos activos, pulse **Supervisión → Trabajos**.

Acerca de esta tarea

El proceso de actualización del paquete actualiza primero el controlador de gestión de la placa base y la UEFI fuera de banda. Una vez completadas estas actualizaciones, el proceso crea una imagen del paquete del firmware restante de la política de cumplimiento según el tipo de equipo. A continuación, el proceso monta la imagen en el dispositivo seleccionado y reinicia el dispositivo para arrancar la imagen. La imagen se ejecuta automáticamente para realizar el resto de actualizaciones.

Puede actualizar firmware del paquete en un máximo de 10 dispositivos a la vez. Si elige actualizar firmware del paquete en más de 10 dispositivos, el resto de los dispositivos se ponen en la cola. Un dispositivo en cola se saca de la cola de “actualización de firmware del paquete” cuando la activación se completa en un dispositivo en el que se realizó una actualización de firmware del paquete.

Si se produce un error al actualizar un componente del dispositivo, el proceso de actualización de firmware no actualiza el firmware para ese componente específico. En cambio, el proceso de actualización de firmware continúa actualizando el resto de los componentes en el dispositivo y prosigue con la actualización de todos los demás dispositivos en el trabajo de actualización de firmware actual.

Procedimiento

Para aplicar actualizaciones de firmware en forma de imagen del paquete en dispositivos gestionados, lleve a cabo los pasos siguientes.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Actualizaciones de firmware: Aplicar/Activar**. Se muestra la página Actualizaciones de firmware: Aplicar/Activar.

Paso 2. Haga clic en la pestaña **Actualizar con política**.

Paso 3. Seleccione uno o más dispositivos y componentes a los que deben aplicarse las actualizaciones de firmware.

Puede ordenar las columnas de la tabla para que sea más fácil encontrar dispositivos específicos. Además, puede filtrar la lista de dispositivos visualizados al seleccionar una opción en el menú **Mostrar** de modo que se muestren solo los dispositivos en un chasis, bastidor o grupo específico al introducir texto (como un nombre o dirección IP) en el campo **Filtro** o haciendo clic en los siguientes iconos para mostrar solo los dispositivos con un estado específico.

- Icono **Ocultar dispositivos no compatibles** ()
- Icono **Ocultar estado de dispositivos en incumplimiento** ()
- Icono **Ocultar dispositivos sin una política de cumplimiento asignada** ()
- Ícono **Ocultar dispositivos que no se están supervisando** ()
- Ícono **Ocultar dispositivos con firmware en espera de activación** ()
- Ícono **Ocultar dispositivos con errores de cumplimiento** ()
- Icono **Ocultar dispositivos no compatibles con actualizaciones** ()
- Icono **Ocultar dispositivos sometidos a actualizaciones de firmware** ()
- Ícono **Ocultar dispositivos con firmware que no se puede implementar en etapas** ()

La columna **Grupos** indica los grupos en los que cada dispositivo es un miembro. Puede posar el cursor sobre la columna **Grupos** para obtener una lista completa de los grupos ordenada por tipo de grupo

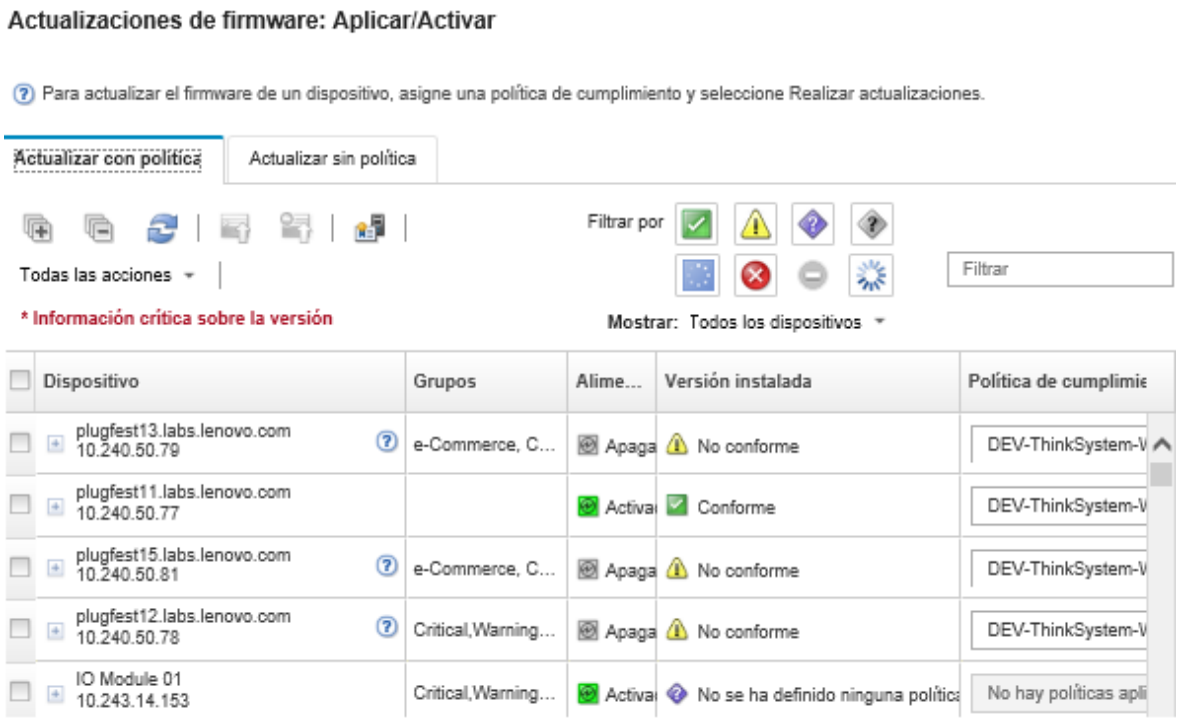
La columna **Versión instalada** indica la versión de firmware instalada, el estado de cumplimiento o el estado del dispositivo.

El estado de cumplimiento puede ser cualquiera de los siguientes:

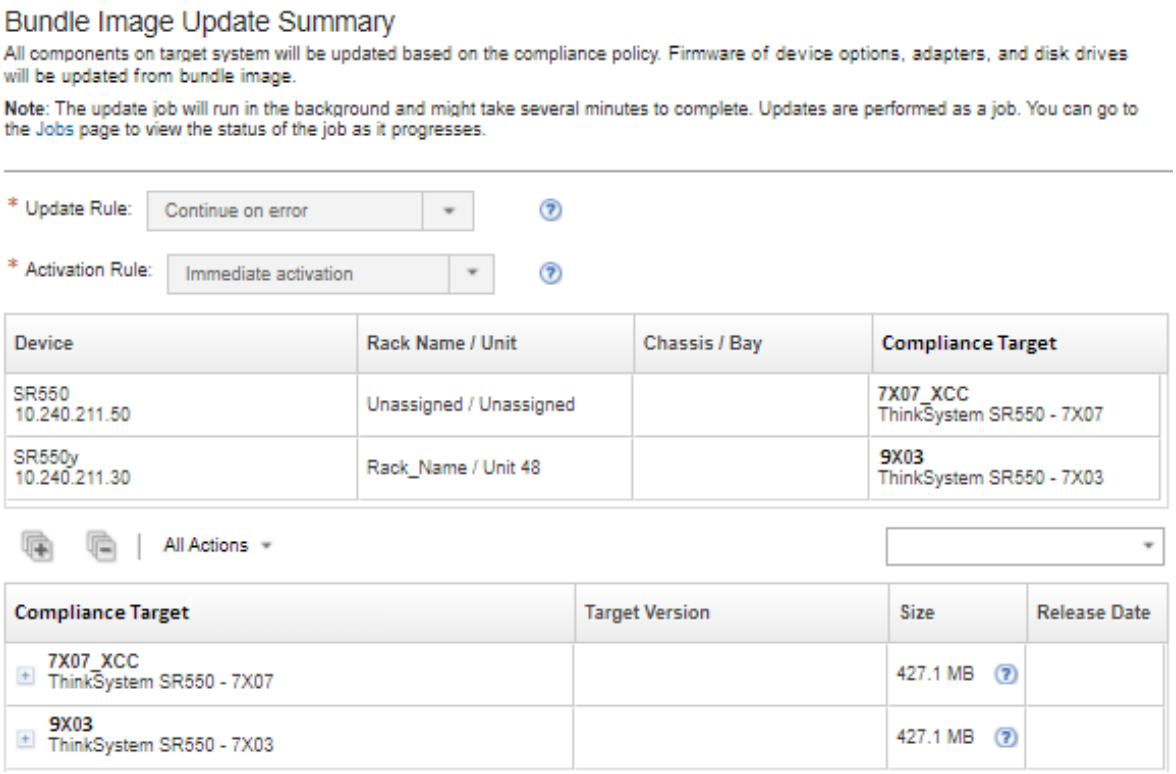
-  **Conforme**
-  **Error de cumplimiento**
-  **No conforme**
-  **No se ha definido ninguna política de cumplimiento**
-  **No supervisado**

El estado del dispositivo puede ser uno de los siguientes:

- **No se admiten actualizaciones**
- **Actualización en curso**



Paso 4. Haga clic en el icono **Realizar actualización desde la imagen del paquete** ( ). Se muestra el cuadro de diálogo Resumen de actualización de la imagen del paquete. Este cuadro de diálogo lista los dispositivos seleccionados y lasa actualizaciones de firmware que se incluyen en la imagen del paquete.



Paso 5. Haga clic en **Realizar actualización desde la imagen del paquete** para actualizar de inmediato, o bien haga clic en **Programación** planificar que esta actualización se ejecute posteriormente.

Después de finalizar

Si el servidor no logra iniciar el modo de mantenimiento cuando se aplica una actualización de firmware, intente volver a aplicar la actualización.

Si las actualizaciones no se han completado correctamente, consulte Problemas relacionados con el repositorio y la actualización de firmware en la documentación en línea de XClarity Administrator para saber cómo resolver problemas y aplicar acciones correctivas.

En la página Actualizaciones de firmware: Aplicar/Activar, puede realizar las siguientes acciones.

- Exportar firmware e información de cumplimiento para cada dispositivo gestionado pulsando **Todas las acciones → Exportar vista como CSV**.

  Nota: El archivo CSV solo contiene información filtrada en la vista actual. No se incluye la información que se filtra fuera de la descripción y la información en columnas ocultas.
- Cancelar una actualización que se está aplicando a un dispositivo, seleccionando el dispositivo y pulsando el icono **Cancelar actualización** ( ).

  Nota: Puede cancelar las actualizaciones de firmware que están en espera para comenzar. Una vez comienza el proceso de actualización, solo se puede cancelar cuando el proceso de actualización realiza una tarea que no sea aplicar la actualización, por ejemplo, cambiar al modo de mantenimiento o reiniciar el dispositivo.
- Ver el estado de la actualización de firmware directamente en la columna **Estado** de la página Aplicar/Activar.
- Supervisar el estado del proceso de actualización desde el registro de trabajos. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Supervisión → Trabajos**.

Para obtener más información acerca del registro de trabajos, consulte Supervisión de trabajos.

Cuando los trabajos de actualización del firmware se hayan completado, puede verificar que los dispositivos cumplen con los estándares haciendo clic en **Aprovisionamiento → Actualizaciones de firmware: Aplicar/Activar** para volver a la página Actualizaciones de firmware: Aplicar/Activar y luego pulsando el icono **Actualizar** ( ). La versión actual del hardware que está activa en cada dispositivo aparece en la columna **Versión instalada**.

Aplicación de paquetes de firmware seleccionados con políticas de cumplimiento

Después de que Lenovo XClarity Administrator identifica un dispositivo como no conforme, puede aplicar y activar manualmente las actualizaciones de firmware en estos dispositivos gestionados. Puede elegir si desea aplicar y activar todas las actualizaciones de firmware que se aplican a una política de cumplimiento de firmware o seleccionar únicamente actualizaciones de firmware específicas de una política. Solo se aplican las actualizaciones de firmware descargadas.

Más información:

- XClarity Administrator: Aumento de la eficiencia al actualizar firmware
- Prácticas recomendadas para las actualizaciones de firmware y de controladores de Lenovo ThinkSystem
- XClarity Administrator: implementación básica a clúster
- XClarity Administrator: actualización de firmware
- XClarity Administrator: aprovisionamiento de actualizaciones de seguridad de firmware

Antes de empezar

- Antes de actualizar el firmware en los dispositivos gestionados, lea las consideraciones sobre la actualización de firmware (consulte Consideraciones sobre la actualización de firmware).
- Inicialmente, los dispositivos que no admiten actualizaciones se ocultan en la vista. No se puede seleccionar los dispositivos que no se admiten actualizaciones.
- De manera predeterminada, todos los componentes detectados se muestran como disponibles para aplicar actualizaciones; no obstante, un firmware de nivel inferior puede impedir que un componentes aparezca en el inventario o presente la información completa de la versión. Para mostrar todos los paquetes basados en políticas que están disponibles para aplicar actualizaciones, haga clic en **Todas las**

acciones → Valores globales y, a continuación, seleccione **Compatibilidad mejorada para dispositivos de nivel inferior**. Si esta opción está seleccionada, aparece “Otro software disponible” en la columna Installed Version (Versión instalada) de los dispositivos no detectados. Para obtener más información, consulte el apartado Configuración de los valores globales de actualización de firmware.

Notas:

- Los valores globales no se pueden cambiar cuando las actualizaciones en los dispositivos gestionados están en curso.
- Las opciones adicionales tardan unos minutos en generarse. Después de unos instantes, puede que tenga que hacer clic en icono **Actualizar** ( ) para actualizar la tabla.

- Asegúrese de que no haya trabajos que se encuentren en ejecución en la actualidad en el servidor de destino. Si hay trabajos en ejecución, el trabajo de actualización queda en cola hasta que se completen todos los otros trabajos. Para ver una lista de los trabajos activos, haga clic en **Supervisión → Trabajos**.
- Asegúrese de que el repositorio de actualizaciones de firmware contiene los paquetes de firmware que desea desplegar. En caso contrario, actualice el catálogo de productos y descargue las actualizaciones de firmware adecuadas (consulte Actualización del catálogo de productos y Descarga de actualizaciones de firmware).

  Nota: Cuando XClarity Administrator se instala por primera vez, el catálogo de productos y el repositorio están vacíos.

  Si tiene intención de instalar el firmware de requisito previo, asegúrese de que este también se descargue en el repositorio.

  En algunos casos, se pueden necesitar varias versiones para actualizar el firmware y todas las versiones se deberán descargar en el repositorio. Por ejemplo, para actualizar el conmutador escalable SAN de IBM FC5022 v7.4.0a a v8.2.0a, primero debe instalar v8.0.1-pha, v8.1.1 y luego v8.2.0a. Las tres versiones deben estar en el repositorio para actualizar el conmutador para v8.2.0a.
- Por lo general, los dispositivos deben reiniciarse para activar la actualización de firmware. Si elige reiniciar el dispositivo durante el proceso de actualización (*activación inmediata*), asegúrese de que las cargas de trabajo en ejecución se hayan detenido o, si está trabajando en un entorno virtualizado, se hayan desplazado a otro servidor.
- Para servidores ThinkSystem SR635 y SR655, puede utilizar esta función de actualización tradicional para aplicar únicamente actualizaciones de firmware del controlador de gestión de la placa base y de la UEFI. Se requiere una versión de firmware del controlador de gestión AMBT10M o posterior, y se requiere la versión de firmware de la UEFI CFE114L o posterior. Para actualizar todos los componentes (incluido el controlador de gestión, la UEFI, las unidades de disco y las opciones de E/S), utilice la función de actualización del paquete (consulte Aplicación de actualizaciones de firmware del paquete con políticas de cumplimiento).

Acerca de esta tarea

- Puede actualizar firmware seleccionado en un máximo de 50 dispositivos a la vez. Si elige actualizar el firmware seleccionado en más de 50 dispositivos, el resto de los dispositivos se ponen en la cola. Un dispositivo en cola se saca de la cola de “actualización de firmware seleccionado” cuando la activación se completa en un dispositivo actualizado o un dispositivo actualizado se coloca en el estado de modo de mantenimiento pendiente (si se requiere un reinicio en ese dispositivo). Cuando un dispositivo en el estado de modo de mantenimiento pendiente se reinicia, el dispositivo arranca en el modo de mantenimiento y continúa con el proceso de actualización, incluso si el número máximo de actualizaciones de firmware ya está en curso.
- Puede aplicar y activar el firmware que es posterior al firmware instalado actualmente.

- Puede optar por aplicar todas las actualizaciones para un dispositivo. No obstante, también puede elegir expandir un dispositivo para determinar actualizaciones para componentes específicos, como el controlador de gestión de la placa base o la UEFI.
- Si elige instalar un paquete de actualización de firmware que contiene actualizaciones para varios componentes, se actualizan todos los componentes a los que se aplica dicho paquete de actualización.

Procedimiento

Lleve a cabo los pasos siguientes para aplicar y activar actualizaciones en dispositivos gestionados.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Actualizaciones de firmware: Aplicar/Activar**. Se muestra la página Actualizaciones de firmware: Aplicar/Activar.

Paso 2. Haga clic en la pestaña **Actualizar con política**.

Paso 3. Seleccione uno o varios dispositivos y dispositivos a los que deben aplicarse las actualizaciones de firmware.

Puede ordenar las columnas de la tabla para que sea más fácil encontrar servidores específicos. Además, puede filtrar la lista de dispositivos visualizados al seleccionar una opción en el menú **Mostrar** de modo que se muestren solo los dispositivos en un chasis, bastidor o grupo específico al introducir texto (como un nombre o dirección IP) en el campo **Filtro** o haciendo clic en los siguientes iconos para mostrar solo los dispositivos con un estado específico.

- Icono **Ocultar dispositivos no compatibles** ()
- Icono **Ocultar estado de dispositivos en incumplimiento** ()
- Icono **Ocultar dispositivos sin una política de cumplimiento asignada** ()
- Ícono **Ocultar dispositivos que no se están supervisando** ()
- Ícono **Ocultar dispositivos con firmware en espera de activación** ()
- Ícono **Ocultar dispositivos con errores de cumplimiento** ()
- Icono **Ocultar dispositivos no compatibles con actualizaciones** ()
- Icono **Ocultar dispositivos sometidos a actualizaciones de firmware** ()
- Ícono **Ocultar dispositivos con firmware que no se puede implementar en etapas** ()

La columna **Grupos** indica los grupos en los que cada dispositivo es un miembro. Puede posar el cursor sobre la columna **Grupos** para obtener una lista completa de los grupos ordenada por tipo de grupo

La columna **Versión instalada** indica la versión de firmware instalada, el estado de cumplimiento o el estado del dispositivo.

El estado de cumplimiento puede ser cualquiera de los siguientes:

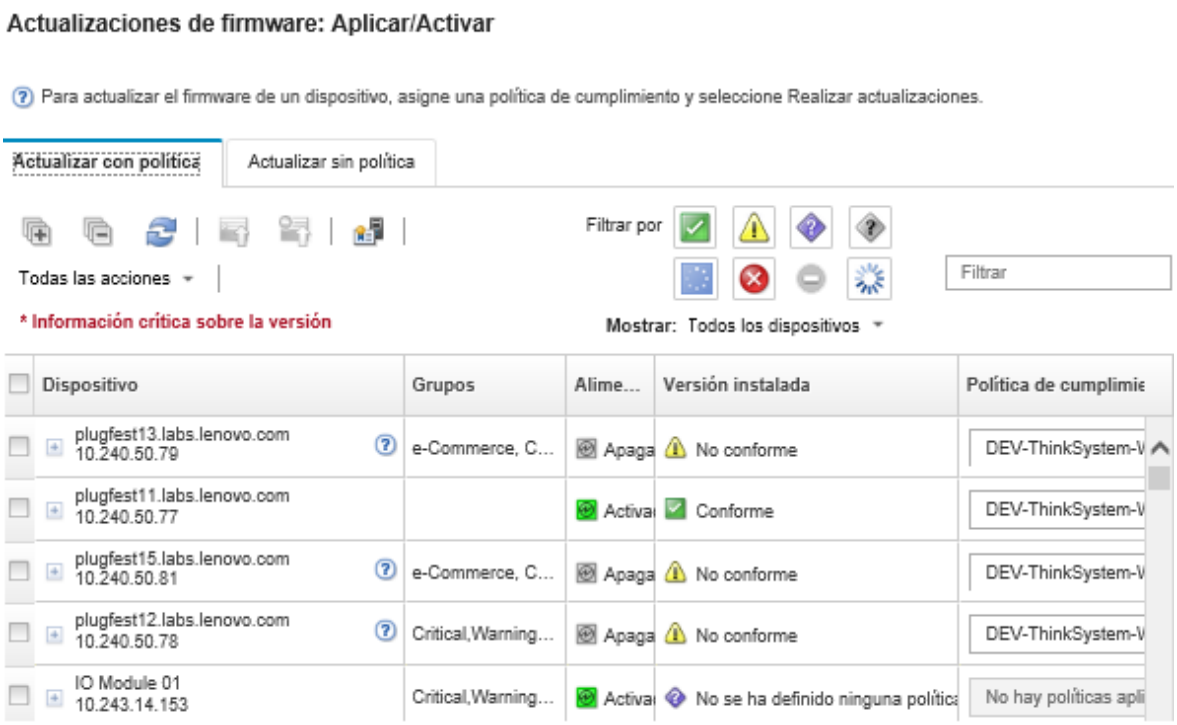
-  **Conforme**
-  **Error de cumplimiento**
-  **No conforme**
-  **No se ha definido ninguna política de cumplimiento**
-  **No supervisado**

El estado del dispositivo puede ser uno de los siguientes:

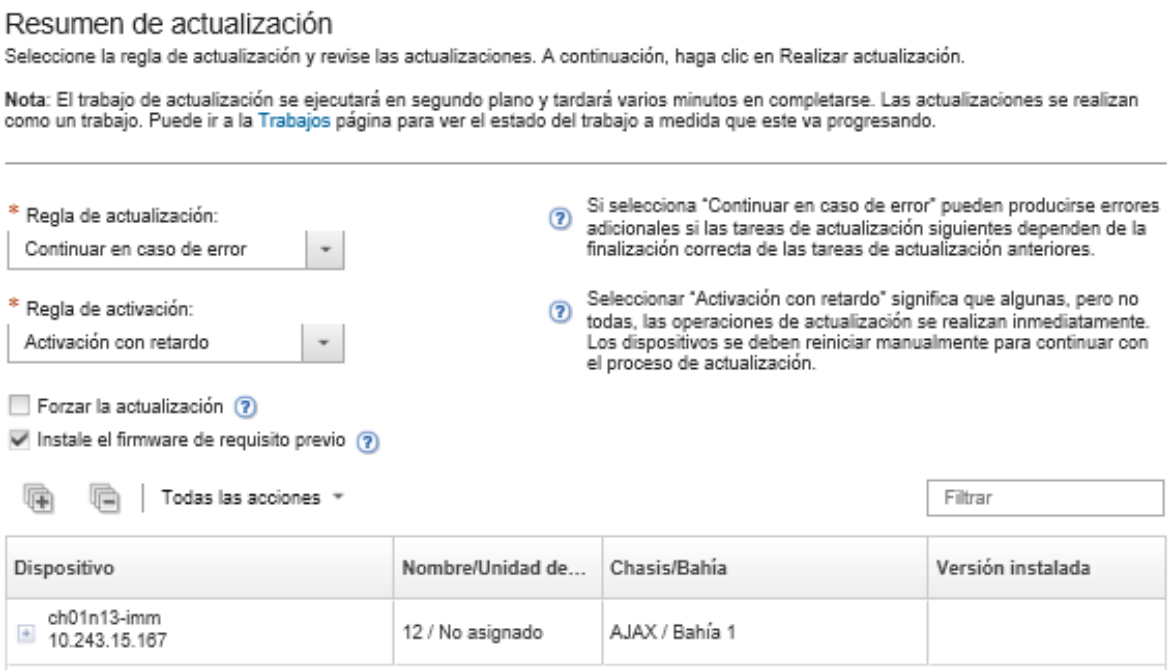
- **No se admiten actualizaciones**
- **Actualización en curso**

Notas: Si la versión de firmware instalada está en espera de activación, "(En espera de activación)" se agrega en el estado de la versión de firmware instalada o el estado de cumplimiento de cada dispositivo aplicable, por ejemplo "2.20 / A9E12EUS (en espera de activación)." Para ver el estado pendiente activación, la versión de firmware siguiente debe instalarse en el controlador de gestión de placa base principal en el servidor.

- **IMM2**: TCOO46F, TCOO46E o una versión posterior (según la plataforma)
- **XCC**: CDI328M, PSI316N, TEI334I o una versión posterior (según la plataforma)



Paso 4. Haga clic en el icono **Realizar actualizaciones** ( ). Se muestra el cuadro de diálogo Resumen de actualización.



Paso 5. Seleccione una de las siguientes reglas de actualización:

- **Detener todas las actualizaciones en caso de error**. Si se produce un error al actualizar alguno de los componentes (como un adaptador o el controlador de gestión) en el dispositivo objetivo, el proceso de actualización de firmware se detiene para todos los dispositivos seleccionados en el trabajo de actualización de firmware actual. En este caso, no se aplicará ninguna de las actualizaciones del paquete de actualizaciones para el dispositivo. El firmware actual que está instalado en todos los sistemas seleccionados sigue en efecto.
- **Continuar en caso de error**. Si se produce un error al actualizar alguno de los dispositivos del dispositivo, el proceso de actualización de firmware no actualiza el firmware para ese dispositivo específico. En cambio, el proceso de actualización de firmware continúa actualizando el resto de dispositivos en el dispositivo y prosigue con la actualización de todos los demás dispositivos en el trabajo de actualización de firmware actual.
- **Ir al siguiente sistema en caso de error**. Si se produce un error al actualizar alguno de los dispositivos del dispositivo, el proceso de actualización de firmware detiene todos los intentos de actualizar el firmware para ese dispositivo específico, de modo que el firmware actual que está instalado en dicho dispositivo continúa siendo efectivo. El proceso de actualización de firmware sigue actualizando todos los demás dispositivos del trabajo de actualización de firmware actual.

Paso 6. Seleccione una de las siguientes reglas de activación:

- **Activación inmediata**. Durante el proceso de actualización, el dispositivo se puede reiniciar automáticamente varias veces hasta que se complete el proceso de actualización. Asegúrese de poner en modo de inactividad todas las aplicaciones en el dispositivo antes de continuar.
- **Activación con retardo**. Se realizan algunas de las operaciones de actualización, pero no todas ellas. Los dispositivos se deben reiniciar para continuar con el proceso de actualización. Se realizan reinicios adicionales hasta que se completa la operación de actualización.

  Cuando el estado cambia a **modo de mantenimiento de firmware pendiente**, se produce un suceso para notificarle cuando se debe reiniciar el servidor.

  Si un dispositivo se reinicia por cualquier motivo, el proceso de actualización con retardo finaliza.

Esta regla de activación solo se admite para servidores y conmutadores de bastidor. Los CMM y los conmutadores Flex se activan de inmediato, independientemente de esta configuración.

Cuando el estado cambia a **modo de mantenimiento de firmware pendiente**, se produce un suceso para notificarle cuando se debe reiniciar el servidor.

El proceso de actualización con retardo finaliza cuando el dispositivo se reinicia por cualquier motivo (incluido un reinicio manual). No hay un límite de tiempo para cuando se debe reiniciar el servidor.

XClarity Administrator puede aplicar actualizaciones con activación con retardo para un máximo de 50 dispositivos a la vez. Si intenta aplicar actualizaciones con activación con retardo para más de 50 dispositivos, los dispositivos restantes se ponen en cola. Un dispositivo sale de la cola cuando el dispositivo que se está actualizando se coloca en el **estado Modo de mantenimiento de firmware pendiente.**

Importante:

- Si XClarity Administrator se reinicia durante el trabajo de actualización, este se detendrá con un error.
- Si un servidor en el estado **Modo de mantenimiento de firmware pendiente** se reinicia mientras XClarity Administrator está desactivado o no se puede acceder a él, el servidor arranca en la BMU; sin embargo, debido a que XClarity Administrator no puede conectarse a la BMU y supera el tiempo de espera después de 60 segundos, el controlador de gestión de la placa base restablece el estado de alimentación del sistema (se apaga si estaba apagado, se reinicia si estaba encendido).

- **Activación con prioridades**. Las actualizaciones se activan de inmediato en el controlador de gestión de placa base; todas las demás actualizaciones de firmware se activan la próxima vez que se reinicia el dispositivo. Se realizan reinicios adicionales hasta que se completa la operación de actualización. Esta regla solamente se admite para servidores.

  Se produce un suceso cuando el estado cambia a modo de mantenimiento de firmware pendiente para notificarlo cuando se debe reiniciar el servidor.

Nota: Cuando está habilitada, la opción de arranque de Wake on LAN puede interferir con las operaciones de XClarity Administrator que apaga el servidor, incluyendo las actualizaciones de firmware si hay un cliente Wake on LAN en su red que emita comandos “Wake on Magic Packet”

Paso 7. **Opcional:** seleccione **Forzar la actualización** para actualizar el firmware en los componentes seleccionados aun cuando el nivel de firmware esté actualizado o para aplicar una actualización de firmware más reciente que la instalada actualmente en los componentes seleccionados.

Nota: Puede aplicar versiones de firmware más recientes a las opciones, los adaptadores y las unidades del dispositivo que admiten versiones anteriores. Consulte la documentación del hardware para determinar si se admiten versiones anteriores.

Paso 8. **Opcional:** borrar **el firmware de requisitos previos de instalación** si no desea instalar el firmware de requisitos previos. El firmware de requisitos previos está instalado de manera predeterminada.

Nota: Cuando utiliza **Activación con retardo** o **Activación con prioridad** para requisitos previos para actualizaciones de firmware, es posible que deba reiniciar el servidor para activar el firmware de requisito previo. Después del reinicio inicial, las demás actualizaciones de firmware se instalan mediante **Activación inmediata**.

Paso 9. **Opcional:** si seleccionó **Activación inmediata**, seleccione **Prueba de memoria** para ejecutar una prueba de memoria después de que la actualización de firmware se complete, si el servidor se reinicia durante la actualización.

Esta opción es compatible con los servidores ThinkSystem v1 y v2 (excepto servidores ThinkSystem SR635, SR645, SR655 y SR665).

Paso 10. Haga clic en **Realizar actualización** para actualizar de inmediato, o bien haga clic en **Programación** planificar que esta actualización se ejecute posteriormente.

Si es necesario, puede realizar acciones de alimentación en los dispositivos gestionados. Las acciones de alimentación son útiles cuando se selecciona **Activación con retardo** y desea que las actualizaciones continúen cuando el dispositivo está en espera en el estado de "Mantenimiento pendiente". Para realizar una acción de alimentación en un dispositivo gestionado desde esta página, haga clic en **Todas las acciones → Acciones de alimentación** y, luego, haga clic en una de las siguientes acciones de alimentación.

- **Encender**
- **Apagar el SO y apagar**
- **Apagar**
- **Apagar el SO y reiniciar**
- **Reiniciar**

Después de finalizar

Si el servidor no logra iniciar el modo de mantenimiento cuando se aplica una actualización de firmware, intente volver a aplicar la actualización.

Si las actualizaciones no se han completado correctamente, consulte Problemas relacionados con el repositorio y la actualización de firmware en la documentación en línea de XClarity Administrator para saber cómo resolver problemas y aplicar acciones correctivas.

En la página Actualizaciones de firmware: Aplicar/Activar, puede realizar las siguientes acciones:

- Exportar firmware e información de cumplimiento para cada dispositivo gestionado pulsando **Todas las acciones → Exportar vista como CSV**.

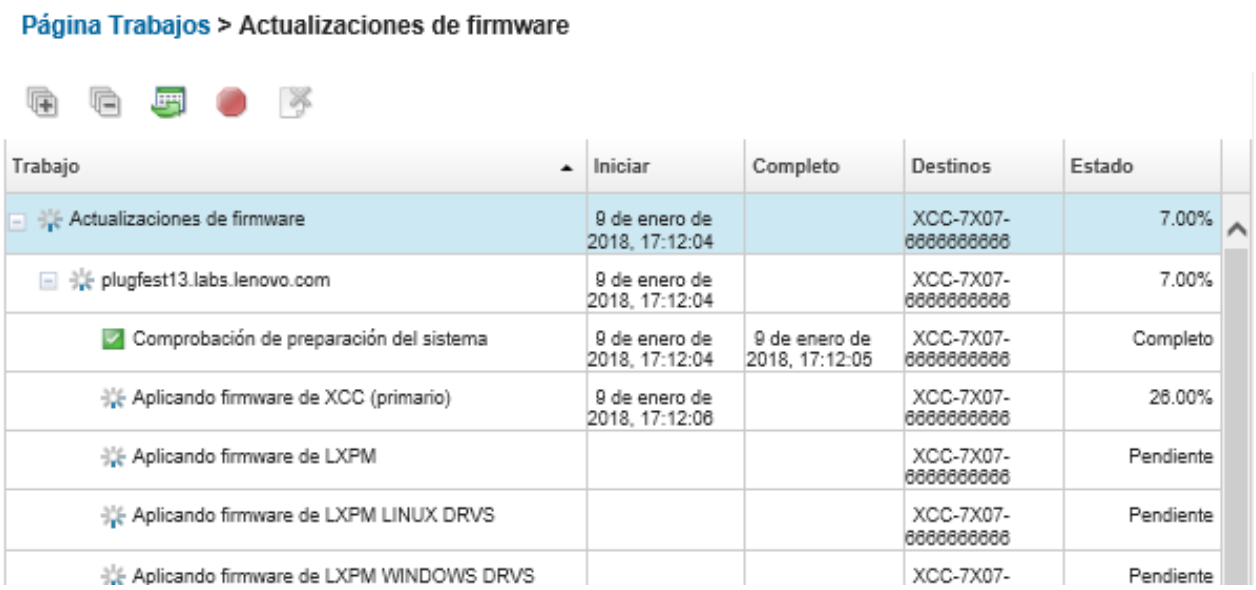
  Nota: El archivo CSV solo contiene información filtrada en la vista actual. No se incluye la información que se filtra fuera de la descripción y la información en columnas ocultas.

- Cancelar una actualización que se está aplicando a un dispositivo, seleccionando el dispositivo y pulsando el icono **Cancelar actualización** ().

  Nota: Puede cancelar las actualizaciones de firmware que están en espera para comenzar. Una vez comienza el proceso de actualización, solo se puede cancelar cuando el proceso de actualización realiza una tarea que no sea aplicar la actualización, por ejemplo, cambiar al modo de mantenimiento o reiniciar el dispositivo.

- Ver el estado de la actualización de firmware directamente en la columna **Estado** de la página Aplicar/Activar.
- Supervisar el estado del proceso de actualización desde el registro de trabajos. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Supervisión → Trabajos**.

  Para obtener más información acerca del registro de trabajos, consulte Supervisión de trabajos.



Cuando los trabajos de actualización del firmware se hayan completado, puede verificar que los dispositivos cumplen con los estándares haciendo clic en **Aprovisionamiento → Actualizaciones de firmware: Aplicar/Activar** para volver a la página Actualizaciones de firmware: Aplicar/Activar y luego pulsando el icono **Actualizar** ( ). La versión actual del hardware que está activa en cada dispositivo aparece en la columna **Versión instalada**.

Aplicación de actualizaciones de firmware seleccionadas sin utilizar políticas de cumplimiento

Puede aplicar y activar rápidamente firmware que es posterior al firmware instalado actualmente en un único dispositivo gestionado o grupo de dispositivos sin utilizar políticas de cumplimiento.

Más información:

- XClarity Administrator: Aumento de la eficiencia al actualizar firmware
- Prácticas recomendadas para las actualizaciones de firmware y de controladores de Lenovo ThinkSystem
- XClarity Administrator: implementación básica a clúster
- XClarity Administrator: actualización de firmware
- XClarity Administrator: aprovisionamiento de actualizaciones de seguridad de firmware

Antes de empezar

- Antes de actualizar el firmware en los dispositivos gestionados, lea las consideraciones sobre la actualización de firmware (consulte Consideraciones sobre la actualización de firmware).
- Inicialmente, los dispositivos que no admiten actualizaciones se ocultan en la vista. No se puede seleccionar los dispositivos que no se admiten actualizaciones.
- De manera predeterminada, todos los componentes detectados se muestran como disponibles para aplicar actualizaciones; no obstante, un firmware de nivel inferior puede impedir que un componentes aparezca en el inventario o presente la información completa de la versión. Para mostrar todos los paquetes basados en políticas que están disponibles para aplicar actualizaciones, haga clic en **Todas las acciones → Valores globales** y, a continuación, seleccione **Compatibilidad mejorada para dispositivos de nivel inferior**. Si esta opción está seleccionada, aparece “Otro software disponible” en la columna Installed Version (Versión instalada) de los dispositivos no detectados. Para obtener más información, consulte el apartado Configuración de los valores globales de actualización de firmware.

Notas:

- Los valores globales no se pueden cambiar cuando las actualizaciones en los dispositivos gestionados están en curso.
- Las opciones adicionales tardan unos minutos en generarse. Después de unos instantes, puede que tenga que hacer clic en icono **Actualizar** () para actualizar la tabla.

- Asegúrese de que no haya trabajos que se encuentren en ejecución en la actualidad en el servidor de destino. Si hay trabajos en ejecución, el trabajo de actualización queda en cola hasta que se completen todos los otros trabajos. Para ver una lista de los trabajos activos, haga clic en **Supervisión → Trabajos**.
- Asegúrese de que el repositorio de actualizaciones de firmware contiene los paquetes de firmware que desea desplegar. En caso contrario, actualice el catálogo de productos y descargue las actualizaciones de firmware adecuadas (consulte Actualización del catálogo de productos y Descarga de actualizaciones de firmware).

  Nota: Cuando XClarity Administrator se instala por primera vez, el catálogo de productos y el repositorio están vacíos.

  Si tiene intención de instalar el firmware de requisito previo, asegúrese de que este también se descargue en el repositorio.

  En algunos casos, se pueden necesitar varias versiones para actualizar el firmware y todas las versiones se deberán descargar en el repositorio. Por ejemplo, para actualizar el conmutador escalable SAN de IBM FC5022 v7.4.0a a v8.2.0a, primero debe instalar v8.0.1-pha, v8.1.1 y luego v8.2.0a. Las tres versiones deben estar en el repositorio para actualizar el conmutador para v8.2.0a.
- Por lo general, los dispositivos deben reiniciarse para activar la actualización de firmware. Si elige reiniciar el dispositivo durante el proceso de actualización (*activación inmediata*), asegúrese de que las cargas de trabajo en ejecución se hayan detenido o, si está trabajando en un entorno virtualizado, se hayan desplazado a otro servidor.

Acerca de esta tarea

- Puede actualizar firmware seleccionado en un máximo de 50 dispositivos a la vez. Si elige actualizar el firmware seleccionado en más de 50 dispositivos, el resto de los dispositivos se ponen en la cola. Un dispositivo en cola se saca de la cola de “actualización de firmware seleccionado” cuando la activación se completa en un dispositivo actualizado o un dispositivo actualizado se coloca en el estado de modo de mantenimiento pendiente (si se requiere un reinicio en ese dispositivo). Cuando un dispositivo en el estado de modo de mantenimiento pendiente se reinicia, el dispositivo arranca en el modo de mantenimiento y continúa con el proceso de actualización, incluso si el número máximo de actualizaciones de firmware ya está en curso.
- Puede aplicar y activar el firmware que es posterior al firmware instalado actualmente.
- Puede optar por aplicar todas las actualizaciones para un dispositivo. No obstante, también puede elegir expandir un dispositivo para determinar actualizaciones para componentes específicos, como el controlador de gestión de la placa base o la UEFI.
- Si elige instalar un paquete de actualización de firmware que contiene actualizaciones para varios componentes, se actualizan todos los componentes a los que se aplica dicho paquete de actualización.

Procedimiento

Lleve a cabo los pasos siguientes para aplicar y activar actualizaciones para los dispositivos gestionados.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Actualizaciones de firmware: Aplicar/Activar**. Se muestra la página Actualizaciones de firmware: Aplicar/Activar.

Paso 2. Haga clic en la pestaña **Actualizar sin política**.

Paso 3. Seleccione el nivel de firmware en la columna **Versiones posteriores descargadas** para cada dispositivo que quiera actualizar.

Paso 4. Seleccione uno o varios dispositivos y dispositivos que desee actualizar.

Puede ordenar las columnas de la tabla para que sea más fácil encontrar servidores específicos. Además, puede filtrar la lista de dispositivos visualizados al seleccionar una opción en el menú **Mostrar** de modo que se muestren solo los dispositivos en un chasis, bastidor o grupo específico al introducir texto (como un nombre o dirección IP) en el campo **Filtro** o haciendo clic en los siguientes iconos para mostrar solo los dispositivos con un estado específico.

- Icono **Ocultar componentes con algunas versiones posteriores** ()
- Icono **Ocultar componentes sin versiones posteriores** ()
- Icono **Ocultar dispositivos no compatibles con actualizaciones** ()
- Icono **Ocultar dispositivos sometidos a actualizaciones de firmware** ()
- Ícono **Ocultar dispositivos con firmware que no se puede implementar en etapas** ()

La columna **Grupos** indica los grupos en los que cada dispositivo es un miembro. Puede posar el cursor sobre la columna **Grupos** para obtener una lista completa de los grupos ordenada por tipo de grupo

La columna **Versión instalada** indica la versión de firmware instalada, el estado de cumplimiento o el estado del dispositivo.

El estado de cumplimiento puede ser cualquiera de los siguientes:

-  **Conforme**
-  **Error de cumplimiento**
-  **No conforme**
-  **No se ha definido ninguna política de cumplimiento**
-  **No supervisado**

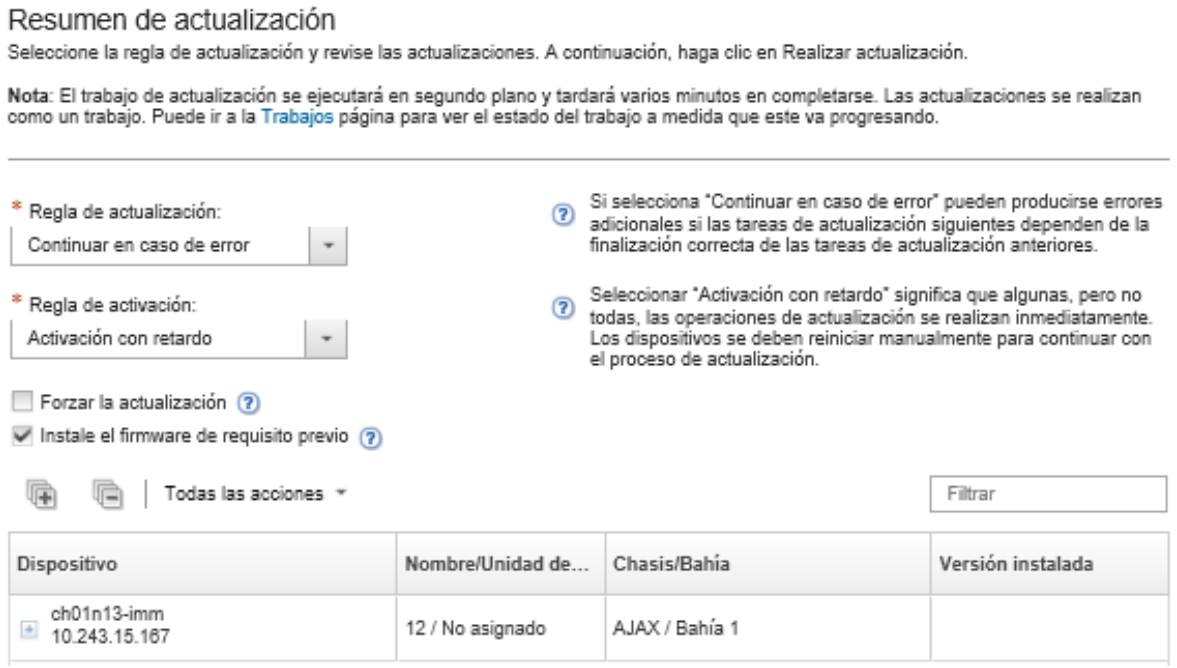
El estado del dispositivo puede ser uno de los siguientes:

-  **No se admiten actualizaciones**
-  **Actualización en curso**

Notas: Si la versión de firmware instalada está en espera de activación, "(En espera de activación)" se agrega en el estado de la versión de firmware instalada o el estado de cumplimiento de cada dispositivo aplicable, por ejemplo "2.20 / A9E12EUS (en espera de activación)." Para ver el estado pendiente activación, la versión de firmware siguiente debe instalarse en el controlador de gestión de placa base principal en el servidor.

- **IMM2**: TCOO46F, TCOO46E o una versión posterior (según la plataforma)
- **XCC**: CDI328M, PSI316N, TEI334I o una versión posterior (según la plataforma)

Paso 5. Haga clic en el icono **Realizar actualizaciones** ( ). Se muestra el cuadro de diálogo Resumen de actualización.



Paso 6. Seleccione una de las siguientes reglas de actualización:

- **Detener todas las actualizaciones en caso de error**. Si se produce un error al actualizar alguno de los componentes (como un adaptador o el controlador de gestión) en el dispositivo objetivo, el proceso de actualización de firmware se detiene para todos los dispositivos seleccionados en el trabajo de actualización de firmware actual. En este caso, no se aplicará ninguna de las actualizaciones del paquete de actualizaciones para el dispositivo. El firmware actual que está instalado en todos los sistemas seleccionados sigue en efecto.
- **Continuar en caso de error**. Si se produce un error al actualizar alguno de los dispositivos del dispositivo, el proceso de actualización de firmware no actualiza el firmware para ese dispositivo

específico. En cambio, el proceso de actualización de firmware continúa actualizando el resto de dispositivos en el dispositivo y prosigue con la actualización de todos los demás dispositivos en el trabajo de actualización de firmware actual.

- **Ir al siguiente sistema en caso de error**. Si se produce un error al actualizar alguno de los dispositivos del dispositivo, el proceso de actualización de firmware detiene todos los intentos de actualizar el firmware para ese dispositivo específico, de modo que el firmware actual que está instalado en dicho dispositivo continúa siendo efectivo. El proceso de actualización de firmware sigue actualizando todos los demás dispositivos del trabajo de actualización de firmware actual.

Nota: Cuando está habilitada, la opción de arranque de Wake on LAN puede interferir con las operaciones de XClarity Administrator que apaga el servidor, incluyendo las actualizaciones de firmware si hay un cliente Wake on LAN en su red que emita comandos “Wake on Magic Packet”

Paso 7. Seleccione una de las siguientes reglas de activación:

- **Activación inmediata**. Durante el proceso de actualización, el dispositivo se puede reiniciar automáticamente varias veces hasta que se complete el proceso de actualización. Asegúrese de poner en modo de inactividad todas las aplicaciones en el dispositivo antes de continuar.
- **Activación con retardo**. Se realizan algunas de las operaciones de actualización, pero no todas ellas. Los dispositivos se deben reiniciar para continuar con el proceso de actualización. Se realizan reinicios adicionales hasta que se completa la operación de actualización.

  Cuando el estado cambia a **modo de mantenimiento de firmware pendiente**, se produce un suceso para notificarle cuando se debe reiniciar el servidor.

  Si un dispositivo se reinicia por cualquier motivo, el proceso de actualización con retardo finaliza.

  Esta regla de activación solo se admite para servidores y conmutadores de bastidor. Los CMM y los conmutadores Flex se activan de inmediato, independientemente de esta configuración.

  Cuando el estado cambia a **modo de mantenimiento de firmware pendiente**, se produce un suceso para notificarle cuando se debe reiniciar el servidor.

  El proceso de actualización con retardo finaliza cuando el dispositivo se reinicia por cualquier motivo (incluido un reinicio manual). No hay un límite de tiempo para cuando se debe reiniciar el servidor.

  XClarity Administrator puede aplicar actualizaciones con activación con retardo para un máximo de 50 dispositivos a la vez. Si intenta aplicar actualizaciones con activación con retardo para más de 50 dispositivos, los dispositivos restantes se ponen en cola. Un dispositivo sale de la cola cuando el dispositivo que se está actualizando se coloca en el **estado Modo de mantenimiento de firmware pendiente.**

  Importante:

  – Si XClarity Administrator se reinicia durante el trabajo de actualización, este se detendrá con un error.

  – Si un servidor en el estado **Modo de mantenimiento de firmware pendiente** se reinicia mientras XClarity Administrator está desactivado o no se puede acceder a él, el servidor arranca en la BMU; sin embargo, debido a que XClarity Administrator no puede conectarse a la BMU y supera el tiempo de espera después de 60 segundos, el controlador de gestión de la placa base restablece el estado de alimentación del sistema (se apaga si estaba apagado, se reinicia si estaba encendido).
- **Activación con prioridades**. Las actualizaciones se activan de inmediato en el controlador de gestión de placa base; todas las demás actualizaciones de firmware se activan la próxima vez

que se reinicia el dispositivo. Se realizan reinicios adicionales hasta que se completa la operación de actualización. Esta regla solamente se admite para servidores.

Se produce un suceso cuando el estado cambia a modo de mantenimiento de firmware pendiente para notificarlo cuando se debe reiniciar el servidor.

Nota: Cuando está habilitada, la opción de arranque de Wake on LAN puede interferir con las operaciones de XClarity Administrator que apaga el servidor, incluyendo las actualizaciones de firmware si hay un cliente Wake on LAN en su red que emita comandos “Wake on Magic Packet”

Paso 8. **Opcional:** seleccione **Forzar la actualización** para actualizar el firmware en los componentes seleccionados aun cuando el nivel de firmware esté actualizado o para aplicar una actualización de firmware más reciente que la instalada actualmente en los componentes seleccionados.

Nota: Puede aplicar versiones de firmware más recientes a las opciones, los adaptadores y las unidades del dispositivo que admiten versiones anteriores. Consulte la documentación del hardware para determinar si se admiten versiones anteriores.

Paso 9. **Opcional:** borrar **el firmware de requisitos previos de instalación** si no desea instalar el firmware de requisitos previos. El firmware de requisitos previos está instalado de manera predeterminada.

Nota: Cuando utiliza **Activación con retardo** o **Activación con prioridad** para requisitos previos para actualizaciones de firmware, es posible que deba reiniciar el servidor para activar el firmware de requisito previo. Después del reinicio inicial, las demás actualizaciones de firmware se instalan mediante **Activación inmediata**.

Paso 10. **Opcional:** si seleccionó **Activación inmediata**, seleccione **Prueba de memoria** para ejecutar una prueba de memoria después de que la actualización de firmware se complete, si el servidor se reinicia durante la actualización.

Esta opción es compatible con los servidores ThinkSystem v1 y v2 (excepto servidores ThinkSystem SR635, SR645, SR655 y SR665).

Paso 11. Haga clic en **Realizar actualización** para actualizar de inmediato, o bien haga clic en **Programación** planificar que esta actualización se ejecute posteriormente.

Si es necesario, puede realizar acciones de alimentación en los dispositivos gestionados. Las acciones de alimentación son útiles cuando se selecciona **Activación con retardo** y desea que las actualizaciones continúen cuando el dispositivo está en espera en el estado de “Mantenimiento pendiente”. Para realizar una acción de alimentación en un dispositivo gestionado desde esta página, haga clic en **Todas las acciones → Acciones de alimentación** y, luego, haga clic en una de las siguientes acciones de alimentación.

- **Encender**
- **Apagar el SO y apagar**
- **Apagar**
- **Apagar el SO y reiniciar**
- **Reiniciar**

Después de finalizar

Si el servidor no logra iniciar el modo de mantenimiento cuando se aplica una actualización de firmware, intente volver a aplicar la actualización.

Si las actualizaciones no se han completado correctamente, consulte Problemas relacionados con el repositorio y la actualización de firmware en la documentación en línea de XClarity Administrator para saber cómo resolver problemas y aplicar acciones correctivas.

En la página Actualizaciones de firmware: Aplicar/Activar, puede realizar las siguientes acciones:

- Exportar firmware e información de cumplimiento para cada dispositivo gestionado pulsando **Todas las acciones → Exportar vista como CSV**.

  Nota: El archivo CSV solo contiene información filtrada en la vista actual. No se incluye la información que se filtra fuera de la descripción y la información en columnas ocultas.
- Cancelar una actualización que se está aplicando a un dispositivo, seleccionando el dispositivo y pulsando el icono **Cancelar actualización** ( ).

  Nota: Puede cancelar las actualizaciones de firmware que están en espera para comenzar. Una vez comienza el proceso de actualización, solo se puede cancelar cuando el proceso de actualización realiza una tarea que no sea aplicar la actualización, por ejemplo, cambiar al modo de mantenimiento o reiniciar el dispositivo.
- Ver el estado de la actualización de firmware directamente en la columna **Estado** de la página Aplicar/Activar.
- Supervisar el estado del proceso de actualización desde el registro de trabajos. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Supervisión → Trabajos**.

  Para obtener más información acerca del registro de trabajos, consulte Supervisión de trabajos.

Cuando los trabajos de actualización del firmware se hayan completado, puede verificar que los dispositivos cumplen con los estándares haciendo clic en **Aprovisionamiento → Actualizaciones de firmware: Aplicar/Activar** para volver a la página Actualizaciones de firmware: Aplicar/Activar y luego pulsando el icono **Actualizar** ( ). La versión actual del hardware que está activa en cada dispositivo aparece en la columna **Versión instalada**.

Capítulo 14. Actualización de los controladores de dispositivos de Windows en servidores gestionados

Utilizando Windows UpdateXpress System Packs (UXSPs), puede actualizar controladores de dispositivos de SO en sistemas operativos Windows desplegados.

Antes de empezar

Debe tener autoridad de **lxc-os-admin**, **lxc-supervisor**, **lxc-admin** o **lxc-hw-admin** para gestionar y desplegar controladores de dispositivos de SO y realizar acciones avanzadas en servidores gestionados desde las páginas de Actualización del controlador Windows.

La actualización del firmware y de los controladores de dispositivo son procesos independientes en XClarity Administrator; no existe una conexión entre estos procesos. XClarity Administrator no mantiene la conformidad entre el firmware y los controladores de dispositivos en dispositivos gestionados, aunque se recomienda actualizar los controladores de dispositivo al mismo tiempo que el firmware.

Acerca de esta tarea

Windows UpdateXpress System Packs (UXSPs) contiene los controladores de dispositivos Windows para las versiones de Windows compatibles y los servidores de Lenovo compatibles con Windows.

Solo se admiten los controladores de dispositivos para Windows Server 2012 R2 y versiones posteriores. XClarity Administrator no admite la actualización de controladores de dispositivos Linux o VMware.

Para obtener información acerca de cómo instalar controladores de dispositivos al implementar sistemas operativos, consulte Instalación de sistemas operativos en servidores sin sistema operativo.

Procedimiento

Paso 1. **Configuración del servidor de Windows para actualizaciones del controlador de dispositivo del SO**

Lenovo XClarity Administrator utiliza el servicio de gestión remota de Windows (WinRM) escuchando sobre HTTPS o HTTP para ejecutar los comandos de actualización de controladores de dispositivos en los sistemas de Windows de destino. El servicio WinRM debe configurarse correctamente en los servidores de destino antes de intentar actualizar los controladores de dispositivo de SO (consulte Configuración del servidor de Windows para actualizaciones del controlador de dispositivo del SO).

Paso 2. **Gestionar el repositorio de controladores de dispositivos del SO**

El *repositorio de controladores de dispositivos del SO* contiene un catálogo de controladores de dispositivos de Windows disponibles y los paquetes de controladores de dispositivos que se pueden aplicar a los dispositivos gestionados.

El *catálogo* contiene información acerca de los UpdateXpress System Packs (UXSPs) de Windows y las actualizaciones de controladores de dispositivos que están disponibles para todos los servidores Lenovo compatibles con Windows. El catálogo organiza las actualizaciones de controladores de dispositivos por tipo de dispositivo. Cuando actualiza el catálogo, XClarity Administrator recupera información acerca de las UXSP disponibles desde Sitio web del Soporte del Centro de Datos de Lenovo (incluidos el archivo .xml de metadatos y el archivo .txt de Léame) y almacena la información en el repositorio. No se descarga el archivo de carga útil (.exe). Para

obtener más información sobre actualizar el catálogo, consulte Actualización del catálogo de controladores de dispositivos del SO.

Puede descargar o importar los UXSP de Windows en el repositorio. Los UXSP de Windows contiene los controladores de dispositivos Windows para las versiones de Windows compatibles y los servidores de Lenovo compatibles con Windows. Los UXSP deben estar disponibles en el repositorio antes de poder actualizar los controladores de dispositivos de Windows en los servidores gestionados. Para obtener más información sobre cómo descargar controladores de dispositivos, consulte Descarga de controladores de dispositivos de Windows .

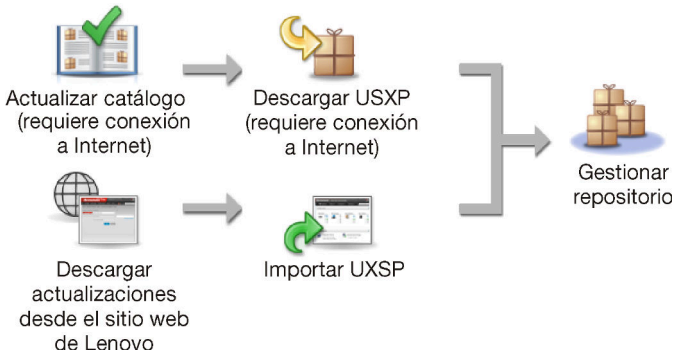
Puede determinar si los UXSP están almacenados en el repositorio de controladores de dispositivos de SO desde la columna Estado de descarga en la pestaña Actualizaciones individuales en la página de Repositorio de actualizaciones de controladores de Windows. Esta columna contiene los siguientes valores.

- **Descargado**. El paquete completo o cada actualización se almacenan en el repositorio.
- ***x* de *y* descargado**. Algunas de las actualizaciones del paquete se almacenan en el repositorio, pero no todas. Los números entre paréntesis indican el número de actualizaciones disponibles y el número de actualizaciones almacenadas, o no hay actualizaciones para el tipo de dispositivo específico.
- **No descargado**. El paquete completo o la actualización individual no se almacenan en el repositorio.

Nota: Cuando descarga o importa UXSP desde la página Actualizaciones de controladores de dispositivo: Repositorio, solo se descargan los controladores de dispositivo y se almacenan en el repositorio. Las actualizaciones de firmware se descartan. Para obtener información acerca de cómo descargar o importar actualizaciones de firmware, consulte la sección Gestión del repositorio de actualizaciones de firmware.

XClarity Administrator debe estar conectado a Internet para actualizar el catálogo y descargar UXSP. Si no está conectado a Internet, puede descargar manualmente el UXSP a una estación de trabajo que disponga de acceso de red para el host XClarity Administrator utilizando un navegador web. Esta descarga de UXSP es un archivo de formato de archivo zip y contiene todos los archivos de controlador de dispositivos requeridos para el UXSP, incluidos los de carga útil (.exe), metadatos (.xml), de historial de cambios (.chg) y los archivos Léame (.txt).

Nota: Puede ver los mensajes de que los archivos de firmware (fw) no son necesarios y se eliminaron. Esto es normal porque los controladores de dispositivos de Windows solo se actualizan mediante este proceso.



Atención:

- No descomprima el UXSP antes de importarlo.

- Windows UXSP incluye los controladores de los dispositivos y las actualizaciones de firmware. Las actualizaciones de firmware en Windows UXSP se descartan cuando se importan los UXSP al repositorio y se muestra un mensaje de advertencia. Solo se importan los controladores de dispositivos.

Paso 3. **Aplicar controladores de dispositivos de SO**

XClarity Administrator no actualizar los controladores de dispositivos automáticamente a los servidores gestionados. Para actualizar los controladores de dispositivos, debe aplicar y activar manualmente los controladores de dispositivos en los servidores seleccionados.

Atención: Antes de intentar actualizar los controladores de dispositivos en los servidores gestionados, asegúrese de haber revisado las siguientes consideraciones y haber completado todas las acciones de requisitos previos aplicables.

- No se puede seleccionar los dispositivos que no se admiten actualizaciones.
- Antes de intentar actualizar los controladores de dispositivos en los servidores gestionados, lea las consideraciones sobre la actualización de controladores de dispositivos (consulte Consideraciones sobre la actualización de controladores de dispositivos de SO).
- Asegúrese de que el repositorio contenga los UXSP y controladores de dispositivos que desea desplegar (consulte Descarga de controladores de dispositivos de Windows).

  Nota: Cuando XClarity Administrator se instala por primera vez, el catálogo y el repositorio están vacíos.
- XClarity Administrator puede utilizar el servicio de gestión remota de Windows (WinRM) escuchando sobre HTTPS o HTTP para ejecutar los comandos de actualización de controladores de dispositivos en los sistemas de Windows de destino. HTTPS es el valor predeterminado. Para utilizar HTTP, haga clic en **Todas las acciones → Valores globales** en las actualizaciones de controlador de Windows: página Aplicar y luego borre **Utilizar HTTPS para actualizaciones de controlador de Windows**.

  Atención: Cuando utiliza HTTP, las credenciales de usuario de Windows se envían a través de la red de usuario *sin* cifrado y se pueden ver fácilmente utilizando herramientas de resolución de problemas de red comúnmente disponibles.

  Importante:

  – Asegúrese de que la gestión remota de Windows (WinRM) en el servidor de destino esté configurada para usar el mismo valor (HTTPS o HTTP) que se define en XClarity Administrator (consulte Configuración del servidor de Windows para actualizaciones del controlador de dispositivo del SO).

  – Asegúrese de que WinRM en el servidor de destino esté configurado con autenticación básica.

  – Cuando utiliza HTTPS, asegúrese de que WinRM en el servidor de destino esté configurado con **allowUnencrypted=false**.
- Asegúrese de que PowerShell sea compatible con el servidor de destino.
- Asegúrese de que el servidor de destino esté encendido antes de intentar actualizar a controladores de dispositivo. Si el servidor no está encendido, seleccione el servidor de destino y haga clic en **Todas las acciones → Acciones de alimentación → Encender**.
- Asegúrese de que XClarity Administrator tenga la información que necesita acceder al sistema operativo del host (consulte Gestión de acceso a los sistemas operativos en servidores gestionados.

- Si desea utilizar una cuenta de dominio al actualizar los controladores de dispositivos del SO, asegúrese de que creó el archivo de configuración necesario (consulte Configuración de una cuenta de dominio para actualizaciones de controladores de dispositivo del SO).
- Asegúrese de que no haya trabajos que se encuentren en ejecución en la actualidad en el servidor de destino. No puede actualizar los controladores de dispositivos en un servidor gestionado que esté bloqueado por un trabajo en ejecución. Si está ejecutando otro trabajo de actualización del servidor de destino, el trabajo de actualización queda en espera hasta que se completa el trabajo de actualización actual. Para ver una lista de los trabajos activos, haga clic en **Supervisión → Trabajos**.

Para obtener más información sobre cómo actualizar los controladores de dispositivos, consulte Aplicar controladores de dispositivos de Windows.

Consideraciones sobre la actualización de controladores de dispositivos de SO

Antes de empezar a actualizar los controladores de dispositivo de SO para los dispositivos gestionados utilizando Lenovo XClarity Administrator, tenga en cuenta las siguientes consideraciones importantes.

Nota: Debe tener autoridad de **lxc-os-admin**, **lxc-supervisor**, **lxc-admin** o **lxc-hw-admin** para gestionar y desplegar controladores de dispositivos y realizar acciones avanzadas en servidores gestionados desde las páginas de Actualización del controlador Windows.

Consideraciones de red

- Los puertos y direcciones de Internet requeridos deben estar disponibles antes de que intente descargar UpdateXpress System Packs (UXSPs). Para obtener más información, consulte Disponibilidad de puertos y Firewall y servidores proxy en la XClarity Administrator documentación en línea.
- XClarity Administrator debe tener acceso a la red de gestión y de datos para acceder al sistema operativo.
- XClarity Administrator debe poder comunicarse con el servidor de destino (tanto con el controlador de gestión de placa base como la red de datos del servidor) por la interfaz de red (Eth0 o Eth1) seleccionada al configurar el acceso de red de XClarity Administrator y que la interfaz esté configurada con una dirección IPv4 o una dirección ULA automática IPv6.

  Para especificar una interfaz que se debe utilizar para el despliegue del sistema operativo, consulte Configuración del acceso de red).

  Para obtener más información acerca de la red y de las interfaces de despliegue del sistema operativo, consulte Consideraciones de red en la documentación en línea de XClarity Administrator.
- Las direcciones de IP deben ser únicas para el sistema operativo del host.
- XClarity Administrator puede utilizar el servicio de gestión remota de Windows (WinRM) escuchando sobre HTTPS o HTTP para ejecutar los comandos de actualización de controladores de dispositivos en los sistemas de Windows de destino. HTTPS es el valor predeterminado. Para utilizar HTTP, haga clic en **Todas las acciones → Valores globales** en las actualizaciones de controlador de Windows: página Aplicar y luego borre **Utilizar HTTPS para actualizaciones de controlador de Windows**.

  Atención: Cuando utiliza HTTP, las credenciales de usuario de Windows se envían a través de la red de usuario *sin* cifrado y se pueden ver fácilmente utilizando herramientas de resolución de problemas de red comúnmente disponibles.

Consideraciones de dispositivo gestionado

- Los controladores de dispositivos de Windows no son compatibles con los servidores ThinkAgile, ThinkSystem SR635 y ThinkSystemSR655.
- Solo se admiten los servidores ThinkSystem, Lenovo System x y Lenovo Flex System.

- XClarity Administrator no valida la relación entre el controlador de gestión y el sistema operativo. El controlador de gestión de la placa base se utiliza para encender o apagar el servidor.
- Asegúrese de que la interfaz sobre USB del LAN esté habilitada. Se utiliza la LAN sobre USB al actualizar los controladores de dispositivos del SO.

Consideraciones de controladores de dispositivos y sistemas operativos

- Puede actualizar los controladores de dispositivos para los siguientes sistemas operativos.
  - Windows Server 2012 R2
  - Windows Server 2016
  - Windows Server 2019

  Nota: XClarity Administrator se prueba solo con versiones de Windows que son compatibles con Microsoft al momento del lanzamiento de la versión XClarity Administrator.
- La gestión remota de Windows (WinRM) se debe configurar para HTTPS en el servidor de destino (consulte Configuración del servidor de Windows para actualizaciones del controlador de dispositivo del SO).
- PowerShell debe ser compatible con el servidor de destino.
- Debe proporcionar la información que se necesita para acceder al sistema operativo del host del servidor de destino, incluida la dirección IP del sistema operativo y las credenciales (consulte Gestión de acceso a los sistemas operativos en servidores gestionados). Debe indicar las credenciales de una cuenta de usuario con autoridad de administrador.
- XClarity Administrator solo actualiza los controladores de dispositivos que no están en conformidad. Los controladores de dispositivos que no están en conformidad cuando la versión en el servidor es anterior a la versión UXSP. Los controladores de dispositivos que son iguales o posteriores a la versión en el UXSP seleccionado se omiten.
- El cumplimiento de controlador de dispositivo solo es preciso cuando el hardware está presente. Si el hardware no está presente, los controladores de dispositivos se aplican igualmente al servidor. Cuando se agrega el hardware faltante al servidor, Windows carga la última versión.
- Los servidores System x no admiten algunos controladores de dispositivos predefinidos que vienen con XClarity Administrator. Para desplegar controladores de dispositivos en estos servidores, cree un perfil personalizado que incluya solo los controladores de dispositivos necesarios.

Gestión del repositorio de controladores de dispositivos del SO

El *repositorio de controladores de dispositivos del SO* incluye el catálogo y los controladores de dispositivos de Windows descargados.

Acerca de esta tarea

El *catálogo* contiene información acerca de los UpdateXpress System Packs (UXSPs) de Windows y las actualizaciones de controladores de dispositivos que están disponibles para todos los servidores Lenovo compatibles con Windows. El catálogo organiza las actualizaciones de controladores de dispositivos por tipo de dispositivo. Cuando actualiza el catálogo, XClarity Administrator recupera información acerca de las UXSP disponibles desde Sitio web del Soporte del Centro de Datos de Lenovo (incluidos el archivo .xml de metadatos y el archivo .txt de Léame) y almacena la información en el repositorio. No se descarga el archivo de carga útil (.exe). Para obtener más información sobre actualizar el catálogo, consulte Actualización del catálogo de controladores de dispositivos del SO.

Windows UpdateXpress System Packs (UXSPs) contiene los controladores de dispositivos Windows para las versiones de Windows compatibles y los servidores de Lenovo compatibles con Windows. Puede descargar o importar los UXSP de Windows en el repositorio. Los UXSP de Windows contiene los controladores de dispositivos Windows para las versiones de Windows compatibles y los servidores de

Lenovo compatibles con Windows. Los UXSP deben estar disponibles en el repositorio antes de poder actualizar los controladores de dispositivos de Windows en los servidores gestionados.Para obtener más información sobre cómo descargar controladores de dispositivos, consulte Descarga de controladores de dispositivos de Windows .

XClarity Administrator debe estar conectado a Internet para actualizar el catálogo y descargar UXSP. Si no está conectado a Internet, puede descargar manualmente el UXSP a una estación de trabajo que disponga de acceso de red para el host XClarity Administrator utilizando un navegador web. Esta descarga de UXSP es un archivo de formato de archivo zip y contiene todos los archivos de controlador de dispositivos requeridos para el UXSP, incluidos los de carga útil (.exe), metadatos (.xml), de historial de cambios (.chg) y los archivos Léame (.txt).

Después de que se descargue un UXSP en el repositorio, se agrega información acerca de los controladores de dispositivos en el paquete a la página Repositorio de actualizaciones de controladores de Windows. Esto incluye la fecha de publicación, el tamaño y la gravedad. La gravedad indica el impacto y la necesidad de aplicar la actualización para ayudarle a evaluar en qué se puede ver afectado su entorno.

- **Versión inicial**. Esta es la primera versión del controlador de dispositivo.
- **Crítico**. El controlador de dispositivo contiene arreglos urgentes para problemas de corrupción de datos, seguridad o estabilidad.
- **Sugerido**. El controlador de dispositivo contiene arreglos importantes para problemas que posiblemente encuentre.
- **No crítico**. El controlador de dispositivo contiene arreglos menores, mejoras de rendimiento y cambios textuales.

Notas:

- La gravedad es relativa a la versión anterior del controlador de dispositivo. Por ejemplo, si el controlador de dispositivo instalado es v1.01 y la actualización v1.02 es crítica y se recomienda la actualización v1.03, esto significa que se recomienda la actualización desde 1.02 a 1.03, pero que la actualización de v1.01 a v1.03 es crítica porque es acumulativa (v1.03 incluye problemas críticos de v1.02).
- Pueden surgir casos especiales en los que una actualización puede ser únicamente crítica o recomendada para un tipo de equipo específico. Para obtener más información, consulte las Notas de la versión.

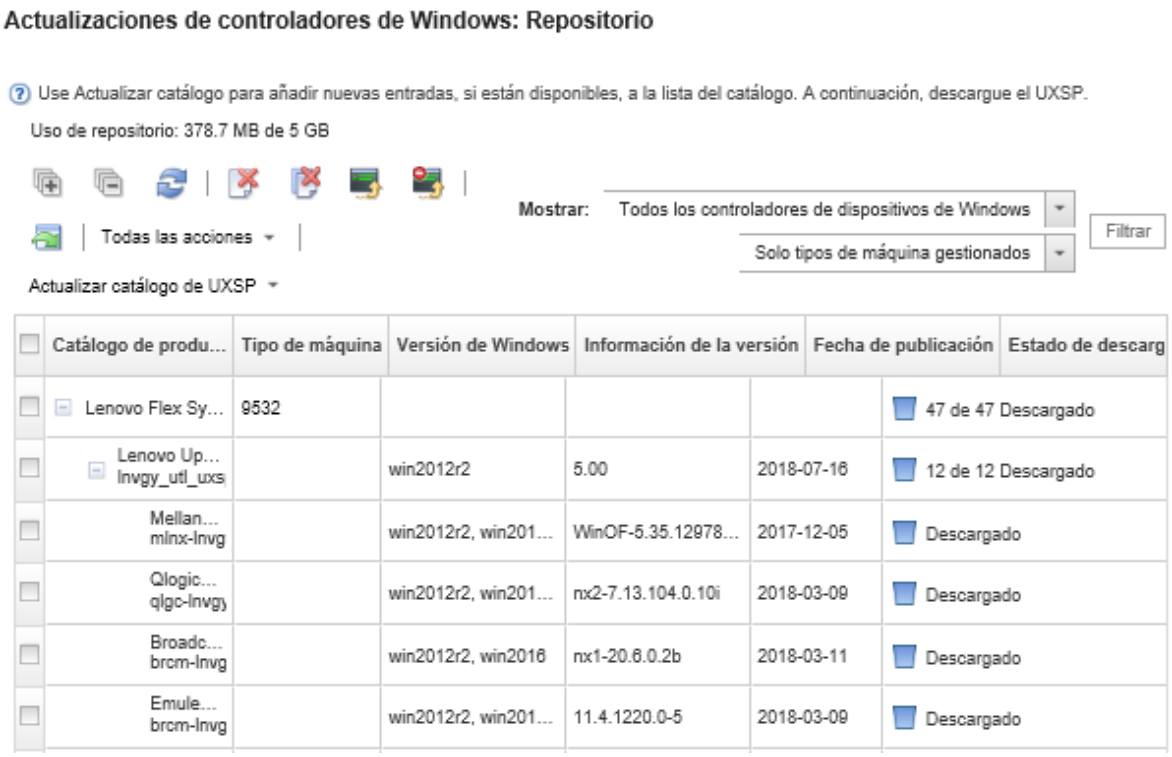
Procedimiento

Para ver las UXSP y controladores de dispositivos que están disponibles en el repositorio, lleve a cabo los pasos siguientes.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Actualizaciones de controladores de dispositivo: Repositorio**. Se muestra la página Repositorio de actualizaciones de controladores de Windows con una lista de UXSP disponibles, organizados por tipo de dispositivo.

Paso 2. Expanda un tipo de servidor y luego los UXSP que están disponibles para ese tipo de servidor para listar los controladores de dispositivos que están disponibles para ese tipo de servidor.

Puede ordenar las columnas de la tabla y haga clic en el icono **Expandir** todo ( ) y el icono **Contraer** todas ( ) para que sea más fácil encontrar los controladores de dispositivos específicos. Además, puede filtrar la lista de tipos de servidores y controladores de dispositivos que se muestran al seleccionar una opción en el menú **Mostrar** de modo que se enumeren solo los controladores de dispositivos de una específica edad, controladores de dispositivos para todos los tipos de servidor o solo aquellos de tipo servidor gestionado o aquello que se ingrese como texto en el campo **Filtro**.



Desde esta página puede llevar a cabo las siguientes acciones:

- Para recuperar la información más reciente sobre las UXSP disponibles, haga clic en **Actualizar catálogo**.

  La recuperación de esta información puede tardar varios minutos. Para obtener más información, consulte el apartado Actualización del catálogo de controladores de dispositivos del SO.
- Descargue UXSP y controladores de dispositivos XClarity Administrator actualizando el catálogo y haciendo clic en el icono **Descargar** ( ). Cuando las UXSP y los controladores de dispositivos se hayan descargado y agregado al repositorio, el estado cambia a “Descargado”.

  Para obtener más información sobre cómo descargar UXSP y controladores de dispositivos, consulte Descarga de controladores de dispositivos de Windows .
- Importación UXSP que descargo manualmente a una estación de trabajo desde la web o controladores de dispositivos que exportó desde XClarity Administrator (consulte Descarga de controladores de dispositivos de Windows).
- Para detener descargas que están en progreso actualmente, haga clic en el icono **Cancelar descargas** ( ).
- Para eliminar UXSP o controladores de dispositivos individuales desde el repositorio, haga clic en el icono **Eliminar** ( ).

Actualización del catálogo de controladores de dispositivos del SO

El catálogo de controladores de dispositivos de SO contiene información acerca de todos los controladores de Windows UpdateXpress System Packs (UXSPs) y de dispositivos que están disponibles para todos los servidores Lenovo compatibles con las actualizaciones de controladores de dispositivos de Windows.

Antes de empezar

Asegúrese de que Lenovo XClarity Administrator está conectado a Internet.

Acerca de esta tarea

Cuando actualiza el catálogo, XClarity Administrator recupera información acerca de las UXSP disponibles desde Sitio web del Soporte del Centro de Datos de Lenovo (incluidos el archivo .xml de metadatos y el archivo .txt de Léame) y almacena la información en el repositorio. No se descarga el archivo de carga útil (.exe). Debe descargar las cargas útiles de UXSP y controladores de dispositivos de SO antes de actualizar los controladores de dispositivos en los servidores gestionados. Para obtener más información sobre cómo descargar controladores de dispositivos, consulte Descarga de controladores de dispositivos de Windows .

Nota: La actualización del catálogo puede tardar varios minutos en finalizar.

Procedimiento

Para actualizar el catálogo, lleve a cabo los pasos siguientes.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Actualizaciones de controladores de Windows: Repositorio** para mostrar la página Actualizaciones de controladores de Windows: Repositorio.

Paso 2. Haga clic en **Actualizar catálogo** y luego haga clic en una de las siguientes opciones para obtener información sobre las últimas UXSP disponibles.

- **Actualizar selección - Solo reciente**. Permite recuperar información acerca de la versión más actual de las UXSP que están disponibles solo para los servidores seleccionados.
- **Actualizar todo - Solo reciente**. Recupera información acerca de las versiones más recientes de UXSP para todos los servidores compatibles.
- **Actualizar selección**. Permite recuperar información acerca de todas las versiones de las UXSP que están disponibles solo para los servidores seleccionados.
- **Actualizar todo**. Permite recuperar información acerca de todas las versiones de las UXSP que están disponibles para todos los servidores admitidos.

Paso 3. Haga clic en **Actualizar catálogo** para actualizar de inmediato, o bien haga clic en **Programación** planificar que esta actualización se ejecute posteriormente.

Descarga de controladores de dispositivos de Windows

Windows UpdateXpress System Packs (UXSPs) contiene los controladores de dispositivos Windows para las versiones de Windows compatibles y los servidores de Lenovo compatibles con Windows. Puede descargar o importar los UXSP de Windows en el repositorio. Los UXSP de Windows contiene los controladores de dispositivos Windows para las versiones de Windows compatibles y los servidores de Lenovo compatibles con Windows. Los UXSP deben estar disponibles en el repositorio antes de poder actualizar los controladores de dispositivos de Windows en los servidores gestionados.

Antes de empezar

Asegúrese de que todos los puertos y direcciones de Internet requeridos están disponibles antes de que intente descargar UpdateXpress System Packs (UXSPs). Para obtener más información, consulte Disponibilidad de puertos y Firewall y servidores proxy en la XClarity Administrator documentación en línea.

Para descargar UXSP utilizando XClarity Administrator, asegúrese de que XClarity Administrator esté conectado a Internet.

Los navegadores web Internet Explorer y Microsoft Edge tienen un límite de carga de 4 GB. Si el archivo que desea importar es mayor a 4 GB, considere usar otro navegador web (por ejemplo, Chrome o Firefox).

Acerca de esta tarea

XClarity Administrator debe estar conectado a Internet para actualizar el catálogo y descargar UXSP. Si XClarity Administrator no está conectado a Internet, puede descargar manualmente los archivos en una estación de trabajo que tenga acceso de red al host de XClarity Administrator utilizando un navegador web y luego importar las actualizaciones al repositorio de actualizaciones de firmware.

Puede determinar si UXSP se almacenan en el repositorio desde la columna **Estado de descarga** en la página de Repositorio de actualizaciones de controladores de Windows. Esta columna contiene los siguientes valores:

- **Descargado**. Todos los controladores de dispositivos en el UXSP o el controlador de dispositivo individual se descargan en el repositorio.
- *x* **de** *y* **descargado**. Algunos de los controladores de dispositivos del UXSP se descargan en el repositorio, pero no todas. Los números entre paréntesis indican el número de controladores de dispositivos disponibles y el número de descargas de controladores de dispositivos.
- **No descargado**. El UXSP o controlador de dispositivo individual está disponible en el sitio de soporte técnico de Lenovo, pero no se descarga en el repositorio.

Aparece un mensaje en la página repositorio de actualizaciones de controladores de Windows cuando el espacio que está disponible para UXSP y controladores de dispositivos está más de un 50 % lleno. Se muestra otro mensaje en la página cuando la capacidad de uso del repositorio está sobre el 85 por ciento. Para reducir el espacio utilizado en el repositorio, puede eliminar archivos en desuso seleccionando los archivos de destino y haciendo clic en el icono **Eliminar** ( ). Para obtener más información, consulte Gestión del espacio en el disco duro.

Atención: Windows UXSP incluye los controladores de los dispositivos y las actualizaciones de firmware. Las actualizaciones de firmware en Windows UXSP se descartan cuando se importan los UXSP al repositorio y se muestra un mensaje de advertencia. Solo se importan los controladores de dispositivos.

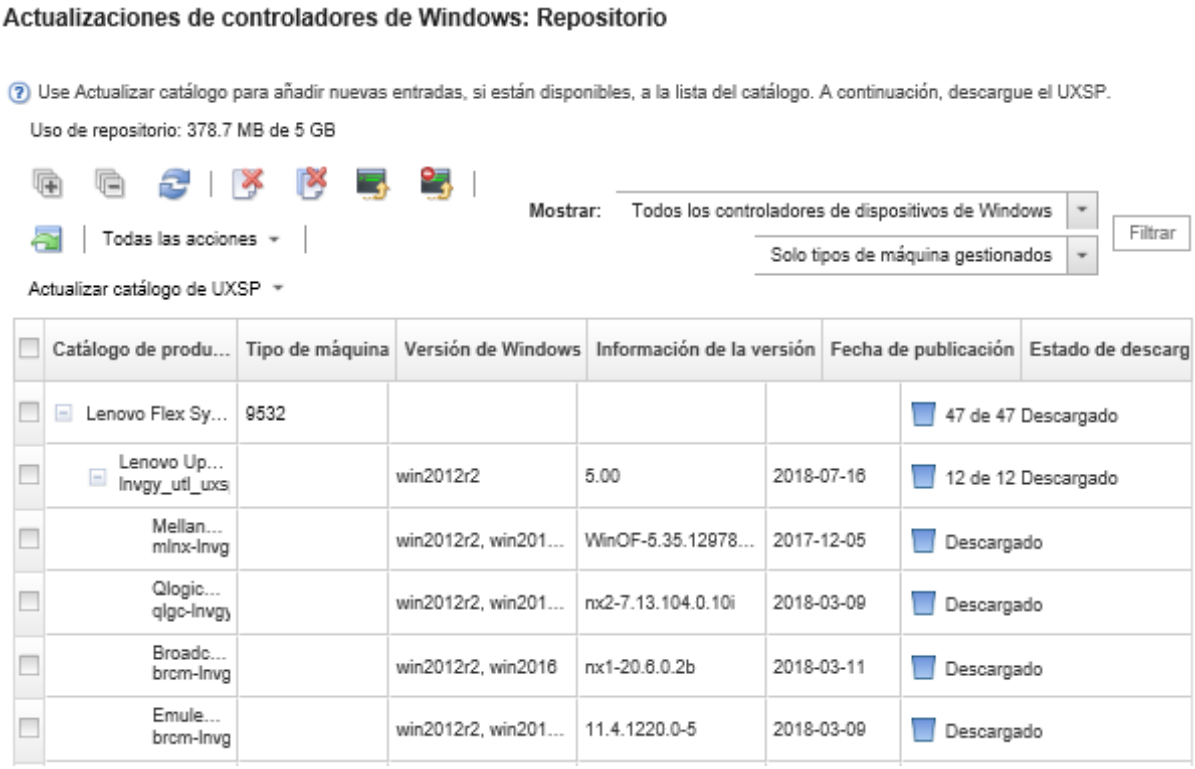
Procedimiento

Para descargar UXSP y los controladores de dispositivo específicos, lleve a cabo uno de los siguientes procedimientos.

- Cuando XClarity Administrator está conectado a Internet:
  1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Actualizaciones de controladores de Windows: Repositorio** para mostrar la página Actualizaciones de controladores de Windows: Repositorio.
  2. Haga clic en **Actualizar catálogo** y luego haga clic en una de las siguientes opciones para obtener información sobre las últimas UXSP disponibles.
     - **Actualizar selección - Solo reciente**. Permite recuperar información acerca de la versión más actual de las UXSP que están disponibles solo para los servidores seleccionados.
     - **Actualizar todo - Solo reciente**. Recupera información acerca de las versiones más recientes de UXSP para todos los servidores compatibles.
     - **Actualizar selección**. Permite recuperar información acerca de todas las versiones de las UXSP que están disponibles solo para los servidores seleccionados.
     - **Actualizar todo**. Permite recuperar información acerca de todas las versiones de las UXSP que están disponibles para todos los servidores admitidos.

     Nota: La actualización del catálogo puede tardar varios minutos en finalizar.

3. Expanda el tipo de servidor para mostrar la lista de UXSP disponibles. Expanda el UXSP para ver una lista de controladores de dispositivo disponibles.



4. Seleccione uno o más UXSP y servidores de destino para descargar.
5. Haga clic en el icono **Descargar selección** ( ).
6. Haga clic en **Descargar** para descargar de inmediato, o bien haga clic en **Programación** planificar que esta descarga se ejecute posteriormente.

   La descarga de las UXSP pueden tardar algunos minutos. Cuando las UXSP y controladores de dispositivos se hayan descargado y almacenado en el repositorio, la fila del catálogo de productos se resalta y la columna **Estado de descarga** cambia a “Descargado”.

   Puede supervisar el estado del proceso de descarga desde el registro de trabajos. En la barra de menús de XClarity Administrator, haga clic en **Supervisión → Trabajos**. Para obtener más información acerca del registro de trabajos, consulte Supervisión de trabajos.

- Cuando XClarity Administrator *no* está conectado a Internet:
  1. Descargue la UXSP en una estación de trabajo que tenga conexión de red con el host de XClarity Administrator desde el Sitio web del Soporte del Centro de Datos de Lenovo.
  2. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Actualizaciones de controladores de Windows: Repositorio** para mostrar la página Actualizaciones de controladores de Windows: Repositorio.
  3. Haga clic en el icono **Importar** ( ).
  4. Haga clic en **Seleccionar archivos** y desplácese hasta la ubicación de la UXSP en la estación de trabajo.
  5. Seleccione el archivo UXSP .zip (descomprima el archivo zip antes de importar) y luego haga clic en **Abrir**.

El archivo .zip UXSP que contiene el archivo de metadatos (.xml), carga útil (.exe), el archivo de historial de cambios (.chg) y el archivo Léame (.txt).

6. Haga clic en **Importar**.

   Puede supervisar el estado del proceso de importación desde el registro de trabajos. En la barra de menús de XClarity Administrator, haga clic en **Supervisión → Trabajos**. Para obtener más información acerca del registro de trabajos, consulte Supervisión de trabajos.

Después de finalizar

Desde esta página puede realizar las acciones siguientes en los UXSP seleccionados.

- Para cancelar una descarga que está en proceso actualmente, haga clic en el icono **Cancelar descarga** ( ).
- Para eliminar todos los archivos asociados con el UXSP, haga clic en el icono **Eliminar** ( ).

Configuración del servidor de Windows para actualizaciones del controlador de dispositivo del SO

Lenovo XClarity Administrator utiliza el servicio de gestión remota de Windows (WinRM) escuchando sobre HTTPS o HTTP para ejecutar los comandos de actualización de controladores de dispositivos en los sistemas de Windows de destino. El servicio WinRM debe configurarse correctamente en los servidores de destino antes de intentar actualizar los controladores de dispositivo de SO.

Antes de empezar

Los puertos requeridos deben estar disponibles. Para obtener más información, consulte Disponibilidad de puertos en la documentación en línea de XClarity Administrator.

Para obtener más información sobre la configuración de Windows Server antes de actualizar el controlador de dispositivo del SO, consulte XClarity Administrator: preparación para las actualizaciones del controlador de dispositivo del SO (documentación técnica).

Procedimiento

Para configurar el servidor de Windows para admitir la actualización de los controladores de dispositivos de SO, lleve a cabo los siguientes pasos.

- **Para HTTPS**
  1. Inicie sesión e instale un certificado de servidor en cada uno de los sistemas Windows de destino.

     Importante: El certificado debe contener la siguiente información.

     – En el Tema, asegúrese de que el componente de dominio esté definido (por ejemplo, DC=labs, DC=com, DC=company).

     – En el Nombre alternativo de asunto, asegúrese de que el nombre de DNS y la dirección IP del host estén definidos (por ejemplo, el nombre de DNS=node1325C554A6F.labs.company.com y la dirección IP=10.245.43.149).

  2. Configure los datos y los comandos de gestión remota a través de una conexión HTTPS ejecutando uno de los siguientes comandos desde un indicador de comandos de administración y luego confirme los cambios de configuración sugeridos.

     –

     ```
     winrm quickconfig -transport:https
     ```

–

```
winrm create winrm/config/Listener?Address=*+Transport=HTTPS
@{Hostname="host_name";CertificateThumbprint="certificate_thumbprint"}
```

Para configurar manualmente un oyente HTTPS WinRM según la documentación WinRM, consulte el Cómo configurar WinRM para la página Web HTTPS.

3. Habilite la autenticación básica de usuarios locales de Windows, ejecute el siguiente comando desde un indicador de comando de administración.
   ```
   winrm set winrm/config/service/Auth @{Basic="true"}
   ```
4. Para evitar un posible tiempo de espera y enviar errores de solicitud de WinRM en la comprobación de conformidad y la realización de actualizaciones de controladores, aumente el valor predeterminado del tiempo de espera de respuesta de WinRM ejecutando el siguiente comando desde un indicador de comando administrativo. Se recomienda un valor de 280000. Para obtener más información, consulte el Página Web de instalación y configuración de gestión remota de Windows
   ```
   winrm set winrm/config @{MaxTimeoutms="280000"}
   ```
5. Abra el puerto en su firewall que configuró para la escucha WinRM HTTPS. El puerto HTTPS predeterminado es 5986. Por ejemplo
   ```
   netsh advfirewall firewall add rule name="Windows Remote Management (HTTPS-In)" dir=in action=allow
   protocol=TCP localport=5986
   ```
6. Si está utilizando la escucha HTTPS, agregue el certificado al almacén de confianza de XClarity Administrator llevando a cabo los pasos siguientes. Agregar el certificado al almacén de confianza permite a XClarity Administrator confiar en la escucha WinRM HTTPS a la que se conecta. Repita los siguientes pasos para las rutas de certificación adicionales que deben ser de confianza para el servicio de Gestión remota de Windows.
   a. Identifique y recopile el certificado raíz de la entidad de certificación que utiliza para firmar los certificados de servidor para los sistemas de Windows de destino. Si no tiene acceso al certificado raíz de la CA, recopile el certificado de servidor propio u otro certificado en la ruta de certificación.
   b. En la barra de menús de XClarity Administrator, haga clic en **Administración → Seguridad** para mostrar la página Seguridad.
   c. Haga clic en **Certificados de confianza** en la sección Gestión de certificados.
   d. Haga clic en el icono **Crear** ( ) para mostrar el cuadro de diálogo Agregar certificado.
   e. Busque el archivo de certificado que recopiló en el paso 1 o copie/pegue el contenido del archivo de certificado en el cuadro de texto.
   f. Haga clic en **Crear**.
7. Después de que la escucha WinRM se esté ejecutando en los sistemas Windows de destino, XClarity Administrator puede conectarse a los sistemas y realizar las actualizaciones de controladores de dispositivo.

- **Para HTTP**
  1. Configure los datos y los comandos de gestión remota a través de una conexión HTTP ejecutando el siguiente comando desde un indicador de comandos de administración y luego confirme los cambios de configuración sugeridos.
     ```
     winrm quickconfig
     ```
  2. Habilite la autenticación básica de usuarios locales de Windows, ejecute el siguiente comando desde un indicador de comando de administración.
     ```
     winrm set winrm/config/service/Auth @{Basic="true"}
     ```
  3. Asigne la memoria suficiente para los comandos de actualización en el sistema ejecutando el siguiente comando desde un indicador de comando de administración.
     ```
     winrm set winrm/config/winrs @{MaxMemoryPerShellMB="1024"}
     ```

4. Permita datos no cifrados ejecutando el siguiente comando desde un indicador de comando de administración.
   ```
   winrm set winrm/config/service @{AllowUnencrypted="true"}
   ```
5. Abra el puerto en su firewall que configuró para el oyente WinRM HTTP. El puerto HTTPS predeterminado es 5985. Por ejemplo
   ```
   netsh advfirewall firewall add rule name="Windows Remote Management (HTTP-In)" dir=in action=allow
   protocol=TCP localport=5985
   ```

Después de que la escucha WinRM se esté ejecutando en los sistemas Windows de destino, XClarity Administrator puede conectarse a los sistemas y realizar las actualizaciones de controladores de dispositivo.

Configuración de una cuenta de dominio para actualizaciones de controladores de dispositivo del SO

Puede elegir usar las cuentas de dominio para gestionar fácilmente los privilegios con un controlador de dominio. Para utilizar una cuenta de dominio al actualizar los controladores de dispositivos del SO, tiene que configurar una cuenta de dominio.

Antes de empezar

Asegúrese de que los servidores de Windows gestionados estén en una red de dominio antes de configurar las cuentas de dominio.

Cuando agregue la cuenta de usuario de Windows en Lenovo XClarity Administrator, utilice el formato `USER@DOMAIN`. El formato `DOMAIN/USER` no es compatible.

Procedimiento

Para configurar una cuenta de dominio, lleve a cabo los pasos siguientes.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Aprovisionamiento → Actualizaciones de controlador de Windows: Aplicar**. Se muestra la página Actualizaciones de controlador de Windows: Aplicar.

Paso 2. Haga clic en **Todas las acciones → Gestionar cuenta de dominio**. Se muestra la página Cuentas de dominio.

Paso 3. Haga clic en el icono **Crear** ( ). Para añadir un ámbito para la cuenta de dominio. Se muestra el cuadro de diálogo Crear ámbito.

Paso 4. Especifique un nombre y uno o varios nombres de hosts del centro de distribución de claves para el ámbito. Utilice el icono **Añadir** ( ) para añadir otro nombre de host y utilice el icono **Quitar** ( ) para quitar un nombre de host.

Paso 5. Haga clic en **Aceptar** para guardar el ámbito.

Paso 6. En la página Cuentas de dominio, seleccione opcionalmente el lugar donde se usará de manera predeterminada.

Paso 7. Haga clic en **Guardar** para guardar la configuración.

Después de finalizar

Puede realizar las siguientes acciones desde la página Configurar cuenta de dominio.

- Modifique un ámbito seleccionado haciendo clic en el icono **Editar** ( ).
- Elimine un ámbito seleccionado haciendo clic en el icono de **Eliminar** ( ).

Configuración de valores de actualización de controlador de dispositivo Windows global

Valores globales se utilizan como valores predeterminados cuando se aplican las actualizaciones de controlador de dispositivo de Windows.

Acerca de esta tarea

En la página Valores globales, puede configurar los siguientes valores:
- Use HTTPS para las actualizaciones de controlador de Windows
- Mostrar controladores de dispositivo para el hardware instalado

Procedimiento

Para configurar los valores globales que se utilizarán en todos los servidores, lleve a cabo los pasos siguientes.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Aprovisionamiento → Actualizaciones de controlador de Windows: Aplicar**. Se muestra la página Actualizaciones de controlador de Windows: Aplicar.

Paso 2. Haga clic en **Todas las acciones → Valores globales** para mostrar el cuadro de diálogo Valores globales: Aplicar actualizaciones de controlador de Windows.

Paso 3. Opcionalmente, seleccione una de las siguientes opciones.

- Seleccione **Utilizar HTTPS para actualizaciones de controlador de Windows** para utilizar el servicio de gestión remota de Windows (WinRM) escuchando sobre HTTPS para ejecutar los comandos de actualización de controladores de dispositivos en los sistemas de Windows de destino. HTTPS es el valor predeterminado.

  Borre este valor para utilizar HTTP.

  Atención: Cuando utiliza HTTP, las credenciales de usuario de Windows se envían a través de la red de usuario *sin* cifrado y se pueden ver fácilmente utilizando herramientas de resolución de problemas de red comúnmente disponibles.
- Seleccione **Mostrar controladores de dispositivos para el hardware instalado** para enumerar solo los controladores de dispositivo para el hardware gestionado.

  Si desactiva este valor, se enumeran todos los controladores de dispositivos de cada UpdateXpress System Packs (UXSP) importados.

Importante: Después de seleccionar esta opción, debe realizar una comprobación de conformidad haciendo clic en el icono **Revisar el cumplimiento** () en la página Actualizaciones de controlador de Windows: Aplicar.

Paso 4. Haga clic en **Aceptar** para cerrar el cuadro de diálogo.

Aplicar controladores de dispositivos de Windows

Puede aplicar controladores de dispositivos a los servidores gestionados que ejecutan Windows.

Antes de empezar

- Lenovo XClarity Administrator utiliza el servicio de gestión remota de Windows (WinRM) escuchando sobre HTTPS o HTTP para ejecutar los comandos de actualización de controladores de dispositivos en los sistemas de Windows de destino. El servicio WinRM debe configurarse correctamente en los servidores de destino antes de intentar actualizar los controladores de dispositivo de SO (consulte Configuración del servidor de Windows para actualizaciones del controlador de dispositivo del SO).
- No se puede seleccionar los dispositivos que no se admiten actualizaciones.
- Antes de intentar actualizar los controladores de dispositivos en los servidores gestionados, lea las consideraciones sobre la actualización de controladores de dispositivos (consulte Consideraciones sobre la actualización de controladores de dispositivos de SO).
- Asegúrese de que el repositorio contenga los UXSP y controladores de dispositivos que desea desplegar (consulte Descarga de controladores de dispositivos de Windows).

  Nota: Cuando XClarity Administrator se instala por primera vez, el catálogo y el repositorio están vacíos.
- XClarity Administrator puede utilizar el servicio de gestión remota de Windows (WinRM) escuchando sobre HTTPS o HTTP para ejecutar los comandos de actualización de controladores de dispositivos en los sistemas de Windows de destino. HTTPS es el valor predeterminado. Para utilizar HTTP, haga clic en **Todas las acciones → Valores globales** en las actualizaciones de controlador de Windows: página Aplicar y luego borre **Utilizar HTTPS para actualizaciones de controlador de Windows**.

  Atención: Cuando utiliza HTTP, las credenciales de usuario de Windows se envían a través de la red de usuario *sin* cifrado y se pueden ver fácilmente utilizando herramientas de resolución de problemas de red comúnmente disponibles.

  Importante:

  - Asegúrese de que la gestión remota de Windows (WinRM) en el servidor de destino esté configurada para usar el mismo valor (HTTPS o HTTP) que se define en XClarity Administrator (consulte Configuración del servidor de Windows para actualizaciones del controlador de dispositivo del SO).
  - Asegúrese de que WinRM en el servidor de destino esté configurado con autenticación básica.
  - Cuando utiliza HTTPS, asegúrese de que WinRM en el servidor de destino esté configurado con **allowUnencrypted=false**.
- Asegúrese de que PowerShell sea compatible con el servidor de destino.
- Asegúrese de que el servidor de destino esté encendido antes de intentar actualizar a controladores de dispositivo. Si el servidor no está encendido, seleccione el servidor de destino y haga clic en **Todas las acciones → Acciones de alimentación → Encender**.
- Asegúrese de que XClarity Administrator tenga la información que necesita acceder al sistema operativo del host (consulte Gestión de acceso a los sistemas operativos en servidores gestionados.
- Si desea utilizar una cuenta de dominio al actualizar los controladores de dispositivos del SO, asegúrese de que creó el archivo de configuración necesario (consulte Configuración de una cuenta de dominio para actualizaciones de controladores de dispositivo del SO).

- Asegúrese de que no haya trabajos que se encuentren en ejecución en la actualidad en el servidor de destino. No puede actualizar los controladores de dispositivos en un servidor gestionado que esté bloqueado por un trabajo en ejecución. Si está ejecutando otro trabajo de actualización del servidor de destino, el trabajo de actualización queda en espera hasta que se completa el trabajo de actualización actual. Para ver una lista de los trabajos activos, haga clic en **Supervisión → Trabajos**.

Acerca de esta tarea

XClarity Administrator solo actualiza los controladores de dispositivos que no están en conformidad. Los controladores de dispositivos que no están en conformidad cuando la versión en el servidor es anterior a la versión UXSP. Los controladores de dispositivos que son iguales o posteriores a la versión en el UXSP seleccionado se omiten.

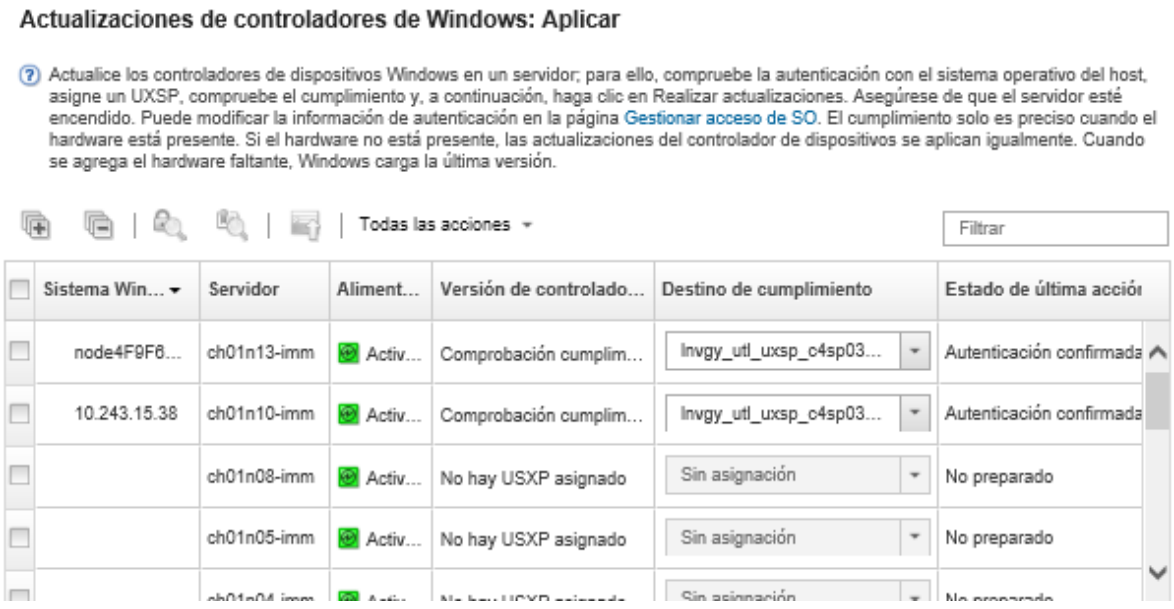
Procedimiento

Lleve a cabo los siguientes pasos para aplicar controladores de dispositivos Windows a servidores gestionados.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Actualizaciones de controlador de Windows: Aplicar** para mostrar la página Actualizaciones de controlador de Windows: Aplicar.

Importante:

- Para detectar los controladores de dispositivos en el servidor de destino y determinar el cumplimiento, debe seleccionar el servidor de destino y ejecutar la comprobación de conformidad. Después de que la comprobación de conformidad se ejecuta por primera vez, puede expandir la fila para ver una lista de controladores de dispositivos en el servidor de destino.
- La columna **Sistema Windows** identifica el nombre de host o la dirección IP del sistema operativo del host.
- La columna **Servidor** identifica el nombre y la dirección IP del servidor gestionado.



Paso 2. Seleccione uno o más controladores de dispositivos y servidores de destino.

Puede ordenar las columnas de la tabla para que sea más fácil encontrar servidores específicos. Además, puede ingresar texto para filtrar la lista de servidores que se muestran (como un nombre o una dirección IP) en el campo **Filtro**.

Consejo:

- Puede elegir actualizar todos los controladores de dispositivos para un sistema operativo específico, o puede ampliar un sistema operativo y seleccionar Actualizar solo los dispositivos específicos
- La columna **Estado de la actualización** muestra el estado de autenticación para cada servidor y el estado de actualización para cada controlador de dispositivo.
- La columna **Credencial de SO** muestra las credenciales almacenadas que se utilizan para autenticar el sistema operativo (por ejemplo, “901: company\USER1.”

  Si las credenciales del SO no están definidas para el sistema operativo del host en el servidor de destino, se muestra el cuadro de diálogo Editar credenciales de SO. Para un solo servidor de destino, especifique el nombre de usuario y la contraseña que desea utilizar para esta operación. Para varios servidores de destino, seleccione la credencial almacenada que se va a utilizar para cada servidor. A continuación, haga clic en **Guardar**.

  Nota: Las credenciales del SO que selecciona en el cuadro de diálogo Editar credenciales de SO no se guardan para el sistema operativo de host. Para guardar las credenciales del SO, consulte Gestión de acceso a los sistemas operativos en servidores gestionados.

Paso 3. Haga clic en el icono **Comprobar autenticación** () para ejecutar comprobaciones de autenticación y de requisitos previos.

XClarity Administrator se conecta con el sistema operativo del host con la credencial almacenada que se enumera en la columna **Credencial de SO**, determina la versión del sistema operativo, comprueba que WinRM esté habilitado, realiza comprobaciones de requisitos previos adicionales y luego se desconecta del sistema operativo del host.

Para obtener información acerca de cómo cambiar las credenciales almacenadas para el sistema operativo del host, consulte Gestión de acceso a los sistemas operativos en servidores gestionados.

Paso 4. Para cada servidor de destino, seleccione el destino UXSP que desea utilizar para actualizar los controladores de dispositivo desde la columna **Destino de cumplimiento**.

Paso 5. Vuelva a seleccionar los servidores de destino y haga clic en el icono **Revisar el cumplimiento** () para comprobar el cumplimiento de los controladores de dispositivo.

La revisión del cumplimiento actualiza el estado del cumplimiento en la columna **Versión de controlador instalada**. Esta columna muestra el estado global de cumplimiento para el servidor y la versión instalada y el estado de cumplimiento para cada controlador de dispositivo medido contra el UXSP asignado.

-  **Conforme**. El controlador de dispositivo instalado es igual o posterior a la versión del UXSP asignado.
-  **No conforme**. El controlador de dispositivo instalado es anterior a la versión del UXSP asignado. Puede hacer clic en el enlace para obtener más información sobre la no conformidad.

Nota: El cumplimiento de controlador de dispositivo solo es preciso cuando el hardware está presente. Si el hardware no está presente, los controladores de dispositivos se aplican igualmente al servidor. Cuando se agrega el hardware faltante al servidor, Windows carga la última versión.

Paso 6. Haga clic en el icono **Realizar actualizaciones** ().

Paso 7. Seleccione una de las siguientes reglas de actualización.

- **Detener todas las actualizaciones en caso de error**. Si se produce un error al actualizar alguno de los controladores de dispositivos en un dispositivo objetivo, el proceso de actualización se detiene para todos los dispositivos de destino en el trabajo de actualización del controlador de dispositivo actual. En este caso, no se aplicará ninguna de las actualizaciones de controladores de dispositivos en el UXSP para el dispositivo objetivo. El controlador de dispositivo actual que está instalado en todos los dispositivos de destino sigue en efecto.
- **Continuar en caso de error**. Si se produce un error al actualizar alguno de los controladores de dispositivo del dispositivo objetivo, el proceso de actualización de firmware no actualiza el controlador de dispositivo para ese dispositivo específico. En cambio, el proceso de actualización de firmware continúa actualizando el resto de los controladores de dispositivo en el dispositivo y prosigue con la actualización de todos los demás dispositivos de destino en el trabajo de actualización de controlador de dispositivo actual.
- **Ir al siguiente sistema en caso de error**. Si se produce un error al actualizar alguno de los controladores de dispositivos del dispositivo, el proceso de actualización detiene todos los intentos de actualizar el controlador de dispositivos para ese dispositivo específico, de modo que los controladores de dispositivos actuales que está instalado en dicho dispositivo continúan siendo efectivos. El proceso de actualización sigue actualizando todos los demás dispositivos del trabajo de actualización del controlador de dispositivos actual.

Paso 8. Haga clic en **Realizar actualizaciones** para actualizar de inmediato, o bien haga clic en **Programación** planificar que esta actualización se ejecute posteriormente.

Después de finalizar

Si el servidor de destino no logra iniciar el modo de mantenimiento cuando se aplica una actualización, intente volver a aplicar la actualización.

Si las actualizaciones no se han completado correctamente, consulte Consideraciones sobre la actualización de controladores de dispositivos de SO para saber cómo resolver problemas y aplicar acciones correctivas.

En la página Actualizaciones de controlador de Windows: Aplicar, puede realizar las siguientes acciones.

- Ver el estado de la actualización de controlador de dispositivo directamente en la página Aplicar de la columna **Estado de la página**.
- Supervisar el estado de la actualización de controlador de dispositivo desde el registro de trabajos. En la barra de menús de XClarity Administrator, haga clic en **Supervisión → Trabajos**.

  Para obtener más información acerca del registro de trabajos, consulte Supervisión de trabajos.

  Una vez completado el trabajo de actualización, puede verificar que los dispositivos sean compatibles desde la página Actualizaciones de controlador de Windows: Aplicar. La versión actual del controlador que está activa en cada dispositivo aparece en la columna **Versión de controlador instalada**.

Capítulo 15. Instalación de sistemas operativos en servidores sin sistema operativo

Puede utilizar Lenovo XClarity Administrator para gestionar Repositorio de imágenes del SO y desplegar imágenes de sistema operativo en hasta 28 servidores sin sistema operativo al mismo tiempo.

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

Antes de empezar

Después de que la prueba gratuita de 90 días termine, puede continuar utilizando XClarity Administrator para gestionar y supervisar el hardware de manera gratuita; sin embargo, debe comprar licencias de habilitación de todas las funciones para cada servidor gestionado que admita las funciones avanzadas de XClarity Administrator para continuar usando la función de despliegue de SO. Lenovo XClarity Pro proporciona titularidad para servicios y soporte y la licencia rehabilitación de funciones completas. Para obtener más información acerca de cómo adquirir Lenovo XClarity Pro, póngase en contacto con su representante de Lenovo o un business partner autorizado. Para obtener más información, consulte Instalación de licencia de habilitación de funciones completas en la XClarity Administrator documentación en línea.

Acerca de esta tarea

XClarity Administrator proporciona una forma sencilla de desplegar imágenes de sistema operativo en servidores *sin sistema operativo*.

Atención: Si despliega un sistema operativo en un servidor que tiene un sistema operativo instalado, XClarity Administrator lleva a cabo una instalación nueva que sobrescribe las particiones en los discos de destino

Hay varios factores que determinan la cantidad de tiempo que se requiere para desplegar un sistema operativo en un servidor:

- La cantidad de RAM instalada en el servidor, que afecta al tiempo que tarda el servidor en arrancar.
- El número y los tipos de adaptadores de E/S instalados en el servidor, que afecta a la cantidad de tiempo que XClarity Administrator tarda en hacer un inventario del servidor. También afecta a la cantidad de tiempo que tarda en iniciarse el firmare del UEFI cuando se arranca el servidor. Durante el despliegue del sistema operativo, el servidor se reinicia varias veces.
- Tráfico de red. XClarity Administrator descarga la imagen del sistema operativo a través de la red de datos o la red de despliegue del sistema operativo.
- La configuración de hardware del host donde está instalado el dispositivo virtual de Lenovo XClarity Administrator. La cantidad de RAM, procesadores y almacenamiento de disco duro pueden afectar a los tiempos de descarga.

Importante: Para desplegar una imagen del sistema operativo desde XClarity Administrator, al menos una de las interfaces de XClarity Administrator (Eth0 o Eth1) debe tener conectividad de red IP a la interfaz de red del servidor que se utiliza para acceder al sistema operativo del host. En el despliegue del sistema operativo se utiliza la interfaz definida en la página Acceso de red. Para obtener más información sobre los valores de red, consulte Configuración del acceso de red.

Antes de realizar el despliegue de un sistema operativo completo en un servidor, debe prepararlo actualizando el firmware con la versión más reciente y configurando el servidor utilizando Patrones de configuración. Para obtener más información, consulte Actualización de firmware en dispositivos gestionados, Configuración de servidores mediante el uso de patrones de configuración.

Atención: Se recomienda *no* utilizar XClarity Administrator para realizar un despliegue del sistema operativo completo en dispositivos Converged y ThinkAgile.

Procedimiento

En la siguiente figura se ilustra el flujo de trabajo para desplegar una imagen del SO en un servidor.

Paso 1. **Importar imágenes del SO.**

Antes de desplegar la imagen del SO en un servidor, primero debe importar el sistema operativo al repositorio. Cuando se importa una imagen del SO, XClarity Administrator:

- Asegúrese de que haya espacio suficiente en el Repositorio de imágenes del SO antes de importar el sistema operativo. En caso negativo, elimine una imagen existente del repositorio y vuelva a intentar importar la nueva.
- Crea uno o varios perfiles de esa imagen y lo almacena en el Repositorio de imágenes del SO. Cada *perfil* incluye opciones de imagen del SO e instalación. Para obtener más información acerca de los perfiles de imagen del SO predefinidos, consulte Perfiles de las imágenes del sistema operativo.

Un *sistema operativo base* es la imagen completa de un SO importado al repositorio de imágenes de SO. La imagen de base importada contiene perfiles predefinidos que describen las configuraciones de instalación de dicha imagen. Puede crear perfiles personalizados en la imagen de SO base que se pueden desplegar para configuraciones específicas.

También puede importar *sistemas operativos personalizados* admitidos. Esta imagen personalizada contiene un perfil de espacio reservado predefinido que no se puede desplegar. Debe importar un perfil personalizado que se pueda desplegar o crear su propio perfil personalizado con base en el perfil de espacio reservado. Después de añadir el perfil personalizado, se quita el perfil de espacio reservado automáticamente.

En Microsoft Windows Server 2016 y 2019, se puede importar una imagen del sistema operativo personalizada para cada versión. La imagen de base importada contiene perfiles predefinidos que describen las configuraciones de instalación de dicha imagen. No se puede crear perfiles personalizados en la imagen de SO personalizada.

Para ver una lista de los sistemas operativos básicos y personalizados compatibles, consulte Sistemas operativos compatiblesSistemas operativos compatibles en la documentación en línea de Lenovo XClarity Administrator.

Paso 2. **(Opcional) Personalice la imagen del SO.**

Puede personalizar una imagen del SO al agregar controladores de dispositivos, archivos de arranque (solo para Windows), valores de configuración, archivos de instalación desatendida, scripts posteriores a la instalación y software. Al personalizar una imagen del SO base, XClarity

Administrator crea un perfil de imagen del SO personalizado que incluye archivos personalizados y opciones de instalación.

El repositorio de imágenes del SO puede almacenar un número ilimitado de archivos predefinidos y personalizados, en caso que haya espacio disponible para almacenar los archivos.

Paso 3. **Configuración de valores globales.**

Los valores globales son opciones de configuración que se utilizan como valores predeterminados en el despliegue del sistema operativo. Puede configurar los valores globales siguientes.

- La contraseña que la cuenta de usuario de administrador utiliza para desplegar sistemas operativos
- El método utilizado para asignar direcciones IP a los servidores
- Las claves de licencia que deben usarse para activar los sistemas operativos instalados
- Opcionalmente es posible unir un dominio de Active Directory como parte del despliegue del sistema operativo Windows.

Paso 4. **Configuración de valores de red.**

Puede especificar los valores de red de cada servidor en el que se desplegarán los sistemas operativos.

Si va a utilizar DHCP para asignar direcciones IP de forma dinámica, debe configurar la dirección MAC.

Si utiliza direcciones IP estáticas, debe configurar los valores de red siguientes para un servidor específico antes de desplegar un sistema operativo en ese servidor. Una vez configurados estos valores, el estado de despliegue el servidor cambia a “Preparado”. (Tenga en cuenta que algunos campos no están disponibles para las direcciones IPv6 estáticas.)

- Nombre de host

  El nombre de host debe cumplir con las reglas siguientes:
  - El nombre de host de cada servidor gestionado debe ser único.
  - El nombre de host puede contener cadenas (etiquetas) separadas por un punto (.).
  - Cada etiqueta puede contener letras ASCII, dígitos y guiones (-); sin embargo, la cadena no puede comenzar ni terminar con un guion y no puede estar compuesta únicamente de dígitos.
  - La primera etiqueta puede ser 2 a 15 caracteres de longitud. Las etiquetas siguientes pueden ser de 2 a 63 caracteres de longitud.
  - La longitud máxima del nombre de host no debe superar los 255 caracteres.
- Dirección MAC del puerto en el host donde va a instalarse el sistema operativo.

  La dirección MAC está configurada en AUTO de forma predeterminada. Esta configuración detecta automáticamente los puertos Ethernet que se pueden configurar y utilizar para el despliegue. La primera dirección MAC (puerto) que se detecta se utiliza manera predeterminada. Si se detecta la conectividad en otra dirección MAC, el host de XClarity Administrator se reinicia automáticamente para utilizar la dirección MAC recién detectada para el despliegue.

  Puede determinar el estado del puerto de dirección MAC que se utiliza para el despliegue del SO desde el menú desplegable de la **Dirección MAC** en el cuadro de diálogo Valores de red. Si hay varios puertos en funcionamiento o si todos los puertos están inactivos, se utiliza AUTO de manera predeterminada.

  Notas:

  - No se admiten los puertos de red virtuales. No utilice un puerto de red físico para simular varios puertos de red virtual.
  - Cuando el valor de red del servidor está establecido en AUTO, XClarity Administrator puede detectar automáticamente los puertos de red en las ranuras 1 a 16. Al menos un puerto de las ranuras 1 a 16 debe tener una conexión a XClarity Administrator.
  - Si desea utilizar un puerto de red en la ranura 17 o superior para la dirección MAC, no puede utilizar AUTO. En su lugar, debe establecer la configuración de red del servidor en la dirección MAC del puerto específico que desee utilizar.
  - Para los servidores ThinkServer, no se muestran todas las direcciones MAC del host. En la mayoría de los casos, las direcciones MAC para los adaptadores Ethernet AnyFabric se muestran en el cuadro de diálogo Editar valores de red. Las direcciones MAC para otros adaptadores Ethernet (como la LAN en placa madre) no se muestran. En los casos donde la dirección MAC de un adaptador no está disponible, utilice el método AUTO para los despliegues que no son VLAN.
- Dirección IP y Máscara de subred
- Puerta de enlace de IP
- Hasta dos servidores del sistema de nombres de dominio (DNS)
- Velocidad de la unidad de transmisión máxima (MTU)
- ID de VLAN, si está habilitado el modo IP de VLAN

Si elige utilizar VLAN, puede asignar un Id. de VLAN al adaptador de red del host que se está configurando.

Paso 5. **Elegir las opciones de almacenamiento**

Para cada despliegue, puede elegir la ubicación de almacenamiento preferida donde se desplegará el sistema operativo. Dependiendo del sistema operativo, puede elegir el despliegue en un disco duro local, una clavija del hipervisor integrada o SAN.

Paso 6. **Elija opciones adicionales y valores de configuración personalizada y despliegue la imagen del SO.**

Puede configurar opciones de despliegue adicionales, como la clave de licencia para despliegue del sistema operativo y valores de configuración personalizada. Si está instalando Microsoft Windows, configure también el dominio de Active Directory al que se unirá.

Notas:

- Si se definen valores de configuración personalizada para un perfil de SO personalizado específico, debe definir los valores de la configuración personalizada antes de desplegar el perfil en un servidor.
- Al desplegar un perfil de SO personalizado que incluye una configuración personalizada, todos los servidores de destino deben usar el mismo perfil de SO personalizado y los valores de la configuración personalizada se aplican a todos los servidores de destino.

A continuación, puede elegir los servidores de destino del despliegue y las imágenes del SO que se desplegarán. Recuerde que para desplegar un sistema operativo, el servidor debe tener un estado de despliegue de “Preparado”.

Puede desplegar imágenes de sistemas operativos hasta en 28 servidores al mismo tiempo.

Antes de intentar desplegar la imagen de un sistema operativo, revise Consideraciones del despliegue del sistema operativo.

Consideraciones del despliegue del sistema operativo

Antes de intentar desplegar la imagen de un sistema operativo, revise las siguientes consideraciones.

Consideraciones acerca de Lenovo XClarity Administrator

- Asegúrese de que no haya trabajos que se encuentren en ejecución en la actualidad en el servidor de destino. Para ver una lista de los trabajos activos, haga clic en **Supervisión → Trabajos**.
- Asegúrese de que el servidor de destino no tenga un patrón de servidor aplazado o parcialmente activado. Si un patrón de servidor se ha aplazado o está parcialmente activado en el servidor gestionado, debe reiniciar el servidor para aplicar todos los valores de configuración. No despliegue un sistema operativo en un servidor que tenga un patrón de servidor parcialmente activado. Para determinar el estado de configuración del servidor, consulte el campo **Estado de configuración** en la página Resumen del servidor gestionado (consulte Visualización de los detalles de un servidor gestionado).
- Asegúrese de que en el cuadro de diálogo Valores globales: Desplegar sistemas operativos se especifica la contraseña para la cuenta de administrador que se va a utilizar para desplegar el sistema operativo. Para obtener más información sobre la configuración de la contraseña, consulte Configuración de valores globales de despliegue del SO.
- Asegúrese de que los valores globales predeterminados sean correctos para el despliegue de este sistema operativo (consulte Configuración de valores globales de despliegue del SO).

Consideraciones del sistema operativo

- Asegúrese de que dispone de todas las licencias del sistema operativo aplicables para activar los sistemas operativos instalados. El usuario es responsable de obtener las licencias directamente del fabricante del sistema operativo.
- Asegúrese de que la imagen del sistema operativo que pretende desplegar ya esté cargada en el Repositorio de imágenes del SO. Para obtener más información sobre cómo importar imágenes, consulte Importación de imágenes del sistema operativo.
- Es posible que las imágenes de sistema operativo en el repositorio de XClarity Administrator no se admitan solo en ciertas plataformas de hardware. Solo los perfiles de imagen del SO que son compatibles con el servidor seleccionado se enumeran en la página Desplegar imágenes de SO. Puede identificar si un sistema operativo es compatible con un servidor específico en Sitio web de guía de interoperabilidad de SO de Lenovo.
- Para Windows, debe importar un archivo de arranque en el repositorio de imágenes del SO antes de poder desplegar un perfil de Windows. Lenovo incluye el archivo de arranque predefinido WinPE_64.wim junto con un conjunto de controladores de dispositivos en un único paquete que puede descargarse desde el Página web del repositorio de controladores de Lenovo Windows e imágenes de WinPE y luego importarse al repositorio de imágenes del SO. Si el archivo de paquete contiene los controladores de dispositivos y archivos de arranque, puede importar el archivo de conjunto desde la pestaña **Controlador de dispositivo** o **Archivos de arranque**.
- Para SLES 15 y 15 SP1, debe importar la imagen del instalador y la imagen del paquete asociado desde el Página web del centro de soporte del sistema operativo de servidor. Para SLES 15 SP2 o posterior, solo tiene que importar la imagen del medio de instalación completa porque el instalador unificado y los paquetes de DVD de SUSE Linux Enterprise Server 15 y 15 SP1 están desechados.
- Para los servidores de ThinkSystem, XClarity Administrator incluye controladores de dispositivo predefinidos para permitir la instalación del sistema operativo, así como la configuración básica de red y de almacenamiento para el sistema operativo final. Para otros servidores, asegúrese de que la imagen del sistema operativo que está instalando desplegar incluya los controladores de Ethernet, Fibre Channel y dispositivo de adaptador de almacenamiento para su hardware. Si el controlador de dispositivo del adaptador de E/S no está incluido en el sistema operativo, el adaptador no es compatible con el despliegue del SO. Siempre instale el sistema operativo más reciente para garantizar que cuente con los controladores de dispositivos de adaptador de E/S y los archivos de arranque de entrada más recientes

que necesita. También puede agregar controladores de dispositivo y archivos de controlador predefinidos a los sistemas operativos importado sen XClarity Administrator (consulte Personalización de los perfiles de la imagen del SO en la documentación en línea de XClarity Administrator).

Para VMware, use la imagen personalizada de Lenovo más reciente para ESXi, la cual incluye la compatibilidad para los adaptadores más recientes. Para obtener información sobré cómo conseguir esa imagen, consulte Soporte de VMware - página web de descargas.

- Para servidores ThinkSystem, si desea desplegar SLES 12 SP2, debe usar un perfil kISO. Para obtener los perfiles kISO, debe importar la imagen kISO SLES pertinente después de importar el sistema operativo SLES base. Puede adquirir y descargar la imagen kISO SLES desde el Soporte de Linux - página web de descargas.

  Notas:

  – La imagen kISO de SLES cuenta en el número máximo de imágenes de SO importadas.

    Para ver una lista de los sistemas operativos básicos y personalizados compatibles, consulte Sistemas operativos compatiblesSistemas operativos compatibles en la documentación en línea de Lenovo XClarity Administrator.

  – Si elimina todos los perfiles de kISO, debe eliminar el sistema operativo SLES base y, a continuación, importar el sistema de operación base y la imagen kISO nuevamente para desplegar SLES 12 SP2 en un servidor ThinkSystem.

  – Si crea un perfil de sistema operativo personalizado basado en un perfil kISO, no se incluyen los controladores de dispositivos predefinidos en el sistema operativo base. Se utiliza en su lugar los controladores de dispositivos que se incluyen en la kISO. También puede agregar controladores de dispositivo para el perfil de SO personalizado (consulte Creación de un perfil de imagen de SO personalizado).

Para obtener más información sobre las limitaciones de sistemas operativos específicos, consulte Sistemas operativos compatibles.

Consideraciones de red

- Asegúrese de que todos los puertos necesarios estén abiertos (consulte Disponibilidad de puertos para sistemas operativos desplegados).
- Asegúrese de que XClarity Administrator sea capaz de comunicarse con el servidor de destino (el controlador de gestión de la placa base y la red de datos de los servidores) a través de la interfaz (Eth0 o Eth1) que se seleccionó al configurar el acceso de red XClarity Administrator.

  Para especificar una interfaz que se debe utilizar para el despliegue del sistema operativo, consulte Configuración del acceso de red).

  Para obtener más información sobre la red y las interfaces del despliegue del sistema operativo, consulte Consideraciones de red en la XClarity Administrator documentación en línea.
- Asegúrese de que las direcciones IP del sistema operativo del host sean únicas. XClarity Administrator busca la presencia de duplicados de las direcciones IP especificadas para la dirección de red durante el proceso de despliegue.
- Si la red es inestable o lenta, puede obtener resultados impredecibles al desplegar sistemas operativos.
- La interfaz de red de XClarity Administrator que se utiliza para la gestión debe configurarse para conectarse al controlador de la placa base utilizando el mismo método de dirección IP que elige en el cuadro de diálogo Valores globales: desplegar sistemas operativos. Por ejemplo, si XClarity Administrator esta configurado para utilizar eth0 con fines de gestión y usted elige utilizar las direcciones IPv6 estáticas asignadas manualmente al configurar el SO implementado, entonces eth0 se debe configurar con una dirección IPv6 que tenga conectividad al controlador de gestión de la placa base.

- Si decide utilizar direcciones IPv6 para los valores globales de despliegue de SO, la dirección IPv6 de XClarity Administrator debe poder enrutarse al controlador de gestión de placa base y la red de datos de los servidores.
- No se admite el modo IPv6 para ThinkServer (consulte Limitaciones de configuración IPv6 en la documentación en línea de XClarity Administrator).
- Si va a utilizar DHCP para asignar direcciones IP de forma dinámica, debe configurar la dirección MAC.
- Si utiliza direcciones IP estáticas, debe configurar los valores de red siguientes para un servidor específico antes de desplegar un sistema operativo en ese servidor. Una vez configurados estos valores, el estado de despliegue el servidor cambia a “Preparado”. (Tenga en cuenta que algunos campos no están disponibles para las direcciones IPv6 estáticas.)
  - Nombre de host

    El nombre de host debe cumplir con las reglas siguientes:
    - El nombre de host de cada servidor gestionado debe ser único.
    - El nombre de host puede contener cadenas (etiquetas) separadas por un punto (.).
    - Cada etiqueta puede contener letras ASCII, dígitos y guiones (-); sin embargo, la cadena no puede comenzar ni terminar con un guion y no puede estar compuesta únicamente de dígitos.
    - La primera etiqueta puede ser 2 a 15 caracteres de longitud. Las etiquetas siguientes pueden ser de 2 a 63 caracteres de longitud.
    - La longitud máxima del nombre de host no debe superar los 255 caracteres.
  - Dirección MAC del puerto en el host donde va a instalarse el sistema operativo.

    La dirección MAC está configurada en AUTO de forma predeterminada. Esta configuración detecta automáticamente los puertos Ethernet que se pueden configurar y utilizar para el despliegue. La primera dirección MAC (puerto) que se detecta se utiliza manera predeterminada. Si se detecta la conectividad en otra dirección MAC, el host de XClarity Administrator se reinicia automáticamente para utilizar la dirección MAC recién detectada para el despliegue.

    Puede determinar el estado del puerto de dirección MAC que se utiliza para el despliegue del SO desde el menú desplegable de la **Dirección MAC** en el cuadro de diálogo Valores de red. Si hay varios puertos en funcionamiento o si todos los puertos están inactivos, se utiliza AUTO de manera predeterminada.

    Notas:

    - No se admiten los puertos de red virtuales. No utilice un puerto de red físico para simular varios puertos de red virtual.
    - Cuando el valor de red del servidor está establecido en AUTO, XClarity Administrator puede detectar automáticamente los puertos de red en las ranuras 1 a 16. Al menos un puerto de las ranuras 1 a 16 debe tener una conexión a XClarity Administrator.
    - Si desea utilizar un puerto de red en la ranura 17 o superior para la dirección MAC, no puede utilizar AUTO. En su lugar, debe establecer la configuración de red del servidor en la dirección MAC del puerto específico que desee utilizar.
    - Para los servidores ThinkServer, no se muestran todas las direcciones MAC del host. En la mayoría de los casos, las direcciones MAC para los adaptadores Ethernet AnyFabric se muestran en el cuadro de diálogo Editar valores de red. Las direcciones MAC para otros adaptadores Ethernet (como la LAN en placa madre) no se muestran. En los casos donde la dirección MAC de un adaptador no está disponible, utilice el método AUTO para los despliegues que no son VLAN.
  - Dirección IP y Máscara de subred
  - Puerta de enlace de IP
  - Hasta dos servidores del sistema de nombres de dominio (DNS)
  - Velocidad de la unidad de transmisión máxima (MTU)

  - ID de VLAN, si está habilitado el modo IP de VLAN
- Si elige utilizar VLAN, puede asignar un Id. de VLAN al adaptador de red del host que se está configurando.

Para obtener más información acerca de la red y de las interfaces de despliegue del sistema operativo, consulte Configuración de los valores de red para servidores gestionados, Configuración de los valores de red para servidores gestionados y Consideraciones de red en la documentación en línea de XClarity Administrator.

Consideraciones de almacenamiento y de opciones de arranque

- Asegúrese de que la opción de arranque de la UEFI en el servidor de destino se haya establecido en “Arrancar solo UEFI” antes de desplegar un sistema operativo. Las opciones de arranque “Solo heredado” y “Primero UEFI y después heredado” no son compatibles con el despliegue del sistema operativo.
- Cada servidor debe tener un adaptador RAID de hardware instalado y configurado.

  Atención:

  - Solo se admite almacenamiento configurado con RAID de hardware.
  - No se admite el RAID de software que generalmente se encuentra está presente en el adaptador de almacenamiento Intel SATA incorporado o el almacenamiento generalmente se especifica como JBOD. Sin embargo, si un adaptador de RAID de hardware no está presente, configurar el adaptador SATA en el **Modo de AHCI SATA** habilita el despliegue del sistema operativo o la configuración de discos no configurados en buen estado en JBOD en algunos casos. Para obtener más información, consulte El instalador del SO no puede encontrar el disco en el que desea instalar XClarity Administrator en la documentación en línea de XClarity Administrator.

    Esta excepción no se aplica a las unidades M.2.
  - Si un dispositivo gestionado cuenta con dos unidades locales (SSD, SAS o SATA) que no están configuradas para RAID de hardware y unidades M.2, se deben deshabilitar las unidades locales en el caso que desee usar las unidades M.2, o bien, se deben deshabilitar las unidades M.2 si desea usar las unidades locales. Puede deshabilitar los dispositivos del controlador de almacenamiento incorporado y los ROM heredados y de opción de almacenamiento de UEFI mediante el uso de patrones de configuración. Para esto, seleccione Deshabilitar disco local en la pestaña Almacenamiento local del asistente o cree un patrón de configuración desde un servidor existente y, a continuación, deshabilite los dispositivos M.2 en el patrón de UEFI extendido.
  - Si se habilita un adaptador SATA, el modo SATA *no debe* configurarse en “IDE”.
- El almacenamiento NVMe que está conectado a una placa madre del servidor o controlador HBA no es compatible y no se debe instalar en el dispositivo; de lo contrario, el despliegue del SO en un almacenamiento que no sea NVMe producirá un error.
- Cuando se despliega RHEL, no se admiten los puertos multipuerto que están conectados al mismo LUN en el almacenamiento de destino.
- Asegúrese de que el modo de arranque seguro esté deshabilitado para el servidor. Si esta desplegando un sistema operativo con el modo de arranque seguro habilitado (como Windows), deshabilite el modo de arranque seguro, despliegue el sistema operativo y, a continuación, vuelva a habilitar el modo de arranque seguro.
- Al desplegar Microsoft Windows en un servidor, las unidades instaladas no debe tener particiones de sistema existentes (consulte El despliegue del SO falla debido a la presencia de particiones del sistema en una unidad de disco conectado en la documentación en línea de XClarity Administrator).
- Para servidores ThinkServer, asegúrese de que se cumplan los siguientes requisitos:
  - Los valores de arranque en el servidor deben incluir una política OpROM de almacenamiento que se establece como `UEFI Only`. Para obtener más información, consulte El instalador del SO no arranca en un servidor ThinkServer - XClarity Administrator en la XClarity Administrator documentación en línea.

- Si está desplegando ESXi y hay adaptadores de red que pueden arrancar PXE, deshabilite PXE en los adaptadores de red antes de desplegar el sistema operativo. El despliegue se completó, puede volver a habilitar PXE, si así lo desea.
- Si está desplegando ESXi y hay dispositivos iniciables en la lista del orden de arranque fuera de la unidad en la que el sistema operativo se ha de instalar, quite los dispositivos iniciables de la lista de orden de arranque antes de desplegar el sistema operativo. Después de completar el despliegue, puede agregar el dispositivo iniciable de nuevo a la lista. Asegúrese de que la unidad instalada esté en la parte superior de la lista.

Para obtener más información sobre estos valores de localización de almacenamiento, consulte Elegir la ubicación de almacenamiento de los servidores gestionados.

Consideraciones de dispositivo gestionado

- Para obtener información sobre las limitaciones del despliegue del sistema operativo para dispositivos específicos, consulte Soporte de XClarity Administrator: página web de compatibilidad, haga clic en la pestaña **Compatibilidad** y, a continuación, haga clic en el enlace de los tipos de dispositivo correspondientes.
- Asegúrese de que no haya ningún medio montado (como ISO) en el servidor de destino. Además, asegúrese de no haya ninguna sesión de medio remoto activo abierta para el controlador de gestión.
- Asegúrese de que la marca de hora de BIOS con la fecha y hora actuales.
- Para los servidores con XCC2 que tienen habilitada la función de protección del sistema y la acción establecida en **Evitar el arranque del SO**, asegúrese de que la función de protección del sistema sea conforme con el dispositivo. Si la función de protección del sistema es no conforme, los dispositivos no pueden completar el proceso de arranque, lo que provoca que el despliegue del SO falle. Para aprovisionar estos dispositivos, responda manualmente el mensaje de arranque de la función de protección del sistema para permitir que los dispositivos arranquen con normalidad.
- Para servidores ThinkSystem y System x, asegúrese de que la opción de configuración de BIOS heredado esté deshabilitado. Desde Setup Utility (F1) de BIOS/UEFI, haga clic en **Configuración de UEFI → Valores del sistema** y compruebe que la configuración de BIOS heredada esté establecida en deshabilitado.
- Para los servidores de Flex System, asegúrese de que el chasis esté encendido.
- Para los servidores Converged, NeXtScale y System x, asegúrese de que se haya instalado una clave de característica bajo demanda (FoD) de presencia remota. 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). Para obtener más información acerca las claves de característica bajo demanda (FoD) que están instaladas en los servidores, consulte Ver claves de Características bajo demanda.
- Para servidores ThinkSystem y dispositivos ThinkAgile, se requiere la característica XClarity Controller empresarial para el despliegue de sistemas operativos. Para obtener más información, consulte Ver claves de Características bajo demanda.
- Para los dispositivos Converged y ThinkAgile, se recomienda *no* utilizar XClarity Administrator para realizar un despliegue del sistema operativo completo.

Sistemas operativos compatibles

Lenovo XClarity Administrator admite el despliegue de varios sistemas operativos. Solo las versiones compatibles de sistemas operativos se pueden cargar en el Repositorio de imágenes del SO de XClarity Administrator.

Importante:

- Para obtener información sobre las limitaciones del despliegue del sistema operativo para dispositivos específicos, consulte Soporte de XClarity Administrator: página web de compatibilidad, haga clic en la pestaña **Compatibilidad** y, a continuación, haga clic en el enlace de los tipos de dispositivo correspondientes.
- La característica de gestión criptográfica de XClarity Administrator permite la limitación de la comunicación a ciertos modos mínimos de SSL/TLS. Por ejemplo, si se selecciona TLS 1.2, entonces aquellos sistemas operativos con un proceso de instalación que admita TLS 1.2 y algoritmos criptográficos complejos solo se podrán desplegar mediante XClarity Administrator.
- Es posible que las imágenes de sistema operativo en el repositorio de XClarity Administrator no se admitan solo en ciertas plataformas de hardware. Solo los perfiles de imagen del SO que son compatibles con el servidor seleccionado se enumeran en la página Desplegar imágenes de SO. Puede identificar si un sistema operativo es compatible con un servidor específico en Sitio web de guía de interoperabilidad de SO de Lenovo.
- Para obtener información de compatibilidad y soporte sobre sistemas operativos e hipervisor y recursos y soluciones para servidores de Lenovo, consulte Página web del centro de soporte del sistema operativo de servidor.

La siguiente tabla enumera los sistemas operativos de 64 bits que XClarity Administrator puede desplegar.

Sistema operativo	Versiones	Notas
CentOS Linux	7.2 and later 8.0 8.1 8.2	**Notas:** • Se admiten todas las versiones secundarias existentes y futuras, a menos que se especifique lo contrario. • Se admiten direcciones DHCP, IPv4 estática e IPv6 estática. • El etiquetado VLAN no es compatible. • No se admiten los controladores de uso inmediato. • La personalización del perfil de SO no es compatible. • CentOS 8.3 no es compatible.
Microsoft® Windows® Azure Stack HCI	20H2 21H2	La personalización del perfil de SO no es compatible.
Cliente de Microsoft Windows	10 21H2 10 22H2 11 22H2	

Sistema operativo	Versiones	Notas
Microsoft Windows Server	2012 R2 2012 R2U1 2016 2019 2022	Se admiten tanto las copias de venta minorista como las copias de licencia. **Nota:** XClarity Administrator se prueba solo con versiones de Windows que son compatibles con Microsoft al momento del lanzamiento de la versión XClarity Administrator. Las siguientes *no son compatibles*: • Windows Reseller Option Kit (ROK) • Canal semianual de Windows Server (SAC) v1709, v1803 y v1809 • Windows Server 2019 Essentials • Windows Server 2016 Nanoserver • Copia de evaluación de Windows Server 2012 • Despliegue de imágenes de Windows Server en servidores gestionados con claves de hipervisor. Windows Server 2012 R2 en servidores que contienen procesadores Intel CLX Antes de desplegar una imagen de Windows, debe quitar físicamente la clave de hipervisor integrada de los servidores de destino. Esto incluye Hyper-V mediante uno de los perfiles de virtualización. – Centro de datos – Núcleo del centro de datos – Virtualización del centro de datos (Hyper-V) – Núcleo de la virtualización del centro de datos (Hyper-V con núcleo) – Estándar – Núcleo estándar – Virtualización estándar (Hyper-V) – Núcleo de la virtualización estándar (Hyper-V con núcleo)
Servidor Red Hat® Enterprise Linux (RHEL)	6.8 and later 7.2 and later 8.x 9.x	Incluye KVM **Notas:** • Se admiten todas las versiones secundarias existentes y futuras, a menos que se especifique lo contrario. • Al importar la versión del DVD de la imagen del SO, DVD1 solo es compatible. • Cuando instale RHEL en los servidores de ThinkSystem, se recomienda RHEL v7.4 o posterior. • Para desplegar RHEL 7.2, se debe configurar la asignación de IP global para utilizar direcciones IPv4. Para obtener información acerca de los valores globales, consulte Configuración de valores globales de despliegue del SO. • Se han observado errores de implementación de SO en redes IPv6 con ancho de banda más bajos, debido a los tiempos de espera del instalador de SO. • El etiquetado VLAN no es compatible.
Rocky Linux	8.x 9.x	**Notas:** • Se admiten todas las versiones secundarias existentes y futuras, a menos que se especifique lo contrario. • Se admiten direcciones DHCP, IPv4 estática e IPv6 estática. • El etiquetado VLAN no es compatible. • No se admiten los controladores de uso inmediato.

Sistema operativo	Versiones	Notas
SUSE® Linux Enterprise Server (SLES)	12.x 15.x	Incluye hipervisores KVM y Xen **Notas:** • Se admiten todos los paquetes de servicio existentes y futuros, a menos que se especifique lo contrario. • Al importar la versión del DVD de la imagen del SO, DVD1 solo es compatible. • Se han observado errores de implementación de SO en redes IPv6 con ancho de banda más bajos, debido a los tiempos de espera del instalador de SO. • Si desea desplegar SLES 12 SP2 en un servidor ThinkSystem, debe usar un perfil kISO. Para obtener los perfiles kISO, debe importar la imagen kISO SLES adecuada. Para obtener más información, consulte el apartado Consideraciones del despliegue del sistema operativo. • Para SLES 15 y 15 SP1, debe importar la imagen del instalador y la imagen del paquete asociado desde el Página web del centro de soporte del sistema operativo de servidor. Para SLES 15 SP2 o posterior, solo tiene que importar la imagen del medio de instalación completa porque el instalador unificado y los paquetes de DVD de SUSE Linux Enterprise Server 15 y 15 SP1 están desechados. • El etiquetado VLAN no es compatible.
Servidor Ubuntu	20.04.x 22.04.x	**Notas:** • La imagen se puede instalar en la opción de almacenamiento seleccionada (unidad de disco local, unidad M.2 o volumen SAN FC). • Se admiten todas las versiones secundarias existentes y futuras, a menos que se especifique lo contrario. • Solo se admite DHCP. *No se* admiten direcciones IPv4 estática e IPv6 estática. • *No se* admite el etiquetado VLAN. • *No se* admiten los controladores de uso inmediato. • *No se* admite la personalización del perfil de SO.
VMware vSphere® Hypervisor (ESXi)	5.5 5.5u1 5.5u2 5.5u3 6.0.x 6.5.x 6.7.x 7.0.x 8.0.x	Se admiten imágenes base de VMware vSphere Hypervisor (ESXi) e imágenes personalizadas de Lenovo VMware ESXi. Las imágenes personalizadas de Lenovo VMware ESXi están personalizadas para hardware seleccionado para que pueda gestionar la plataforma en línea, incluida la actualización y configuración del firmware, el diagnóstico de la plataforma y alertas de hardware mejoradas. Las herramientas de gestión de Lenovo también admiten la gestión simplificada del ESXi con servidores System x seleccionados. Esta imagen está disponible para descarga desde el Soporte de VMware - página web de descargas. La licencia que se proporciona con la imagen es una versión de evaluación gratuita para 60 días. El usuario es el responsable de cumplir todos los requisitos de licencia de VMware. **Importante:** • Se admiten todos los paquetes de actualización existentes y futuros para 6.0, 6.5, 6.7, 7.0 y 8.0, a menos que se especifique lo contrario. • Imágenes base de ESXi (sin personalización de Lenovo) incluyen solo controladores básicos incorporados para dispositivos de red y almacenamiento. La imagen base no incluye los controladores de dispositivo (que se incluyen en las imágenes personalizadas de Lenovo VMware ESXi). Para agregar controladores de dispositivos de fábrica, cree sus propios perfiles de imagen OS0 (consulte Personalización de los perfiles de la imagen del SO).

Sistema operativo	Versiones	Notas
		• En algunas versiones de imágenes personalizadas de Lenovo VMware ESXi, pueden haber imágenes separadas disponibles para System x, ThinkSystem y ThinkServer. Solo puede existir una imagen de una versión específica a la vez en el repositorio de imágenes del SO. • El despliegue de ESXi no es compatible con servidores específicos antiguos. Para obtener información sobre los servidores compatibles, consulte el Sitio web de guía de interoperabilidad de SO de Lenovo. • Se admiten las siguientes versiones de dispositivos ThinkServer: ESXi 6.0u3, 6.5 o posterior. • Durante la instalación de ESXi 5.5 (cualquier actualización) o 6.0 en un servidor de un chasis de Flex System, puede que el servidor no responda o se reinicie poco después del siguiente mensaje: `Loading image.pld` • ESXi 5.5 requiere que el espacio de E/S asignado a la memoria (MMIO) esté configurado dentro de los 4 GB iniciales del sistema. Dependiendo de la configuración, algunos sistemas tratan de utilizar una memoria superior a 4 GB, lo que puede provocar un error. Para resolver el problema, consulte El despliegue de VMware provoca que el sistema se cuelgue o se reinicie en la documentación en línea de XClarity Administrator. • Al desplegar ESXi utilizando un modo IPv6 estático, el nombre de host definido en la página de valores de red en XClarity Administrator no se configura en la instancia ESXi desplegada. En cambio, se utiliza el nombre de host predeterminado `localhost`. Debe configurar manualmente el nombre de host en el ESXi implementado para que coincida con el nombre de host definido en XClarity Administrator. • Cuando desplegar ESXi en un servidor gestionado, el sistema operativo no mueve explícitamente la unidad en la que el sistema operativo está instalado en la parte superior de la lista del orden de arranque. Si se especifica un dispositivo de arranque que contiene un SO arrancable o un servidor PXE antes que el dispositivo de arranque que contiene ESXi, ESXi no arrancará. Para el despliegue de ESXi, XClarity Administrator actualiza la lista del orden de arranque de la mayoría de los servidores para asegurarse de que el dispositivo de arranque ESXi está en la parte superior de la lista de orden de arranque; sin embargo, los servidores de ThinkServer no proporcionan una manera en la que XClarity Administrator pueda actualizar la lista del orden de arranque. Debe deshabilitar el soporte de arranque PXE o quitar los dispositivos iniciables que no sean la unidad de instalación antes de desplegar el sistema operativo. Para obtener más información, consulte El sistema operativo no arranca después de desplegar ESXi en un servidor ThinkServer en la XClarity Administrator documentación en línea . **Consejo:** En lugar de definir **MM Config** mediante la Setup Utility para cada servidor, considere la posibilidad de usar uno de los patrones de UEFI extendida predefinidos que están relacionados con la virtualización, que establece la opción MM Config en 3GB y deshabilita la asignación del recurso de 64 bits de la PCI (PCI 64-Bit Resource). Para obtener más información sobre los patrones de configuración, consulte Definición de los valores extendidos de UEFI.

Perfiles de las imágenes del sistema operativo

Al importar una imagen del CO en Repositorio de imágenes del SO, Lenovo XClarity Administrator crea uno o varios perfiles de dicha imagen y los almacena en el Repositorio de imágenes del SO. Cada *perfil* predefinido incluye la imagen del SO y las opciones de instalación de dicha imagen.

Atributos de perfil de imagen del SO

Los atributos de perfil de imagen del SO proporcionan información adicional acerca de un perfil de imagen del SO. Pueden aparecer los siguientes atributos.

- **kISO**. Debe usar un perfil kISO para desplegar SLES 12 SP2 a un servidor ThinkSystem. Puede adquirir y descargar la imagen kISO SLES desde el Soporte de Linux - página web de descargas.

Perfiles de la imagen del SO predefinidos

La siguiente tabla enumera los perfiles predefinidos por XClarity Administratoral importar una imagen del sistema operativo. Esta tabla también enumera los paquetes que se incluyen en cada perfil.

Puede crear un perfil de imagen del SO personalizado para un sistema operativo base. Para obtener más información, consulte Personalización de los perfiles de la imagen del SO.

Sistema operativo	Perfil de	Paquetes incluidos en el perfil	

CentOS Linux	Básico	`@X Window System`
		`@Desktop`
		`@Fonts`
		`compat-libstdc++-33`
		`compat-libstdc++-33.i686`
		`compat-libstdc++-296`
		`libstdc++.i686`
		`pam.i686`	

	Mínimo	`compat-libstdc++-33`
		`compat-libstdc++-33.i686`
		`compat-libstdc++-296`
		`libstdc++.i686`
		`pam.i686`	

	Virtualización	`%packages`
		`@virtualization`
		`@virtualization-client`
		`@virtualization-platform`
		`@virtualization-tools`
		`# begin additional packages`
		`@basic-desktop`
		`@desktop-debugging`
		`@desktop-platform`
		`@fonts`
		`@general-desktop`
		`@graphical-admin-tools`
		`@kde-desktop`
		`@remote-desktop-clients`
		`@x11`
		`@^graphical-server-environment`
		`@gnome-desktop`
		`@x11`
		`@virtualization-client`
		`# end additional packages`
			`libconfig`
			`libsysfs`
			`libicu`
			`lm_sensors-libs`
			`net-snmp`
			`net-snmp-libs`
			`redhat-lsb`
			`compat-libstdc++-33`
			`compat-libstdc++-296`
			`# begin additional rpms`
			`xterm`
			`xorg-x11-xdm`
			`rdesktop`
			`tigervnc-server`
			`device-mapper-multipath`
			`# end additional rpms`

Sistema operativo	Perfil de	Paquetes incluidos en el perfil

Microsoft® Windows® Azure Stack HCI	Azure	`<selection name="Microsoft-Hyper-V" state="true" />`
		`<selection name="MultipathIo" state="true" />`
		`<selection name="FailoverCluster-PowerShell" state="true" />`
		`<selection name="FailoverCluster-FullServer" state="true" />`
		`<selection name="FailoverCluster-CmdInterface" state="true" />`
		`<selection name="FailoverCluster-AutomationServer" state="true" />`
		`<selection name="FailoverCluster-AdminPak" state="true" />`
		`<selection name="Containers" state="true" />`
		`<selection name="MicrosoftWindowsPowerShellRoot" state="true" />`
		`<selection name="MicrosoftWindowsPowerShell" state="true" />`
		`<selection name="ServerManager-Core-RSAT" state="true" />`
		`<selection name="ServerManager-Core-RSAT-Role-Tools" state="true" />`

Cliente de Microsoft Windows	Enterprise	
	Enterprise N	
	Workstations Pro	
	Worksta-tions_Pro N	

Microsoft Windows Hyper-V Server 2016	Hyper_V	`<selection name="Microsoft-Hyper-V" state="true" />`
		`<selection name="MultipathIo" state="true" />`
		`<selection name="FailoverCluster-PowerShell" state="true" />`
		`<selection name="FailoverCluster-FullServer" state="true" />`
		`<selection name="FailoverCluster-CmdInterface" state="true" />`
		`<selection name="FailoverCluster-AutomationServer" state="true" />`
		`<selection name="FailoverCluster-AdminPak" state="true" />`
		`<selection name="MicrosoftWindowsPowerShellRoot" state="true" />`
		`<selection name="MicrosoftWindowsPowerShell" state="true" />`
		`<selection name="ServerManager-Core-RSAT" state="true" />`
		`<selection name="ServerManager-Core-RSAT-Role-Tools" state="true" />`

Microsoft Windows Server **Nota:** Incluye Hyper-V mediante el *Perfil de virtualización*.	Centro de datos	`GUI`
	Virtualización del centro de datos	`GUI` `Hyper-V role`
	Núcleo de la virtualización del centro de datos	`Hyper-V role`
	Núcleo del centro de datos	
	Estándar	`GUI`
	Virtualización estándar	`GUI` `Hyper-V role`
	Núcleo de la virtualización estándar	`Hyper-V role`
	Núcleo estándar	

Sistema operativo	Perfil de	Paquetes incluidos en el perfil	
Microsoft Windows Server personalizado	Datacenter_ customized		
	Standard_ customized		

Red Hat Enterprise Linux (RHEL) **Nota:** Incluye KVM	Básico	`@X Window System`
		`@Desktop`
		`@Fonts`
		`compat-libstdc++-33`
		`compat-libstdc++-33.i686`
		`compat-libstdc++-296`
		`libstdc++.i686`
		`pam.i686`	

	Mínimo	`compat-libstdc++-33`
		`compat-libstdc++-33.i686`
		`compat-libstdc++-296`
		`libstdc++.i686`
		`pam.i686`	

	Virtualización	`%packages`
		`@virtualization`
		`@virtualization-client`
		`@virtualization-platform`
		`@virtualization-tools`
		`# begin additional packages`
		`@basic-desktop`
		`@desktop-debugging`
		`@desktop-platform`
		`@fonts`
		`@general-desktop`
		`@graphical-admin-tools`
		`@kde-desktop`
		`@remote-desktop-clients`
		`@x11`
		`@^graphical-server-environment`
		`@gnome-desktop`
		`@x11`
		`@virtualization-client`
		`# end additional packages`
			`libconfig`
			`libsysfs`
			`libicu`
			`lm_sensors-libs`
			`net-snmp`
			`net-snmp-libs`
			`redhat-lsb`
			`compat-libstdc++-33`
			`compat-libstdc++-296`
			`# begin additional rpms`
			`xterm`
			`xorg-x11-xdm`
			`rdesktop`
			`tigervnc-server`
			`device-mapper-multipath`
			`# end additional rpms`

Rocky Linux	Básico	`@X Window System`
		`@Desktop`
		`@Fonts`
		`compat-libstdc++-33`
		`compat-libstdc++-33.i686`
		`compat-libstdc++-296`
		`libstdc++.i686`
		`pam.i686`	

	Mínimo	`compat-libstdc++-33`
		`compat-libstdc++-33.i686`
		`compat-libstdc++-296`
		`libstdc++.i686`
		`pam.i686`	

Sistema operativo	Perfil de	Paquetes incluidos en el perfil	
	Virtualización	%packages @virtualization @virtualization-client @virtualization-platform @virtualization-tools # begin additional packages @basic-desktop @desktop-debugging @desktop-platform @fonts @general-desktop @graphical-admin-tools @kde-desktop @remote-desktop-clients @x11 @^graphical-server-environment @gnome-desktop @x11 @virtualization-client # end additional packages	libconfig libsysfs libicu lm_sensors-libs net-snmp net-snmp-libs redhat-lsb compat-libstdc++-33 compat-libstdc++-296 # begin additional rpms xterm xorg-x11-xdm rdesktop tigervnc-server device-mapper-multipath # end additional rpms
SUSE Linux Enterprise Server (SLES) 15	Básicos y básica	<pattern>apparmor</pattern> <pattern>devel_basis</pattern> <pattern>enhanced_base</pattern> <pattern>base</pattern> <pattern>basesystem</pattern> <pattern>minimal_base</pattern> <pattern>print_server</pattern> <pattern>sw_management</pattern> <pattern>x11</pattern> <pattern>x11_enhanced</pattern> <pattern>x11_yast</pattern> <pattern>yast2_basis</pattern> <package>wget</package>	
	Mínimo y mínimo	<pattern>base</pattern> <pattern>minimal_base</pattern> <pattern>yast2_basis</pattern> <package>wget</package>	
	Virtualización - KVM y Virtualización - KVM	<pattern>apparmor</pattern> <pattern>devel_basis</pattern> <pattern>enhanced_base</pattern> <pattern>base</pattern> <pattern>basesystem</pattern> <pattern>minimal_base</pattern> <pattern>print_server</pattern> <pattern>sw_management</pattern> <pattern>x11</pattern> <pattern>x11_enhanced</pattern> <pattern>x11_yast</pattern> <pattern>yast2_basis</pattern> <pattern>xen_server</pattern> <pattern>xen_tools</pattern> <package>wget</package>	

Sistema operativo	Perfil de	Paquetes incluidos en el perfil
	Virtualización - Xen y Virtualización - Xen	<pattern>apparmor</pattern> <pattern>devel_basis</pattern> <pattern>enhanced_base</pattern> <pattern>base</pattern> <pattern>basesystem</pattern> <pattern>minimal_base</pattern> <pattern>print_server</pattern> <pattern>sw_management</pattern> <pattern>x11</pattern> <pattern>x11_enhanced</pattern> <pattern>x11_yast</pattern> <pattern>yast2_basis</pattern> <pattern>xen_server</pattern> <pattern>xen_tools</pattern> <package>wget</package>
Ubuntu	Mínimo	OpenSSH: servidor
	Virtualización	qemu qemu-kvm libvirt-daemon libvirt-clients bridge-utils virt-manager
VMware vSphere® Hypervisor (ESXi)	Virtualización	Se admiten imágenes base de VMware vSphere Hypervisor (ESXi) e imágenes personalizadas de Lenovo VMware ESXi.

Disponibilidad de puertos para sistemas operativos desplegados

Algunos perfiles de los sistemas operativos bloquean ciertos puertos. En las tablas siguientes se muestra una lista de los puertos que deben estar abiertos (desbloqueados).

Comunicación	Perfil de virtualización de RHEL, Centos y Rocky[1]	Perfiles básicos y mínimos de RHEL, Centos y Rocky[1]	Perfiles de virtualización, básicos y mínimos de SLES[2]	Perfiles de virtualización, básicos y mínimos de Ubuntu[3]	Perfil de virtualización VMware ESXi[4]	Perfiles de Windows
Salida (puertos abiertos en sistemas externos)	• Comunicación con dispositivos de red RHEL KVM: TCP y UDP en los puertos **53** y **67** • Comunicación con agentes SNMP: UDP en el puerto **161** • Comunicación con el agente de servicio SLP, agente de directorio SLP: TCP y UDP en el puerto **427** • Comunicación de CIM-XML sobre HTTP: TCP en los puertos **15988** y **15989** • Comunicación del servidor virtual KVM: TCP en los puertos **49152 a 49215**					• Comunicación de SMB: TCP en el puerto **445**
Entrada (puertos abiertos en el dispositivo	• SSH: TCP en el puerto **22** • Dispositivos de red RHEL KVM: TCP y UDP en los puertos **53** y **67**	• SSH: TCP en el puerto **22** • Despliegue del SO: TCP y UDP en los puertos **445, 3900** y **8443**	• Despliegue del SO: TCP y UDP en los puertos **445, 3900** y **8443**	• Despliegue del SO: TCP y UDP en los puertos **445, 3900** y **8443**	• Despliegue del SO: TCP y UDP en los puertos **445, 3900** y **8443**	• Despliegue del SO: TCP y UDP en los puertos **445, 3900** y **8443**

Comunicación	Perfil de virtualización de RHEL, Centos y Rocky[1]	Perfiles básicos y mínimos de RHEL, Centos y Rocky[1]	Perfiles de virtualización, básicos y mínimos de SLES[2]	Perfiles de virtualización, básicos y mínimos de Ubuntu[3]	Perfil de virtualización VMware ESXi[4]	Perfiles de Windows
XClarity Administrator)	• Agentes SNMP: UDP en el puerto **162** • Despliegue del SO: TCP y UDP en los puertos **445, 3900** y **8443** • Agente de servicio SLP, agente de directorio SLP: TCP y UDP en el puerto **427** • Servidor virtual KVM: TCP en los puertos **49152 a 49215**					

1. De forma predeterminada, los perfiles de Red Hat Enterprise Linux (RHEL) bloquean todos los puertos excepto los que se indican en la tabla siguiente.
2. Para SUSE Linux Enterprise Server (SLES), algunos puertos abiertos se asignan de forma dinámica, a partir de la versión del sistema operativo y los perfiles. Para obtener una lista completa de los puertos abiertos, consulte la documentación de SUSE Linux Enterprise Server.
3. Para el servidor Ubuntu Linux, algunos puertos abiertos se asignan de forma dinámica, a partir de la versión del sistema operativo y los perfiles. Para obtener una lista completa de los puertos abiertos, consulte la documentación del servidor Ubuntu.
4. Para obtener una lista completa de los puertos abiertos para VMware vSphere Hypervisor (ESXi) con personalización de Lenovo, consulte la documentación de VMware para ESXi en el Sitio web de la base de conocimiento de VMware.

Configurar un servidor de archivo remoto

Puede importar imágenes del SO, controladores de dispositivos y archivos de arranque en el repositorio de imágenes del SO desde el sistema local o desde un servidor de archivo remoto. Para importar archivos desde un servidor de archivo remoto, primero debe crear un perfil que se utilice para autenticar la conexión con el servidor de archivo remoto.

Acerca de esta tarea

Se admiten los algoritmos criptográficos siguientes:
- RSA–2048 bits
- RSA–4096 bits
- ECDSA–521 bits (curva secp521r1)

Se admiten los siguientes protocolos:

- HTTP sin autenticación.
- HTTP con autenticación básica.
- HTTPS (validación del certificado) con autenticación básica.
- HTTPS (validación del certificado) sin autenticación.
- FTP con autenticación de contraseña.
- SFTP (validación del cliente) con autenticación de contraseña.
- SFTP (validación del cliente) con autenticación de clave pública

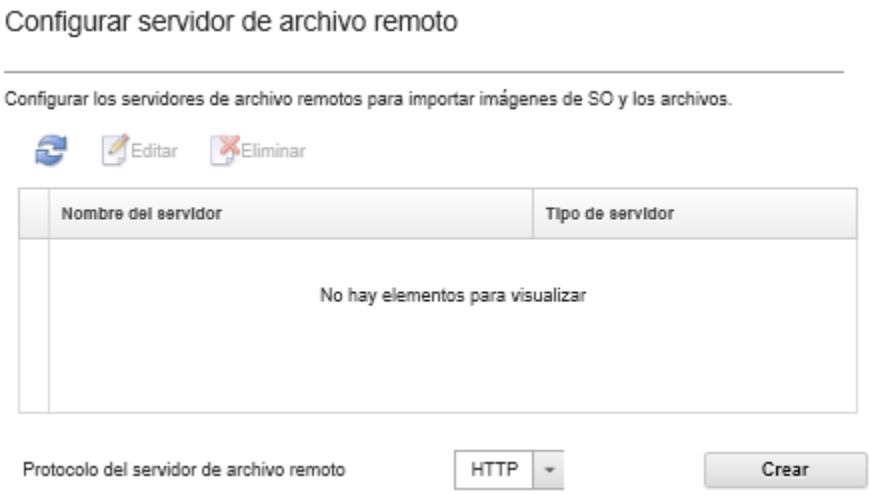
Para la autenticación de clave pública SFTP y la validación del certificado HTTPS, Lenovo XClarity Administrator valida el certificado del servidor de archivo remoto. Si el certificado del servidor no se encuentra en el almacén de confianza, se le solicitará que acepte el certificado del servidor y lo agregue al almacén de confianza. Para obtener información acerca de la resolución de problemas de validación, consulte La validación de la certificación del servidor falla en la documentación en línea de XClarity Administrator.

Procedimiento

Para configurar un servidor de archivo remoto, lleve a cabo los pasos siguientes.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Gestionar imágenes de SO** para mostrar la página Desplegar sistema operativo: Gestionar imágenes de SO.

Paso 2. Haga clic en el icono **Configurar el servidor de archivo** ( ) para mostrar el cuadro de diálogo Configurar el servidor de archivo remoto.



Paso 3. Seleccione el protocolo para el servidor de archivo remoto de la lista **Protocolo del servidor de archivo remoto**.

Paso 4. Haga clic en **Crear**. Se muestra el cuadro de diálogo Configurar el servidor de archivo remoto.

Nota: Este cuadro de diálogo será diferente según el protocolo que haya seleccionado.

Paso 5. Ingrese el nombre, la dirección y el puerto del servidor.

Paso 6. Para HTTP, HTTPS, FTP y SFTP con autenticación básica, ingrese un nombre de usuario y contraseña en caso de que se le solicite autenticarse para acceder al servidor.

Paso 7. Para SFTP con autenticación básica, haga clic en **Validar certificado del servidor** para obtener la firma de clave pública.

Nota: Puede aparecer un cuadro de diálogo que le indicará que el proceso de despliegue del SO no confía en la clave pública del servidor de archivos SFTP. Haga clic en **Aceptar** para almacenar y dar confianza en la clave pública SFTP en el almacenamiento de claves de confianza de despliegue

de SO. Si se realiza correctamente, la firma de clave pública se muestra en el campo **Firma de la clave pública del servidor SFTP**.

Paso 8. Para SFTP con autenticación de clave pública:

a. Ingrese una frase de paso y contraseña y seleccione el tipo de clave si se requiere una autenticación para acceder al servidor.

b. Haga clic en **Generar la clave del servidor de gestión** para obtener la firma de clave pública.

c. Copie la clave generada en el archivo authorized_keys del servidor de archivo remoto SFTP.

d. Seleccione la casilla de verificación **La clave de gestión se copió en el servidor** en XClarity Administrator.

e. Haga clic en **Validar certificado del servidor** para validar la firma de clave pública.

Nota: Puede aparecer un cuadro de diálogo que le indicará que el proceso de despliegue del SO no confía en la clave pública del servidor de archivos SFTP. Haga clic en **Aceptar** para almacenar y dar confianza en la clave pública SFTP en el almacenamiento de claves de confianza de despliegue de SO. Si se realiza correctamente, la firma de clave pública se muestra en el campo **Firma de la clave pública del servidor SFTP**.

f. Haga clic en **Guardar**.

Paso 9. Haga clic en **Guardar servidor**.

Después de finalizar

En el cuadro de diálogo Configurar servidor de archivos remotos, puede llevar a cabo las siguientes acciones:

- Actualizar la lista de servidor de archivos remotos pulsando el icono **Actualizar** ( ).
- Modificar un servidor de archivos remotos seleccionado pulsando el icono **Editar** ( ).
- Quitar un servidor de archivos remotos seleccionado pulsando el icono **Eliminar** ( ).

Importación de imágenes del sistema operativo

Antes de que puedan desplegar un sistema operativo con licencia para servidores gestionados, se debe importar la imagen en el Repositorio de imágenes del SO de XClarity Administrator.

Acerca de esta tarea

Para obtener información acerca de las imágenes del sistema operativo que se pueden importar y desplegar, consulte Sistemas operativos compatibles.

Para ver una lista de los sistemas operativos básicos y personalizados compatibles, consulte Sistemas operativos compatiblesSistemas operativos compatibles en la documentación en línea de Lenovo XClarity Administrator.

Solo se puede importar una imagen a la vez. Espere a que la imagen se muestre en el Repositorio de imágenes del SO antes de intentar importar otra. La importación del sistema operativo puede tardar.

Únicamente para ESXi, puede importar varias imágenes de ESXi con la misma versión principal/menor al repositorio de imágenes de SO.

Únicamente para ESXi, puede importar varias imágenes de ESXi personalizadas con la misma versión principal/menor y número de build al repositorio de imágenes de SO.

Cuando se importa la imagen de un sistema operativo, XClarity Administrator:

- Asegúrese de que haya espacio suficiente en el Repositorio de imágenes del SO antes de importar el sistema operativo. En caso negativo, elimine una imagen existente del repositorio y vuelva a intentar importar la nueva.
- Crea uno o varios perfiles de esa imagen y lo almacena en el Repositorio de imágenes del SO. Cada *perfil* incluye opciones de imagen del SO e instalación. Para obtener más información acerca de los perfiles de imagen del SO predefinidos, consulte Perfiles de las imágenes del sistema operativo.

Nota: Los navegadores web Internet Explorer y Microsoft Edge tienen un límite de carga de 4 GB. Si el archivo que desea importar es mayor a 4 GB, considere usar otro navegador web (por ejemplo, Chrome o Firefox) o copie el archivo a un servidor de archivo remoto e importe el archivo mediante la opción **Importación remota**.

Procedimiento

Lleve a cabo los pasos siguientes para importar una imagen del sistema operativo al Repositorio de imágenes del SO.

Paso 1. Obtenga una imagen ISO con licencia del sistema operativo.

Nota: El usuario es responsable de obtener las licencias aplicables del sistema operativo.

Paso 2. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Gestionar imágenes de SO** para mostrar la página Desplegar sistemas operativos: Gestionar imágenes de SO.

Paso 3. Haga clic en el icono de **Importar archivos** () para mostrar el cuadro de diálogo Importar imágenes y archivos del SO.

Paso 4. Haga clic en la pestaña **Local** para cargar archivos del sistema local, o haga clic en la pestaña **Remoto** para cargar archivos desde un servidor de archivo remoto.

Nota: Para cargar un archivo desde un servidor de archivo remoto, debe crear primero un perfil del servidor de archivo remoto pulsando el icono **Configurar servidor de archivo** (). Para obtener más información, consulte el apartado Configurar un servidor de archivo remoto .

Paso 5. Si desea utilizar un servidor de archivo remoto, seleccione el servidor que desea utilizar desde la lista **Servidor de archivo remoto**.

Paso 6. Ingrese el nombre del archivo y la ruta de la imagen ISO o haga clic en **Examinar** para buscar la imagen ISO que desee importar.

Si elige utilizar el *servidor de archivo local*, debe especificar la ruta absoluta en el archivo de imagen ISO. Si eligió utilizar un *servidor de archivo remoto*, debe especificar la ruta absoluta (por ejemplo, `/home/user/isos.osimage.iso`) o la ruta relativa (por ejemplo, `/isos.osimage.iso`) en el archivo de la imagen ISO (según la configuración del servidor de archivo remoto). Si no se encuentra el archivo, compruebe que la ruta del archivo es correcta y vuelva a intentarlo.

Paso 7. **Opcional:** Ingrese una descripción para la imagen del SO.

Paso 8. **Opcional:** Seleccione un tipo de suma de comprobación para asegurarse de que la imagen ISO que se está importando a XClarity Administrator no está dañada y, a continuación, copie y pegue el valor de suma de comprobación en el campo de texto previsto a tal fin.

Si selecciona un tipo de suma de comprobación, debe especificar un valor de suma de comprobación para comprobar la integridad y la seguridad de la imagen del SO cargada. El valor debe proceder de una fuente segura de una organización de su confianza. Si la imagen cargada concuerda con el valor de suma de comprobación, puede realizar el despliegue con total

tranquilidad. De lo contrario, deberá cargar de nuevo la imagen o comprobar el valor de la suma de comprobación.

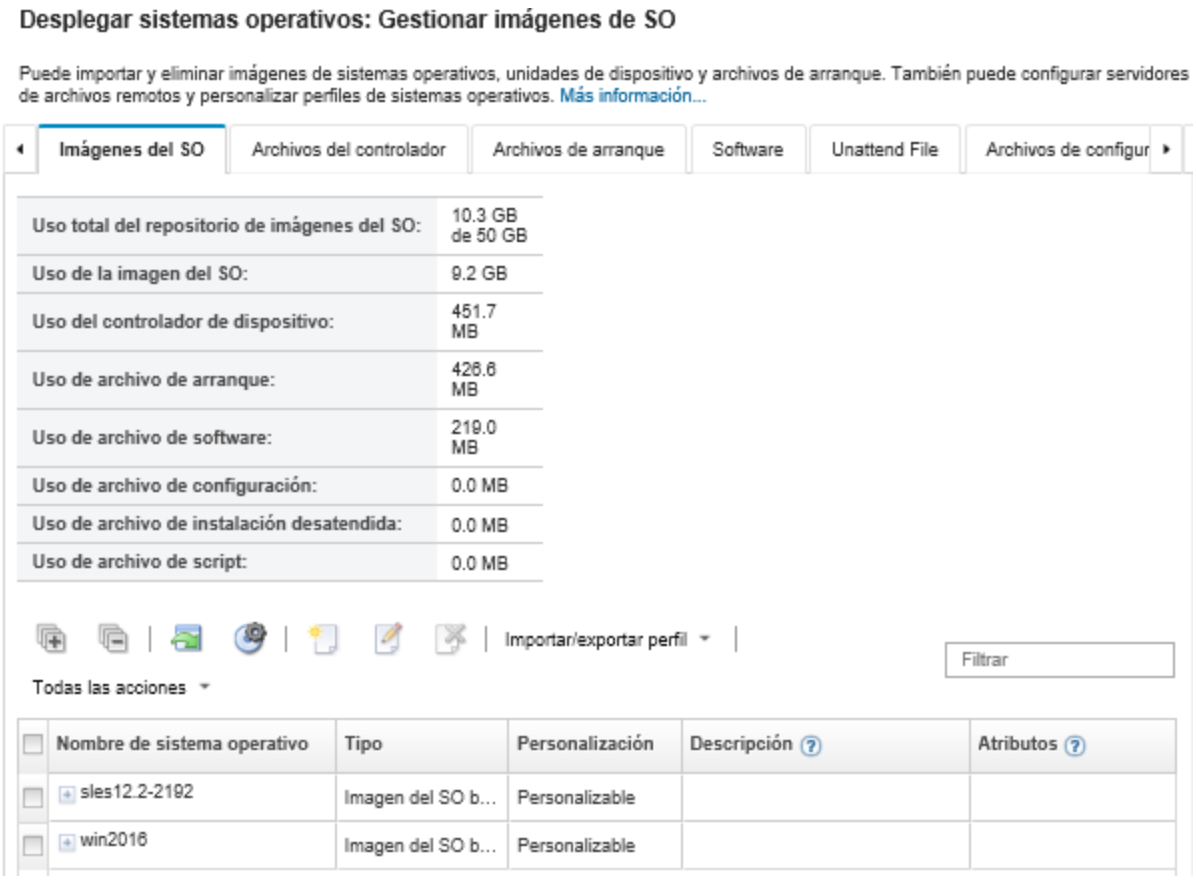
Se admiten tres tipos de suma de comprobación:
- **MD5**
- **SHA1**
- **SHA256**

Paso 9. Haga clic en **Importar**.

Consejo: La imagen ISO se carga a través de una conexión de red segura. Por consiguiente, la fiabilidad y el rendimiento de la red afectan al tiempo que tarda en importarse la imagen. Si cierra la pestaña del navegador web o la ventana en la que se está cargando la imagen del sistema operativo antes de que finalice el proceso, la importación fallará.

Resultados

XClarity Administrator carga la imagen del SO y crea un perfil de imagen en el Repositorio de imágenes del SO.



Desde esta página puede llevar a cabo las siguientes acciones.

- Crear un perfil del servidor de servidor de archivo pulsando el icono **Configurar servidor de archivo** ( ).
- Personalizar una imagen del SO pulsando el icono **Crear perfil personalizado** ( ).
- Modificar una imagen del SO pulsando el icono **Editar** ( ).

- Importar un perfil de imagen del SO personalizado y aplíquelo a una imagen del SO base al hacer clic en **Importar/Exportar perfil → Importar imagen de perfil personalizada** (consulte Importación de un perfil de imagen del SO personalizado).
- Para eliminar una imagen de SO o un perfil de imagen de SO seleccionada, haga clic en el icono **Eliminar** ().
- Exportar un perfil de imagen del SO personalizado seleccionado al hacer clic en **Importar/Exportar perfil → Exportar imagen de perfil personalizada**.

Nota: Cuando importe imágenes del servidor de Windows, también debe importar el archivo de conjunto asociado. Lenovo incluye el archivo de arranque predefinido WinPE_64.wim junto con un conjunto de controladores de dispositivos en un único paquete que puede descargarse desde el Página web del repositorio de controladores de Lenovo Windows e imágenes de WinPE y luego importarse al repositorio de imágenes del SO. Si el archivo de paquete contiene los controladores de dispositivos y archivos de arranque, puede importar el archivo de conjunto desde la pestaña **Controlador de dispositivo** o **Archivos de arranque**.. Para obtener más información, consulte los apartados Importar archivos de arranque y Importación de controladores de dispositivos.

Personalización de los perfiles de la imagen del SO

Un *sistema operativo base* es la imagen completa de un SO importado al repositorio de imágenes de SO. La imagen de base importada contiene perfiles predefinidos que describen las configuraciones de instalación de dicha imagen. También se puede crear perfiles personalizados en la imagen de SO base que se pueden desplegar para configuraciones específicas. El perfil personalizado contiene los archivos personalizados y las opciones de instalación.

Nota: No se puede crear un perfil de imagen de SO personalizada para una imagen personalizada de Microsoft Windows Server.

Varios de los escenarios de ejemplo de personalización y despliegue de imágenes de SO, que incluyen a Windows y SLES, solo están disponibles en inglés. Para obtener más información, consulte Escenarios integrales para configurar dispositivos nuevos.

Se puede agregar los siguientes tipos de archivos a un perfil de imagen de SO personalizado.

- **Archivos de arranque**

  Un archivo de arranque actúa como el entorno de arranque de instalación. Para Windows, este es un archivo de instalación previa de Windows (WinPE). Se requiere un archivo de arranque de WinPE desplegar Windows

  Lenovo XClarity Administrator admite archivos de arranque predefinidos y personalizados.

  – **Archivos de arranque de predefinidos**. Lenovo proporciona un archivo de arranque WinPE_64.wim que puede utilizarse para desplegar perfiles de imagen del SO predefinidos.

    Lenovo incluye el archivo de arranque predefinido WinPE_64.wim junto con un conjunto de controladores de dispositivos en un único paquete que puede descargarse desde el Página web del repositorio de controladores de Lenovo Windows e imágenes de WinPE y luego importarse al repositorio de imágenes del SO. Si el archivo de paquete contiene los controladores de dispositivos y archivos de arranque, puede importar el archivo de conjunto desde la pestaña **Controlador de dispositivo** o **Archivos de arranque**.

    Notas:

    – No se precarga un archivo de arranque predefinido con XClarity Administrator. Debe importar un archivo de arranque en el repositorio de imágenes del SO antes de poder desplegar un perfil de Windows.

  - No puede eliminar los archivos de arranque predefinido que se cargaron cuando instaló XClarity Administrator; sin embargo, puede eliminar los archivos de arranque predefinido que se importaron en un conjunto de Lenovo.
  - XClarity Administrator requiere que los archivos de paquete importados estén firmados por Lenovo. Al importar un archivo de paquete, también se debe importar un archivo de firma .asc.
- **Archivos de arranque personalizados**. También puede crear un archivo de arranque de WinPE para personalizar las opciones de arranque de un despliegue de Windows. Luego puede agregar el archivo de arranque para los perfiles de Windows personalizados.

  XClarity Administrator proporciona scripts para crear archivos de arranque en el formato correcto. Para obtener información acerca de la creación de un archivo de arranque personalizado, Creación de un archivo de arranque (WinPE) consulte Sitio web de introducción a Windows PE (WinPE).

  Se admiten los siguientes tipos de archivo para importar archivos de arranque personalizados.

Sistema operativo	Tipos de archivo de arranque compatibles	Tipos de archivo de paquete compatibles
CentOS Linux	No admitido	No admitido
Microsoft® Windows® Azure Stack HCI	No admitido	No admitido
Microsoft Windows Hyper-V Server	Un archivo .zip que contiene un archivo de WinPE que se crea mediante el script **genimage.cmd**	Un archivo .zip que contiene controladores de dispositivos y archivos de arranque
Microsoft Windows Server	Un archivo .zip que contiene un archivo de WinPE que se crea mediante el script **genimage.cmd**	Un archivo .zip que contiene controladores de dispositivos y archivos de arranque
Servidor Red Hat® Enterprise Linux (RHEL)	No admitido	No admitido
Rocky Linux	No admitido	No admitido
SUSE® Linux Enterprise Server (SLES)	No admitido	No admitido
Ubuntu	No admitido	No admitido
VMware vSphere® Hypervisor (ESXi) con personalización de Lenovo	No admitido	No admitido

- **Controladores de dispositivo**

  La imagen del sistema operativo que está instalando desplegar incluye los controladores de Ethernet, Fibre Channel y dispositivo de adaptador de almacenamiento para su hardware. Si el controlador de dispositivo del adaptador de E/S no está incluido en la imagen o el perfil del sistema operativo, el adaptador no es compatible con el despliegue del SO. También puede crear perfiles de imagen del SO personalizados que incluyen los controladores de dispositivo que necesita.

  Lenovo XClarity Administrator es compatible con controladores de dispositivos incorporados y controladores de dispositivos listos para usar predefinidos y personalizados.

  - **Controladores de dispositivos incorporados**. XClarity Administrator no gestiona los controladores de dispositivos. Siempre instale el sistema operativo más reciente para garantizar que cuente con los controladores de dispositivos incorporados más recientes que necesita.

    Nota: Puede agregar controladores de dispositivos incorporados a un perfil de Windows personalizado al crear un archivo de arranque de WinPE personalizado y copiar los archivos del

controlador de dispositivo al sistema del host en el directorio `C:\drivers`. Cuando se crea un perfil de imágenes del SO personalizado que utiliza el archivo de arranque personalizado, los controladores de dispositivo en el directorio C:\drivers se incluyen en WinPE y en el SO final. Ambos se tratan como si fueran predefinidos. Por lo tanto, no es necesario importar estos controladores de dispositivos incorporados en XClarity Administrator al especificar los controladores de dispositivos para utilizarlos en la creación de perfiles personalizados de imágenes del SO.

- **Controladores de dispositivos predefinidos**. Para los servidores de ThinkSystem, XClarity Administrator viene precargado con un conjunto de controladores de dispositivo listos para usar para Linux para permitir la instalación del sistema operativo, así como la configuración básica de red y de almacenamiento para el sistema operativo final. Puede añadir estos controladores de dispositivos predefinidos para los perfiles de imagen del SO personalizados y desplegar los perfiles en los servidores gestionados

  Lenovo también empaqueta conjuntos de controladores de dispositivos predefinidos en un único paquete que puede descargarse desde el Página web del repositorio de controladores de Lenovo Windows e imágenes de WinPE y luego importarlos al repositorio de imágenes del SO. En la actualidad, los archivos de paquete están disponibles solo para Windows. Si el archivo de paquete contiene los controladores de dispositivos y archivos de arranque, puede importar el archivo de conjunto desde la pestaña **Controlador de dispositivo** o **Imagen de arranque**.

  Notas:

  - De forma predeterminada, los perfiles de imagen del SO predefinidos incluyen controladores de dispositivos predefinidos.
  - No puede eliminar los controladores de dispositivos predefinidos que se cargaron cuando instaló XClarity Administrator; sin embargo, puede eliminar los controladores de dispositivos predefinidos que se importaron en un conjunto de Lenovo.
  - XClarity Administrator requiere que los archivos de paquete importados estén firmados por Lenovo. Al importar un archivo de paquete, también se debe importar un archivo de firma .asc.
- **Controladores de dispositivos personalizados**. Puede importar controladores de dispositivos listos para usar en el repositorio de imágenes del SO y luego agregar los controladores de dispositivos a un perfil de imagen del SO personalizado.

  Puede obtener controladores de dispositivos desde Página web del repositorio de Lenovo YUM, desde un proveedor (como Red Hat) o mediante un controlador de dispositivo personalizado que generó por su cuenta. Para algunos controladores de dispositivos de Windows, puede generar un controlador de dispositivo personalizado al extraer el controlador de dispositivo del exe de instalación a su sistema local y crear un archivo .zip.

  Se admiten los siguientes tipos de archivo para importar archivos de controlador de dispositivo.

Sistema operativo	Tipos de archivos de Controlador de dispositivo admitidos
CentOS Linux	No admitido
Microsoft® Windows® Azure Stack HCI	No admitido
Microsoft Windows Hyper-V Server	Un archivo .zip que contenga los archivos originales del controlador de dispositivo, que generalmente son conjuntos de archivos.inf, .cat y .dll.
Microsoft Windows Server	Un archivo .zip que contenga los archivos originales del controlador de dispositivo, que generalmente son conjuntos de archivos.inf, .cat y .dll.

Sistema operativo	Tipos de archivos de Controlador de dispositivo admitidos
Servidor Red Hat® Enterprise Linux (RHEL)	Disco de actualización de controlador (DUD) en formato de imagen .iso o .rpm **Nota:** Si se aplica un DUD .rpm al perfil personalizado, el .rpm solo se instala en el último sistema operativo. No se instala en el entorno de instalación (initrd). Para instalar a un controlador de dispositivo personalizado para initrd, importe un DUD .iso y aplique el .iso al perfil personalizado.
Rocky Linux	No admitido
SUSE® Linux Enterprise Server (SLES)	Disco de actualización de controlador (DUD) .rpm en formato de imagen .iso **Nota:** Si se aplica un DUD .rpm al perfil personalizado, el .rpm solo se instala en el último sistema operativo. No se instala en el entorno de instalación (initrd). Para instalar a un controlador de dispositivo personalizado para initrd, importe un DUD .iso y aplique el .iso al perfil personalizado.
Ubuntu	No admitido
VMware vSphere® Hypervisor (ESXi) con personalización de Lenovo	Controladores de dispositivos en formato de imagen .vib

Nota: El repositorio de imágenes del SO puede almacenar un número ilimitado de archivos predefinidos y personalizados, en caso que haya espacio disponible para almacenar los archivos.

- **Valores de configuración personalizada**

  Valores de configuración describe los datos que se deben recopilar dinámicamente durante el despliegue del SO. Lenovo XClarity Administrator utiliza un conjunto de valores de configuración predefinidos, lo que incluye valores global, de redes y de ubicación de almacenamiento. Puede utilizar estos valores de configuración predefinidos y agregar valores de configuración personalizada que no están disponibles en el XClarity Administrator.

  Los valores de configuración personalizada se definen a modo de un esquema JSON. El esquema debe adherir a las especificaciones de JSON.

  Al importar valores de configuración personalizada para XClarity Administrator, XClarity Administrator valida el esquema JSON. Si la validación se realiza correctamente, XClarity Administrator genera macros personalizadas para cada valor.

  Puede utilizar las macros personalizadas en el archivo de instalación desatendida y el script de instalación posterior.

  En archivos de instalación desatendida

  Puede asociar el archivo de configuración personalizado a un archivo de instalación desatendida e incluir estas macros personalizadas (y macros predefinidas) en el archivo de instalación desatendida.

  Puede añadir uno o varios archivos de opciones de configuración personalizada en un perfil personalizado. Al desplegar el perfil de SO en un grupo de servidores de destino, puede elegir el archivo de configuración que desea utilizar. XClarity Administrator representa la pestaña **Configuración personalizada** en el cuadro de diálogo Desplegar imágenes de SO en función del esquema JSON en el archivo de valores de configuración y le permite especificar los valores específicos de la configuración (objeto JSON) que se define en el archivo.

  Nota: El despliegue del SO no se llevará a cabo si en la entrada no se especifica ningún valor de configuración personalizada necesaria.

En los scripts de instalación posterior

Después de recopilar los datos durante el despliegue del SO, XClarity Administrator crea una instancia del archivo de configuración (lo que incluye la configuración personalizada del archivo seleccionado y un subconjunto de valores predefinidos) en el sistema host que se puede utilizar en el script de instalación posterior.

Notas:

- El archivo de configuración es único para un perfil de imagen de SO personalizado.
- No se puede modificar los valores de configuración para perfiles de imagen de SO predefinidos.
- Los valores de configuración se admiten solo para los siguientes sistemas operativos:
  - Microsoft® Windows® Server
  - Servidor Red Hat® Enterprise Linux (RHEL)
  - Rocky Linux
  - SUSE® Linux Enterprise Server (SLES)
  - VMware vSphere® Hypervisor (ESXi) con personalización de Lenovo 6.0u3 y actualizaciones posteriores y 6.5 y posteriores.

El repositorio de imágenes del SO puede almacenar un número ilimitado de archivos predefinidos y personalizados, en caso que haya espacio disponible para almacenar los archivos.

- **Archivos de instalación desatendida personalizados**

  Puede personalizar los perfiles de imágenes de SO de modo que utilicen los archivos de instalación desatendida para automatizar el despliegue del sistema operativo.

  Se admite los siguientes tipos de archivo para archivos de instalación desatendida estándar.

Sistema operativo	Tipos de archivo compatibles	Más información
CentOS Linux	No admitido	
Microsoft® Windows® Azure Stack HCI	No admitido	
Microsoft Windows Hyper-V Server	No admitido	
Microsoft Windows Server	Instalación desatendida (.xml)	Para obtener más información acerca de los archivos de instalación desatendida, consulte Página Web de referencia de instalación desatendida de Windows.

Sistema operativo	Tipos de archivo compatibles	Más información
Servidor Red Hat® Enterprise Linux (RHEL)	Comenzar (.cfg)	Para obtener más información acerca de los archivos de instalación desatendida, consulte Página web de Red Hat: Automatización de la instalación con Kickstart . Considere lo siguiente cuando agregue secciones %pre, % post, %firstboot al archivo. – Puede incluir múltiples secciones %pre, %post, % firstboot al archivo desatendido; sin embargo, tenga en cuenta el orden de las secciones. – Cuando la macro recomendada **#predefined. unattendSettings.preinstallConfig#** esté presente en el archivo desatendido, XClarity Administrator agrega una sección %pre antes de todos las otras secciones %pre en el archivo. – Cuando la macro recomendada **#predefined. unattendSettings.postinstallConfig#** está presente en el archivo desatendido, XClarity Administrator agrega secciones %post y %firstboot antes de todas los otras secciones %post y %firstboot en el archivo.
Rocky Linux	Comenzar (.cfg)	Para obtener más información acerca de los archivos de instalación desatendida, consulte Página web de Red Hat: Automatización de la instalación con Kickstart . Considere lo siguiente cuando agregue secciones %pre, % post, %firstboot al archivo. – Puede incluir múltiples secciones %pre, %post, % firstboot al archivo desatendido; sin embargo, tenga en cuenta el orden de las secciones. – Cuando la macro recomendada **#predefined. unattendSettings.preinstallConfig#** esté presente en el archivo desatendido, XClarity Administrator agrega una sección %pre antes de todos las otras secciones %pre en el archivo. – Cuando la macro recomendada **#predefined. unattendSettings.postinstallConfig#** está presente en el archivo desatendido, XClarity Administrator agrega secciones %post y %firstboot antes de todas los otras secciones %post y %firstboot en el archivo.
SUSE® Linux Enterprise Server (SLES)	AutoYast (.xml)	Para obtener más información acerca de los archivos de instalación desatendida, consulte SUSE: Página web de AutoYaST.

Sistema operativo	Tipos de archivo compatibles	Más información
Ubuntu	No admitido	
VMware vSphere® Hypervisor (ESXi) con personalización de Lenovo	Comenzar (.cfg)	Solo se admite para ESXi 6.0u3 y actualizaciones posteriores y 6.5 o posterior. Para obtener más información acerca de los archivos de instalación desatendida, consulte VMware: instalación o actualización de hosts utilizando una página web de script. Considere lo siguiente cuando agregue secciones %pre, % post, %firstboot al archivo. – Puede incluir múltiples secciones %pre, %post, % firstboot al archivo desatendido; sin embargo, tenga en cuenta el orden de las secciones. – Cuando la macro recomendada **#predefined. unattendSettings.preinstallConfig#** esté presente en el archivo desatendido, XClarity Administrator agrega una sección %pre antes de todos las otras secciones %pre en el archivo. – Cuando la macro recomendada **#predefined. unattendSettings.postinstallConfig#** está presente en el archivo desatendido, XClarity Administrator agrega secciones %post y %firstboot antes de todas los otras secciones %post y %firstboot en el archivo.

Atención:

– Puede insertar macros predefinidas y personalizadas (valores de configuración) en el archivo de instalación desatendida utilizando el nombre único del objeto. Los valores predefinidos se basan dinámicamente en las instancias de XClarity Administrator. Las macros personalizadas se basan dinámicamente en la información ingresada por el cliente que se especifique durante el despliegue del SO.

  Notas:

  – Escriba el nombre con un símbolo de número (#).
  – Para objetos anidados, separe cada nombre de objeto utilizando un punto (por ejemplo, **#server_ settings.server0.locale#**).
  – Para macros personalizadas, no incluya el nombre del objeto de nivel superior. Para macros predefinidas, use “predefinido” como el prefijo del nombre de macro.
  – Cuando se crea un objeto desde una plantilla, el nombre se conecta con un número único, comenzando con 0 (por ejemplo, **server0** y **server1**).
  – Puede ver el nombre de cada macro en el cuadro de diálogo Desplegar imágenes de SO en las pestañas Valores personalizados colocando el puntero sobre el icono Ayuda () situado junto a cada configuración personalizada.
  – Para obtener una lista de macros predefinidas, consulte Macros predefinidas. Para obtener información acerca de los valores de configuración y macros personalizados, consulte Macros personalizadas.

– XClarity Administrator proporciona las siguientes macros predefinidas que se utilizan para comunicar el estado del instalador del SO, así como varios pasos de instalación críticos. Se recomienda encarecidamente incluir estas macros en el archivo de instalación desatendida (consulte Inyección de macros predefinidas y personalizadas a un archivo de instalación desatendida).
  – #predefined.unattendSettings.preinstallConfig#

  - #predefined.unattendSettings postinstallConfig#

- **Scripts de instalación**

  Se puede personalizar los perfiles de imágenes de SO para ejecutar un script de instalación, después de que finalice el despliegue del SO.

  Actualmente, solo se admite el uso de scripts posteriores a la instalación.

  La siguiente tabla enumera los tipos de archivo para los scripts de instalación que admite Lenovo XClarity Administrator por cada sistema operativo. Tenga en cuenta que algunas versiones del sistema de operación no son compatibles con todos los otros tipos de archivos que admite XClarity Administrator (por ejemplo, algunas versiones RHEL pueden no incluir Perl en el perfil mínimo y, por lo tanto, no se ejecutarán scripts Perl). Asegúrese de utilizar el tipo de archivo correcto para las versiones de sistema operativo que desee desplegar.

Sistema operativo	Tipos de archivo compatibles	Más información
CentOS Linux	No admitido	
Microsoft® Windows® Azure Stack HCI	No admitido	
Microsoft Windows Hyper-V Server	No admitido	
Microsoft® Windows® Server	Archivo de comandos (.cmd), PowerShell (.ps1)	La ruta de datos y archivos personalizados predeterminada es `C:\lxca`. Para obtener más información acerca de los scripts de instalación, consulte el Pagina web Agregar un script personalizado a la instalación de Windows
Servidor Red Hat® Enterprise Linux (RHEL)	Bash (.sh), Perl (.pm o .pl), Python (.py)	La ruta de datos y archivos personalizados predeterminada es `/home/lxca`. Para obtener más información acerca de los scripts de instalación, consulte el RHEL: Página web de script posterior a la instalación.
Rocky Linux	Bash (.sh), Perl (.pm o .pl), Python (.py)	La ruta de datos y archivos personalizados predeterminada es `/home/lxca`. Para obtener más información acerca de los scripts de instalación, consulte el RHEL: Página web de script posterior a la instalación
SUSE® Linux Enterprise Server (SLES)	Bash (.sh), Perl (.pm o .pl), Python (.py)	La ruta de datos y archivos personalizados predeterminada es `/home/lxca`. Para obtener más información acerca de los scripts de instalación, consulte el SUSE: Sitio web de script de usuario personalizado

Sistema operativo	Tipos de archivo compatibles	Más información
Ubuntu	No admitido	
VMware vSphere® Hypervisor (ESXi) con personalización de Lenovo	Bash (.sh), Python (.py)	La ruta de datos y archivos personalizados predeterminada es `/home/lxca`. Para obtener más información acerca de los scripts de instalación, consulte el VMware: Página Web de instalación y actualización de scripts

- **Software personalizado**

  Puede personalizar los perfiles de imagen de SO para instalar cargas de software personalizado después de completar los scripts posteriores a la instalación y los scripts de despliegue de SO.

  Se admite los siguientes tipos de archivo para software personalizado.

Sistema operativo	Tipos de archivo compatibles	Más información
CentOS Linux	No admitido	
Microsoft® Windows® Azure Stack HCI	No admitido	
Microsoft Windows Hyper-V Server	No admitido	
Microsoft Windows® Server	Un archivo .zip que contenga la carga útil de software.	La ruta de archivos y datos personalizados predeterminada es `C:\lxca`.
Servidor Red Hat® Enterprise Linux (RHEL)	Un archivo .tar.gz que contenga la carga útil de software	La ruta de datos y archivos personalizados predeterminada es `/home/lxca`.
SUSE® Linux Enterprise Server (SLES)	Un archivo .tar.gz que contenga la carga útil de software	La ruta de datos y archivos personalizados predeterminada es `/home/lxca`.
Rocky Linux	Un archivo .tar.gz que contenga la carga útil de software	La ruta de datos y archivos personalizados predeterminada es `/home/lxca`.
Ubuntu	No admitido	
VMware vSphere® Hypervisor (ESXi) con personalización de Lenovo	Un archivo .tar.gz que contenga la carga útil de software	La ruta de datos y archivos personalizados predeterminada es `/home/lxca`.

Importación de un perfil de imagen del SO personalizado

Puede importar un perfil de imagen del SO personalizado y agregarlo a una imagen del SO base existente.

Acerca de esta tarea

Debe importar la imagen del SO base antes de importar un perfil personalizado.

Solo se puede añadir un perfil de imagen de SO personalizado a una imagen del SO base del mismo tipo. Por ejemplo, si el perfil exportado es de una imagen de Windows 2016, el perfil solo se puede importar y agregar a una imagen de Windows 2016 que existe en el repositorio de imágenes del SO.

El repositorio de imágenes del SO puede almacenar un número ilimitado de perfiles personalizados, en caso que haya espacio disponible para almacenar los archivos.

Procedimiento

Para importar un perfil de imagen del SO personalizado, lleve a cabo los pasos siguientes.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Aprovisionamiento → Gestionar imágenes de SO** para mostrar la página Desplegar sistema operativo: Gestionar imágenes de SO.

Paso 2. En la pestaña **Imágenes del SO**, seleccione la imagen del SO base que desea agregar al perfil de imagen del SO personalizado.

Paso 3. Haga clic en **Importar/Exportar perfil → Importar imagen del perfil personalizado**. Se muestra el cuadro de diálogo Importar perfil de imagen del SO personalizado.

Paso 4. Haga clic en la pestaña **Importación local** para cargar archivos del sistema local, o haga clic en la pestaña **Importación remota** para cargar archivos desde un servidor de archivo remoto.

Nota: Para cargar un archivo desde un servidor de archivo remoto, debe crear primero un perfil del servidor de archivo remoto pulsando el icono **Configurar servidor de archivo** (). Para obtener más información, consulte Configurar un servidor de archivo remoto .

Paso 5. Si desea utilizar un servidor de archivo remoto, seleccione el servidor que desea utilizar desde la lista **Servidor de archivo remoto**.

Paso 6. Ingrese el nombre de perfil o haga clic en **Examinar** para buscar el perfil que desee importar.

Paso 7. **Opcional:** para las importaciones locales, seleccione un tipo de suma de comprobación para asegurarse de que el archivo que se está cargando no está dañado y, a continuación, copie y pegue el valor de suma de comprobación en el campo de texto previsto a tal fin.

Si selecciona un tipo de suma de comprobación, debe especificar un valor de suma de comprobación para comprobar la integridad y la seguridad del archivo cargado. El valor debe proceder de una fuente segura de una organización de su confianza. Si el archivo cargado coincide con el valor de suma de comprobación, es seguro realizar el despliegue. De lo contrario, deberá cargar de nuevo el archivo o comprobar el valor de suma de comprobación.

Se admiten tres tipos de suma de comprobación:
- **MD5**
- **SHA1**
- **SHA256**

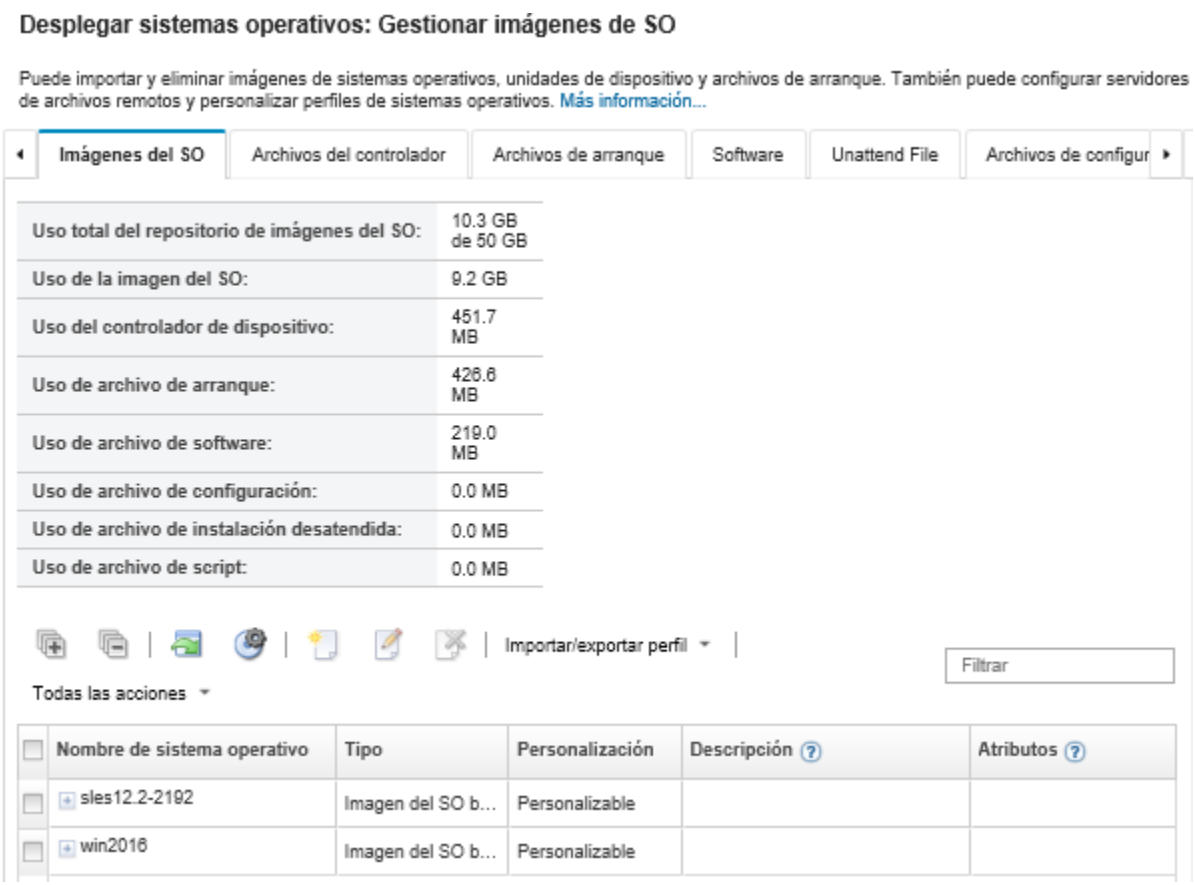
Paso 8. Haga clic en **Importar**.

Consejo: el archivo se carga a través de una conexión de red segura. Por consiguiente, la fiabilidad y el rendimiento de la red afectan al tiempo que tarda en importarse el archivo.

Si cierra la pestaña del navegador web o la ventana en la que se está cargando el archivo localmente antes de que finalice el proceso, la importación fallará.

Después de finalizar

El perfil de imagen del SO personalizado se encuentra en la página Gestionar imágenes de SO del sistema operativo base.



Desde esta página puede llevar a cabo las siguientes acciones:

- Cree un perfil de imagen de SO personalizado (consulte Creación de un perfil de imagen de SO personalizado).
- Exportar un perfil de imagen del SO personalizado seleccionado al hacer clic en **Importar/Exportar perfil → Exportar imagen de perfil personalizada**.

  Importante: Puede exportar perfiles de imágenes del SO personalizados a un servidor de archivo remoto configurado para utilizar protocolos FTP o SFTP. No se puede exportar a un servidor de archivo remoto configurado para utilizar HTTP o HTTPS.
- Modificar un perfil de imagen del SO personalizado seleccionado pulsando el icono **Editar** ( ).
- Quitar un perfil de imagen del SO personalizado seleccionado pulsando el icono **Eliminar** ( ).

Importar archivos de arranque

Puede importar los archivos de arranque en el repositorio de imágenes del SO. Estos archivos se pueden utilizar posteriormente para personalizar y desplegar imágenes de Windows.

Acerca de esta tarea

Un archivo de arranque actúa como el entorno de arranque de instalación. Para Windows, este es un archivo de instalación previa de Windows (WinPE). Se requiere un archivo de arranque de WinPE desplegar Windows

Lenovo XClarity Administrator admite archivos de arranque predefinidos y personalizados.

- **Archivos de arranque de predefinidos**. Lenovo proporciona un archivo de arranque WinPE_64.wim que puede utilizarse para desplegar perfiles de imagen del SO predefinidos.

  Lenovo incluye el archivo de arranque predefinido WinPE_64.wim junto con un conjunto de controladores de dispositivos en un único paquete que puede descargarse desde el Página web del repositorio de controladores de Lenovo Windows e imágenes de WinPE y luego importarse al repositorio de imágenes del SO. Si el archivo de paquete contiene los controladores de dispositivos y archivos de arranque, puede importar el archivo de conjunto desde la pestaña **Controlador de dispositivo** o **Archivos de arranque**.

  Notas:

  – No se precarga un archivo de arranque predefinido con XClarity Administrator. Debe importar un archivo de arranque en el repositorio de imágenes del SO antes de poder desplegar un perfil de Windows.

  – No puede eliminar los archivos de arranque predefinido que se cargaron cuando instaló XClarity Administrator; sin embargo, puede eliminar los archivos de arranque predefinido que se importaron en un conjunto de Lenovo.

  – XClarity Administrator requiere que los archivos de paquete importados estén firmados por Lenovo. Al importar un archivo de paquete, también se debe importar un archivo de firma .asc.

- **Archivos de arranque personalizados**. También puede crear un archivo de arranque de WinPE para personalizar las opciones de arranque de un despliegue de Windows. Luego puede agregar el archivo de arranque para los perfiles de Windows personalizados.

  XClarity Administrator proporciona scripts para crear archivos de arranque en el formato correcto. Para obtener información acerca de la creación de un archivo de arranque personalizado, Creación de un archivo de arranque (WinPE) consulte Sitio web de introducción a Windows PE (WinPE).

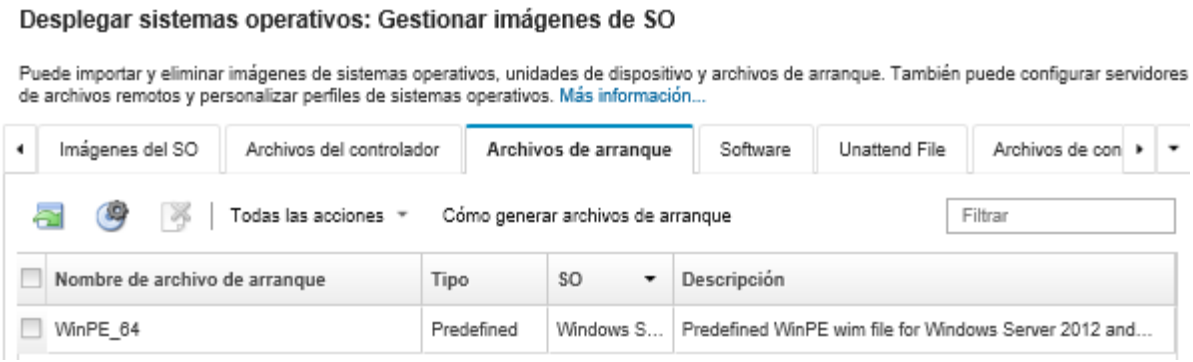
  Se admiten los siguientes tipos de archivo para importar archivos de arranque personalizados.

Sistema operativo	Tipos de archivo de arranque compatibles	Tipos de archivo de paquete compatibles
CentOS Linux	No admitido	No admitido
Microsoft® Windows® Azure Stack HCI	No admitido	No admitido
Microsoft Windows Hyper-V Server	Un archivo .zip que contiene un archivo de WinPE que se crea mediante el script **genimage.cmd**	Un archivo .zip que contiene controladores de dispositivos y archivos de arranque
Microsoft Windows Server	Un archivo .zip que contiene un archivo de WinPE que se crea mediante el script **genimage.cmd**	Un archivo .zip que contiene controladores de dispositivos y archivos de arranque
Servidor Red Hat® Enterprise Linux (RHEL)	No admitido	No admitido
Rocky Linux	No admitido	No admitido
SUSE® Linux Enterprise Server (SLES)	No admitido	No admitido
Ubuntu	No admitido	No admitido
VMware vSphere® Hypervisor (ESXi) con personalización de Lenovo	No admitido	No admitido

Nota: El repositorio de imágenes del SO puede almacenar un número ilimitado de archivos predefinidos y personalizados, en caso que haya espacio disponible para almacenar los archivos.

Procedimiento

- Para importar un archivo de paquete que contenga archivos de arranque en el repositorio de imágenes del SO, lleve a cabo los siguientes pasos.
  1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Gestionar imágenes de SO** para mostrar la página Desplegar sistema operativo: Gestionar imágenes de SO.
  2. Haga clic en la pestaña **Archivos de arranque**.



  3. Haga clic en **Descarga → Archivos de paquete de Windows** para ir a la página Web del soporte de Lenovo y descargar el archivo de paquete apropiado y la firma asociada para la imagen del SO en el sistema local.
  4. Pulse el icono **Importar archivo de paquete** ( ). Se muestra el cuadro de diálogo Importar archivo de paquete.
  5. Haga clic en la pestaña **Importación local** para cargar archivos del sistema local, o haga clic en la pestaña **Importación remota** para cargar archivos desde un servidor de archivo remoto.

     Nota: Para cargar un archivo desde un servidor de archivo remoto, debe crear primero un perfil del servidor de archivo remoto pulsando el icono **Configurar servidor de archivo** ( ). Para obtener más información, consulte Configurar un servidor de archivo remoto .
  6. Si desea utilizar un servidor de archivo remoto, seleccione el servidor que desea utilizar desde la lista **Servidor de archivo remoto**.
  7. Seleccione el tipo del sistema operativo y la versión.
  8. Escriba el nombre del archivo de paquete y el archivo de firma asociado o haga clic en **Examinar** para buscar los archivos que desea importar.
  9. **Opcional:** Escriba una descripción del archivo de paquete.
  10. Haga clic en **Importar**.

      Consejo: el archivo se carga a través de una conexión de red segura. Por consiguiente, la fiabilidad y el rendimiento de la red afectan al tiempo que tarda en importarse el archivo.

      Si cierra la pestaña del navegador web o la ventana en la que se está cargando el archivo localmente antes de que finalice el proceso, la importación fallará.
- Para importar un archivo de arranque individual en el repositorio de imágenes del SO, lleve a cabo los pasos siguientes.
  1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Gestionar imágenes de SO** para mostrar la página Desplegar sistema operativo: Gestionar imágenes de SO.
  2. Haga clic en la pestaña **Archivos de arranque**.
  3. Haga clic en el icono **Importar archivo** ( ). Se muestra el cuadro de diálogo Importar archivo.

4. Haga clic en la pestaña **Importación local** para cargar archivos del sistema local, o haga clic en la pestaña **Importación remota** para cargar archivos desde un servidor de archivo remoto.

   Nota: Para cargar un archivo desde un servidor de archivo remoto, debe crear primero un perfil del servidor de archivo remoto pulsando el icono **Configurar servidor de archivo** (). Para obtener más información, consulte Configurar un servidor de archivo remoto .
5. Si desea utilizar un servidor de archivo remoto, seleccione el servidor que desea utilizar desde la lista **Servidor de archivo remoto**.
6. Seleccione el tipo del sistema operativo y la versión.
7. Ingrese el nombre del archivo o haga clic en **Examinar** para buscar el archivo de arranque que desea importar.
8. **Opcional:** Escriba una descripción del archivo de arranque.
9. **Opcional:** Seleccione un tipo de suma de comprobación para asegurarse de que el archivo que se está cargando no está dañado y, a continuación, copie y pegue el valor de suma de comprobación en el campo de texto previsto a tal fin.

   Si selecciona un tipo de suma de comprobación, debe especificar un valor de suma de comprobación para comprobar la integridad y la seguridad del archivo cargado. El valor debe proceder de una fuente segura de una organización de su confianza. Si el archivo cargado coincide con el valor de suma de comprobación, es seguro realizar el despliegue. De lo contrario, deberá cargar de nuevo el archivo o comprobar el valor de suma de comprobación.

   Se admiten tres tipos de suma de comprobación:
   - **MD5**
   - **SHA1**
   - **SHA256**
10. Haga clic en **Importar**.

    Consejo: el archivo se carga a través de una conexión de red segura. Por consiguiente, la fiabilidad y el rendimiento de la red afectan al tiempo que tarda en importarse el archivo.

    Si cierra la pestaña del navegador web o la ventana en la que se está cargando el archivo localmente antes de que finalice el proceso, la importación fallará.

Después de finalizar

El archivo de arranque se encuentra en la pestaña **Archivos de arranque** de la página Gestionar imágenes de SO.

Desde esta página puede llevar a cabo las siguientes acciones.

- Crear un perfil del servidor de servidor de archivo pulsando el icono **Configurar servidor de archivo** ().
- Quitar un archivo de arranque seleccionado pulsando el icono **Eliminar** ().
- Agregar un archivo de arranque a un perfil de imagen del SO personalizado (consulte Creación de un perfil de imagen de SO personalizado).

Creación de un archivo de arranque (WinPE)

Puede crear archivos de arranque que se pueden utilizar para personalizar las imágenes de Windows.

Antes de empezar

- Asegúrese de que el sistema operativo que va a proporcionar esté instalado en el host. Por ejemplo, si desea proporcionar Windows 2016 utilizando los archivos de WinPE, instale Windows 2016 en el host.

- Asegúrese de que el ADK de Microsoft sea compatible con el sistema operativo instalado también esté instalado en el host. Por ejemplo, Windows 2012R2 requiere actualización de ADK versión 8.1.
- Obtenga los controladores de dispositivos, en formato .inf, que desea agregar al archivo de arranque.

  Puede obtener controladores de dispositivos desde Página web del repositorio de Lenovo YUM, desde un proveedor (como Red Hat) o mediante un controlador de dispositivo personalizado que generó por su cuenta. Para algunos controladores de dispositivos de Windows, puede generar un controlador de dispositivo personalizado al extraer el controlador de dispositivo del exe de instalación a su sistema local y crear un archivo .zip.

  Lenovo también empaqueta conjuntos de controladores de dispositivos predefinidos en un único paquete que puede descargarse desde el Página web del repositorio de controladores de Lenovo Windows e imágenes de WinPE y luego importarlos al repositorio de imágenes del SO. En la actualidad, los archivos de paquete están disponibles solo para Windows. Si el archivo de paquete contiene los controladores de dispositivos y archivos de arranque, puede importar el archivo de conjunto desde la pestaña **Controlador de dispositivo** o **Imagen de arranque**.
- Descargue los archivos `genimage.cmd` y `startnet.cmd` al host en un directorio temporal, como `C:\customwim`.

  El comando `genimage.cmd` se utiliza para generar los archivos de arranque de WinPE, incluido el archivo .wim. XClarity Administrator utiliza el comando `startnet.cmd` para arrancar el instalador de Windows.
- Decida cómo desea inyectar los controladores de dispositivos en el archivo de arranque. Puede hacer esto de una de las formas siguientes:
  - Agregue los controladores de dispositivos a un perfil de Windows personalizado, copiando los archivos del controlador de dispositivo al sistema del host en el directorio C:\drivers. Estos se incluirán en el archivo de arranque al ejecutar genimage.cmd posteriormente.

    Nota: Cuando se crea un perfil de imágenes del SO personalizado que utiliza el archivo de arranque personalizado, los controladores de dispositivo en el directorio C:\drivers se incluyen en WinPE y en el SO final. Ambos se tratan como si fueran predefinidos. Por lo tanto, no es necesario importar estos controladores de dispositivos incorporados en XClarity Administrator al especificar los controladores de dispositivos para utilizarlos en la creación de perfiles personalizados de imágenes del SO.
  - Agregue los controladores de dispositivos predefinidos directamente al archivo de arranque.

    Nota: Si se utiliza este método, los controladores de dispositivos solo se aplicarán al archivo de arranque y, por tanto, al entorno de instalación de WinPE. Los controladores de dispositivo no se aplican al último SO instalado. Debe importar manualmente los controladores de dispositivo al repositorio de controladores de dispositivo de imágenes de SO y seleccionarlos como parte del proceso de personalización de perfil de SO.
- Para obtener más información acerca de los archivos de arranque, consulte Sitio web de introducción a Windows PE (WinPE).

Procedimiento

Para crear un archivo de arranque, lleve a cabo los pasos siguientes.

Paso 1. Mediante un Id. de usuario con autoridad de administrador, ejecute el comando “Deployment and Imaging Tools Environment” de Windows ADK. Se muestra una sesión de comando.

Paso 2. En la sesión de comando, cámbiese al directorio donde se descargaron los archivos `genimage.cmd` y `starnet.cmd` (por ejemplo, `C:\customwim`).

Paso 3. Ejecute el siguiente comando para asegurarse de que el host no contenga imágenes montadas previamente:
```
dism /get-mountedwiminfo
```

Si hay imágenes montadas, ejecute el siguiente comando para desecharlas:

```
dism /unmount-wim /MountDir:C:\<mount_path> /Discard
```

Paso 4. Si agrega controladores de dispositivos a un perfil de Windows personalizado, copie los archivos originales del controlador de dispositivo, en formato .inf, al sistema del host en el directorio `C:\drivers`.

Paso 5. Ejecute el siguiente comando para generar el archivo de arranque, en formato .wim y espere unos minutos para que se complete el comando.
`genimage.cmd amd64 <ADK_Version>`

Donde <*ADK_Version*> es uno de los siguientes valores.

- **8.1**. Para Windows 2012 R2
- **10**. Para Windows 2016

Este comando crea el archivo de arranque: `C:\WinPE_64\media\Boot\WinPE_64.wim`.

Paso 6. Ejecute el siguiente comando para montar el archivo de arranque:
`DISM /Mount-Image /ImageFile:C:\WinPE_64\media\Boot\WinPE_64.wim /index:1 /MountDir:C:\WinPE_64\mount`

Paso 7. Si agrega controladores de dispositivos predefinidos directamente al archivo de arranque, lleve a cabo los pasos siguientes.

1. Cree la siguiente estructura de directorio, donde <*os_release*> es `2012`, `2012R2` o `2016`
   `drivers\<os_release>\`
2. Copie los controladores de dispositivo, en formato .inf, a un directorio dentro de dicha ruta, por ejemplo:
   `drivers\<os_release>\<driver1>\<driver1_files>`
3. Copie el directorio `drivers` al directorio de montaje, por ejemplo:
   `C:\WinPE_64\mount\drivers`

Paso 8. Personalice el archivo de opciones de arranque adicionales, como carpetas, archivos, scripts de inicio, paquetes de idioma y aplicaciones. Para obtener más información acerca de la personalización de los archivos de arranque, consulte Sitio web de WinPE: Montaje y personalización.

Paso 9. Desmonte la imagen ejecutando el siguiente comando.
`DISM /Unmount-Image /MountDir:C:\WinPE_64\mount /commit`

Paso 10. Comprima el contenido del directorio `C:\WinPE_64\media` en un archivo zip llamado `WinPE_64.zip` .

Paso 11. Importe el archivo .zip a XClarity Administrator (consulte Importar archivos de arranque).

Importación de controladores de dispositivos

Puede importar controladores de dispositivos individuales y archivos de paquete en el repositorio de imágenes del SO. Estos archivos se pueden utilizar posteriormente para personalizar las imágenes de Linux y Windows.

Acerca de esta tarea

La imagen del sistema operativo que está instalando desplegar incluye los controladores de Ethernet, Fibre Channel y dispositivo de adaptador de almacenamiento para su hardware. Si el controlador de dispositivo del adaptador de E/S no está incluido en la imagen o el perfil del sistema operativo, el adaptador no es compatible con el despliegue del SO. También puede crear perfiles de imagen del SO personalizados que incluyen los controladores de dispositivo que necesita.

Lenovo XClarity Administrator es compatible con controladores de dispositivos incorporados y controladores de dispositivos listos para usar predefinidos y personalizados.

- **Controladores de dispositivos incorporados**. XClarity Administrator no gestiona los controladores de dispositivos. Siempre instale el sistema operativo más reciente para garantizar que cuente con los controladores de dispositivos incorporados más recientes que necesita.

  Nota: Puede agregar controladores de dispositivos incorporados a un perfil de Windows personalizado al crear un archivo de arranque de WinPE personalizado y copiar los archivos del controlador de dispositivo al sistema del host en el directorio `C:\drivers`. Cuando se crea un perfil de imágenes del SO personalizado que utiliza el archivo de arranque personalizado, los controladores de dispositivo en el directorio C:\drivers se incluyen en WinPE y en el SO final. Ambos se tratan como si fueran predefinidos. Por lo tanto, no es necesario importar estos controladores de dispositivos incorporados en XClarity Administrator al especificar los controladores de dispositivos para utilizarlos en la creación de perfiles personalizados de imágenes del SO.
- **Controladores de dispositivos predefinidos**. Para los servidores de ThinkSystem, XClarity Administrator viene precargado con un conjunto de controladores de dispositivo listos para usar para Linux para permitir la instalación del sistema operativo, así como la configuración básica de red y de almacenamiento para el sistema operativo final. Puede añadir estos controladores de dispositivos predefinidos para los perfiles de imagen del SO personalizados y desplegar los perfiles en los servidores gestionados

  Lenovo también empaqueta conjuntos de controladores de dispositivos predefinidos en un único paquete que puede descargarse desde el Página web del repositorio de controladores de Lenovo Windows e imágenes de WinPE y luego importarlos al repositorio de imágenes del SO. En la actualidad, los archivos de paquete están disponibles solo para Windows. Si el archivo de paquete contiene los controladores de dispositivos y archivos de arranque, puede importar el archivo de conjunto desde la pestaña **Controlador de dispositivo** o **Imagen de arranque**.

  Notas:

  – De forma predeterminada, los perfiles de imagen del SO predefinidos incluyen controladores de dispositivos predefinidos.

  – No puede eliminar los controladores de dispositivos predefinidos que se cargaron cuando instaló XClarity Administrator; sin embargo, puede eliminar los controladores de dispositivos predefinidos que se importaron en un conjunto de Lenovo.

  – XClarity Administrator requiere que los archivos de paquete importados estén firmados por Lenovo. Al importar un archivo de paquete, también se debe importar un archivo de firma .asc.
- **Controladores de dispositivos personalizados**. Puede importar controladores de dispositivos listos para usar en el repositorio de imágenes del SO y luego agregar los controladores de dispositivos a un perfil de imagen del SO personalizado.

  Puede obtener controladores de dispositivos desde Página web del repositorio de Lenovo YUM, desde un proveedor (como Red Hat) o mediante un controlador de dispositivo personalizado que generó por su cuenta. Para algunos controladores de dispositivos de Windows, puede generar un controlador de dispositivo personalizado al extraer el controlador de dispositivo del exe de instalación a su sistema local y crear un archivo .zip.

  Se admiten los siguientes tipos de archivo para importar archivos de controlador de dispositivo.

Sistema operativo	Tipos de archivos de Controlador de dispositivo admitidos
CentOS Linux	No admitido
Microsoft® Windows® Azure Stack HCI	No admitido
Microsoft Windows Hyper-V Server	Un archivo .zip que contenga los archivos originales del controlador de dispositivo, que generalmente son conjuntos de archivos.inf, .cat y .dll.

Sistema operativo	Tipos de archivos de Controlador de dispositivo admitidos
Microsoft Windows Server	Un archivo .zip que contenga los archivos originales del controlador de dispositivo, que generalmente son conjuntos de archivos.inf, .cat y .dll.
Servidor Red Hat® Enterprise Linux (RHEL)	Disco de actualización de controlador (DUD) en formato de imagen .iso o .rpm **Nota:** Si se aplica un DUD .rpm al perfil personalizado, el .rpm solo se instala en el último sistema operativo. No se instala en el entorno de instalación (initrd). Para instalar a un controlador de dispositivo personalizado para initrd, importe un DUD .iso y aplique el .iso al perfil personalizado.
Rocky Linux	No admitido
SUSE® Linux Enterprise Server (SLES)	Disco de actualización de controlador (DUD) .rpm en formato de imagen .iso **Nota:** Si se aplica un DUD .rpm al perfil personalizado, el .rpm solo se instala en el último sistema operativo. No se instala en el entorno de instalación (initrd). Para instalar a un controlador de dispositivo personalizado para initrd, importe un DUD .iso y aplique el .iso al perfil personalizado.
Ubuntu	No admitido
VMware vSphere® Hypervisor (ESXi) con personalización de Lenovo	Controladores de dispositivos en formato de imagen .vib

Nota: El repositorio de imágenes del SO puede almacenar un número ilimitado de archivos predefinidos y personalizados, en caso que haya espacio disponible para almacenar los archivos.

Procedimiento

- Para importar un archivo de paquete que contenga controladores de dispositivo en el repositorio de imágenes del SO, lleve a cabo los siguientes pasos.
  1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Gestionar imágenes de SO** para mostrar la página Desplegar sistema operativo: Gestionar imágenes de SO.
  2. Haga clic en la pestaña **Archivo del controlador**.

3. Haga clic en **Descarga → Archivos de paquete de Windows** para ir a la página Web del soporte de Lenovo y descargar el archivo de paquete apropiado y la firma asociada para la imagen del SO en el sistema local.
4. Pulse el icono **Importar archivo de paquete** ( ). Se muestra el cuadro de diálogo Importar archivo de paquete.
5. Haga clic en la pestaña **Importación local** para cargar archivos del sistema local, o haga clic en la pestaña **Importación remota** para cargar archivos desde un servidor de archivo remoto.

   Nota: Para cargar un archivo desde un servidor de archivo remoto, debe crear primero un perfil del servidor de archivo remoto pulsando el icono **Configurar servidor de archivo** ( ). Para obtener más información, consulte Configurar un servidor de archivo remoto .
6. Si desea utilizar un servidor de archivo remoto, seleccione el servidor que desea utilizar desde la lista **Servidor de archivo remoto**.
7. Seleccione el tipo del sistema operativo y la versión.
8. Escriba el nombre del archivo de paquete y el archivo de firma asociado o haga clic en **Examinar** para buscar los archivos que desea importar.
9. **Opcional:** Escriba una descripción del archivo de paquete.
10. Haga clic en **Importar**.

    Consejo: el archivo se carga a través de una conexión de red segura. Por consiguiente, la fiabilidad y el rendimiento de la red afectan al tiempo que tarda en importarse el archivo.

    Si cierra la pestaña del navegador web o la ventana en la que se está cargando el archivo localmente antes de que finalice el proceso, la importación fallará.

- Para importar un controlador de dispositivo individual en el repositorio de imágenes del SO, lleve a cabo los pasos siguientes.
  1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Gestionar imágenes de SO** para mostrar la página Desplegar sistema operativo: Gestionar imágenes de SO.
  2. Haga clic en la pestaña **Archivos de controlador**.

3. Haga clic en el icono **Importar archivo** (). Se muestra el cuadro de diálogo Importar archivo.
4. Haga clic en la pestaña **Importación local** para cargar archivos del sistema local, o haga clic en la pestaña **Importación remota** para cargar archivos desde un servidor de archivo remoto.

   Nota: Para cargar un archivo desde un servidor de archivo remoto, debe crear primero un perfil del servidor de archivo remoto pulsando el icono **Configurar servidor de archivo** (). Para obtener más información, consulte Configurar un servidor de archivo remoto .
5. Si desea utilizar un servidor de archivo remoto, seleccione el servidor que desea utilizar desde la lista **Servidor de archivo remoto**.
6. Seleccione el tipo del sistema operativo y la versión.
7. Ingrese el nombre del archivo o haga clic en **Examinar** para buscar el controlador de dispositivo que desea importar.
8. **Opcional:** escriba una descripción del controlador de dispositivo.
9. **Opcional:** seleccione un tipo de suma de comprobación para asegurarse de que el archivo que se está cargando no está dañado y, a continuación, copie y pegue el valor de suma de comprobación en el campo de texto previsto a tal fin.

   Si selecciona un tipo de suma de comprobación, debe especificar un valor de suma de comprobación para comprobar la integridad y la seguridad del archivo cargado. El valor debe proceder de una fuente segura de una organización de su confianza. Si el archivo cargado coincide con el valor de suma de comprobación, es seguro realizar el despliegue. De lo contrario, deberá cargar de nuevo el archivo o comprobar el valor de suma de comprobación.

   Se admiten tres tipos de suma de comprobación:
   - **MD5**
   - **SHA1**
   - **SHA256**
10. Haga clic en **Importar**.

    Consejo: el archivo se carga a través de una conexión de red segura. Por consiguiente, la fiabilidad y el rendimiento de la red afectan al tiempo que tarda en importarse el archivo.

    Si cierra la pestaña del navegador web o la ventana en la que se está cargando el archivo localmente antes de que finalice el proceso, la importación fallará.

Después de finalizar

La imagen del controlador del dispositivo se encuentra en la pestaña **Archivos del controlador** de la página Gestionar imágenes de SO.

Desde esta página puede llevar a cabo las siguientes acciones.

- Crear un perfil del servidor de servidor de archivo pulsando el icono **Configurar servidor de archivo** ().
- Quitar un controlador de dispositivo seleccionado pulsando el icono **Eliminar** ().
- Agregar un controlador de dispositivo a un perfil de imagen del SO personalizado (consulte Creación de un perfil de imagen de SO personalizado).

Importación de valores de configuración personalizada

Valores de configuración describe los datos que se deben recopilar dinámicamente durante el despliegue del SO. Lenovo XClarity Administrator utiliza un conjunto de valores de configuración predefinidos, lo que incluye valores global, de redes y de ubicación de almacenamiento. Puede utilizar estos valores de

configuración predefinidos y agregar valores de configuración personalizada que no están disponibles en el XClarity Administrator.

Acerca de esta tarea

Los valores de configuración personalizada se definen a modo de un esquema JSON. El esquema debe adherir a las especificaciones de JSON.

Al importar valores de configuración personalizada para XClarity Administrator, XClarity Administrator valida el esquema JSON. Si la validación se realiza correctamente, XClarity Administrator genera macros personalizadas para cada valor.

Puede utilizar las macros personalizadas en el archivo de instalación desatendida y el script de instalación posterior.

En archivos de instalación desatendida

Puede asociar el archivo de configuración personalizado a un archivo de instalación desatendida e incluir estas macros personalizadas (y macros predefinidas) en el archivo de instalación desatendida.

Puede añadir uno o varios archivos de opciones de configuración personalizada en un perfil personalizado. Al desplegar el perfil de SO en un grupo de servidores de destino, puede elegir el archivo de configuración que desea utilizar. XClarity Administrator representa la pestaña **Configuración personalizada** en el cuadro de diálogo Desplegar imágenes de SO en función del esquema JSON en el archivo de valores de configuración y le permite especificar los valores específicos de la configuración (objeto JSON) que se define en el archivo.

Nota: El despliegue del SO no se llevará a cabo si en la entrada no se especifica ningún valor de configuración personalizada necesaria.

En los scripts de instalación posterior

Después de recopilar los datos durante el despliegue del SO, XClarity Administrator crea una instancia del archivo de configuración (lo que incluye la configuración personalizada del archivo seleccionado y un subconjunto de valores predefinidos) en el sistema host que se puede utilizar en el script de instalación posterior.

Notas:

- El archivo de configuración es único para un perfil de imagen de SO personalizado.
- No se puede modificar los valores de configuración para perfiles de imagen de SO predefinidos.
- Los valores de configuración se admiten solo para los siguientes sistemas operativos:
  - Microsoft® Windows® Server
  - Servidor Red Hat® Enterprise Linux (RHEL)
  - Rocky Linux
  - SUSE® Linux Enterprise Server (SLES)
  - VMware vSphere® Hypervisor (ESXi) con personalización de Lenovo 6.0u3 y actualizaciones posteriores y 6.5 y posteriores.

El repositorio de imágenes del SO puede almacenar un número ilimitado de archivos predefinidos y personalizados, en caso que haya espacio disponible para almacenar los archivos.

Procedimiento

Para importar archivos de valores de configuración dentro del repositorio de imágenes de SO, complete los pasos a seguir.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Gestionar imágenes de SO** para mostrar la página Desplegar sistema operativo: Gestionar imágenes de SO.

Paso 2. Haga clic en la pestaña **Valores de configuración**.

Paso 3. Haga clic en el icono **Importar archivo** ( ). Se muestra el cuadro de diálogo Importar valores de configuración.

Paso 4. Haga clic en la pestaña **Importación local** para cargar archivos del sistema local, o haga clic en la pestaña **Importación remota** para cargar archivos desde un servidor de archivo remoto.

Nota: Para cargar un archivo desde un servidor de archivo remoto, debe crear primero un perfil del servidor de archivo remoto pulsando el icono **Configurar servidor de archivo** ( ). Para obtener más información, consulte Configurar un servidor de archivo remoto .

Paso 5. Si desea utilizar un servidor de archivo remoto, seleccione el servidor que desea utilizar desde la lista **Servidor de archivo remoto**.

Paso 6. Seleccione el tipo de sistema operativo.

Paso 7. Escriba el nombre del archivo de valores de configuración o haga clic en **Examinar** para buscar el archivo que desea importar.

Paso 8. **Opcional:** escriba una descripción de los valores de configuración.

Consejo: utilice el campo **Descripción** para diferenciar archivos personalizados con el mismo nombre.

Paso 9. **Opcional:** seleccione un tipo de suma de comprobación para asegurarse de que el archivo que se está cargando no está dañado y, a continuación, copie y pegue el valor de suma de comprobación en el campo de texto previsto a tal fin.

Si selecciona un tipo de suma de comprobación, debe especificar un valor de suma de comprobación para comprobar la integridad y la seguridad del archivo cargado. El valor debe proceder de una fuente segura de una organización de su confianza. Si el archivo cargado coincide con el valor de suma de comprobación, es seguro realizar el despliegue. De lo contrario, deberá cargar de nuevo el archivo o comprobar el valor de suma de comprobación.

Se admiten tres tipos de suma de comprobación:
- **MD5**
- **SHA1**
- **SHA256**

Paso 10. Haga clic en **Importar**. El formato JSON se valida al importar el archivo. Si se detectan errores, se muestra un cuadro de diálogo con el mensaje de error y la ubicación.

Consejo: el archivo se carga a través de una conexión de red segura. Por consiguiente, la fiabilidad y el rendimiento de la red afectan al tiempo que tarda en importarse el archivo.

Atención: Si cierra la pestaña del navegador web o la ventana en la que se está cargando el archivo localmente antes de que finalice el proceso, la importación fallará.

Después de finalizar

Los archivos de valores de configuración se enumeran en la pestaña **Valores de configuración**, en la página Gestionar imágenes de SO.

Desde esta página también se puede llevar a cabo las siguientes acciones.

- Crear un archivo de configuración al hacer clic en el icono **Crear** () y, a continuación, al especificar el nombre de archivo, la descripción, el tipo de SO y los valores de configuración. Haga clic en **Validar** para validar el esquema antes de guardar el archivo.

  El editor identifica la ubicación de los errores que se encuentran en el archivo. Tenga en cuenta que algunos mensajes solo están disponibles en inglés.

- Ver y modificar un archivo de valores de configuración al hacer clic en el icono **Editar** ().

  No se puede editar un archivo de valores de configuración asociado con un archivo de instalación desatendida.

  El editor identifica la ubicación de los errores que se encuentran en el archivo. Tenga en cuenta que algunos mensajes solo están disponibles en inglés.

- Copiar un archivo de valores de configuración al hacer clic en el icono **Copiar** ().

  Si copia un archivo de valores de configuración que está asociado a un archivo de instalación desatendida, el archivo de instalación desatendida asociado también se copia y se crea la asociación automáticamente entre los dos archivos copiados.

- Quitar los archivos de valores de configuración seleccionados al hacer clic en el icono **Eliminar** ().

- Crear un perfil del servidor de servidor de archivo pulsando el icono **Configurar servidor de archivo** ().

Para obtener información acerca de cómo añadir un archivo de valores de configuración a un perfil de imagen del SO personalizado, consulte Creación de un perfil de imagen de SO personalizado.

Macros personalizadas

Las *macros* ofrecen la posibilidad de añadir datos de variable (valores de configuración) a un archivo desatendido o de script posterior a la instalación. Lenovo XClarity Administrator le permite definir sus propios valores personalizados mediante la creación de un archivo de valores personalizados de configuración, utilizando el formato JSON.

El valor de cada valor de configuración personalizado varía basándose en la entrada del usuario que se especifica durante el despliegue del SO.

Al importar valores de configuración personalizada a XClarity Administrator, XClarity Administrator valida el esquema JSON. Si la validación se realiza correctamente, XClarity Administrator genera macros personalizadas para cada valor.

Para inyectar macros personalizadas en un archivo de instalación desatendida o script posterior a la instalación, utilice el nombre único del objeto, separe los objetos anidados con un punto y luego rodee el nombre de la macro con un símbolo de número (#), por ejemplo, **#server_settings.server0.locale#**.

Notas:

- No incluya el nombre de objeto superior.
- Cuando se crea un objeto desde una plantilla, el nombre se conecta con un número único, comenzando con 0 (por ejemplo, server0 y server1).
- Puede ver el nombre de cada macro en el cuadro de diálogo Desplegar imágenes de SO en las pestañas Valores personalizados colocando el puntero sobre el icono **Ayuda** () situado junto a cada configuración personalizada.

Valores de configuración

Puede definir los valores de configuración personalizada que:

- Sean comunes para todos los servidores de destino o únicos para un servidor de destino específico.
- Tengan valores estáticos (que no se pueden configurar) o valores dinámicos (configurables) que se introducen al desplegar el perfil de la imagen del SO.
- Tiene un número variable de elementos basados en una plantilla. Por ejemplo, puede definir un valor de configuración que le permite especificar 0 a 3 servidores NTP durante el despliegue.

Valores comunes

Durante el despliegue del SO, los elementos de la interfaz de usuario en la pestaña **Valores comunes** del cuadro de diálogo Desplegar imagen de SO se representan en función de los objetos que aparecen en el objeto **content**. Los objetos describen la configuración y los valores que requieren los servidores de destino para el despliegue del SO.

Para representar los valores comunes a todos los servidores, el archivo JSON debe contener un objeto primario con un objeto anidado que contenga el par nombre/valor `"common":true`.

El ejemplo siguiente utiliza los mismos servidores NTP configurables (dinámicos) para todos los servidores.

```
{
   "category": "dynamic",
   "content": [{
      "category": "dynamic",
      "common": true,
      "description": "NTP Servers",
      "label": "NTP Servers",
      "maxElements": 3,
      "minElements": 0,
      "name": "common-ntpservers",
      "optional": true,
      "template": [{
         "autoCreateInstance": true,
         "category": "dynamic",
         "common": true,
         "description": "A NTP Server",
         "label": "NTP Server",
         "name": "ntpserver",
         "optional": true,
         "regex": "[\\w\\.]{1,64}$",
         "type": "string"
      }],
      "type": "array"
   },
   ...,
}
```

El siguiente ejemplo usa el mismo directorio de registro de script de instalación posterior no configurable (estática).

```
{
   "category": "dynamic",
   "content": [{
      "category": "static",
      "common": true,
      "description": "Directory location for post-installation script logging.",
      "name": "logpath",
      "optional": false,
      "type": "string",
      "value": "/tmp/mylogger.log"
   },
   ...,
}
```

Valores específicos de servidor

Durante el despliegue del SO, los elementos de la interfaz de usuario en la pestaña **Valores específicos del servidor** del cuadro de diálogo Desplegar imagen de SO se representan en función de los objetos que aparecen en los objetos **content** de la plantilla. Los objetos describen la configuración y los valores que requieren un servidor de destino específico para el despliegue del SO.

Una vez que se recopilan los valores específicos del servidor en la interfaz de usuario, se crea un objeto **content** en la JSON para cada servidor de destino en función del objeto **template**. Cada objeto **content** contiene campos **name** y **targetServer** únicos, además de los valores ingresados en dicho servidor.

Para representar los valores específicos del servidor, el archivo JSON debe contener un objeto primario con el siguiente contenido:

- El par nombre/valor `"category":"dynamic"`.
- Un objeto anidado que contiene el par nombre/valor `"common":false`. Solo un objeto `"common": false` es compatible con el contenido del objeto primario.
- Un objeto de la plantilla con un objeto contenido integrado. La matriz de plantilla puede contener solo un objeto.

Por ejemplo, si desea definir una configuración regional de SO única para cada servidor de destino

```
{
   "category": "dynamic",
   "content": [{
      "category": "dynamic",
      "common": false,
      "name": "server-settings",
      "optional": false,
      "template": [{
         "category": "dynamic",
         "common": false,
         "content": [{
            "category": "dynamic",
            "choices": ["en_US", "pt_BR", "ja_JP"],
            "common": false,
            "label": "OS Locale",
            "name": "locale",
            "optional": false,
            "type": "string",
            "value": "en_US"
         }],
         "name": "server",
         "optional": false,
         "type": "assoc_array"
```

```
            }],
            "type": "assoc_array"
        },
        ...,
    }
```

especificación JSON

La siguiente tabla describe los campos que se admiten en la especificación de JSON.

Parámetro	Necesario/ Opcional	Tipo	Descripción
autoCreateInstance	opcional	Booleano	Indica si se creó una instancia del objeto de plantilla automáticamente en el archivo JSON durante el despliegue. Puede presentar uno de los valores siguientes. • **verdadero**. Se crea una instancia del objeto de plantilla automáticamente en el archivo JSON durante el despliegue. • **falso**. (predeterminado) *No* se crea una instancia del objeto de plantilla automáticamente en el archivo JSON durante el despliegue. **Nota:** Este campo puede colocarse únicamente en el objeto de la plantilla.
category	Obligatorio	Cadena	Indica cómo se rellena el valor de cada configuración. Puede presentar uno de los valores siguientes: • **dynamic**. El usuario ingresa el valor en tiempo de ejecución. Lenovo XClarity Administrator solicita este valor durante el despliegue del SO. • **predefined**. El valor está preestablecido por Lenovo XClarity Administrator. • **static**. El valor está especificado en el esquema y no cambia en el tiempo de ejecución. Los objetos anidados heredan el valor de este campo del objeto principal. Si **category** está definido en `static` en el objeto primario, entonces también debe establecerse `static` en todos los objetos anidados. Si **category** se establece en `dynamic` en el objeto primario, puede especificarse `static` o `dynamic` en los objetos anidados.
choices	opcional	Matriz de valores que coinciden con la propiedad **type**	Matriz de valores estáticos (como cadenas o números enteros) para los valores de configuración que el usuario puede seleccionar durante el despliegue del SO (por ejemplo, `["enabled","disabled"]`).

Parámetro	Necesa-rio/ Opcional	Tipo	Descripción
común	opcional	Booleano	Indica si este esquema de configuración se aplica a todos los servidores de destino. • **true**. El objeto se aplica a todos los servidores de destino. • **false**. (predeterminado) El objeto se aplica a un servidor de destino específico. Los objetos anidados heredan el valor de este campo del objeto principal. Si **common** está definido en `true` en el objeto primario, entonces también debe establecerse `true` en todos los objetos anidados. Si **common** está definido en `false` en el objeto primario, entonces debe establecerse `false` en todos los objetos anidados.
content	opcional	Matriz de objetos	Patrón que representa los objetos anidados del esquema. Después de recuperar datos ingresados por el usuario durante el despliegue del SO, este campo se utiliza para representar los valores finales de una plantilla en la instancia del archivo de valores de configuración que se creó para el despliegue.
predeterminado	opcional	Varía según **type**	El valor predeterminado.
descripción	opcional	Cadena	Descripción del objeto
etiqueta	opcional	Cadena	Etiqueta de la configuración de la interfaz de usuario que se muestra durante el despliegue del SO
max	opcional	Entero	Valor máximo, cuando **type** esté establecido como un entero. El valor predeterminado es ilimitado.
maxElements	opcional	Entero	Número máximo de entradas de la matriz de este objeto.
min	opcional	Entero	Valor mínimo, cuando **type** esté establecido como un entero. El valor predeterminado es 0.
minElements	opcional	Entero	Número mínimo de entradas de la matriz de este objeto.
name	Obligato-rio	Cadena	Nombre único del objeto. Este nombre puede contener solo los siguientes caracteres: caracteres alfanuméricos (a-z, A-z y 0-9), guion bajo (_) y guion (-). Puede hacer referencia a **name** como una macro personalizada del archivo de instalación desatendida. Para objetos con el parámetro de nombre **name** anidado, separe cada objeto utilizando un punto (por ejemplo, `mydeploy.node.locale`).
optional	Obligato-rio	Booleano	Indica si el objeto es opcional. Puede presentar uno de los valores siguientes. • **verdadero**. El campo es opcional • **falso**. El campo es necesario.

Parámetro	Necesa-rio/ Opcional	Tipo	Descripción
regex	opcional	Cadena	Expresión regular para validar el valor (por ejemplo, `"[\\w\\.]{1,64}$"`)
script	opcional	Matriz de cadenas	Lista de scripts, separadas por coma, que tienen dependencias en los datos de este objeto (por ejemplo, `["/opt/lenovo/saphana/bin/saphana-create-saphana.sh", "create_hana.sh"]`). **Nota:** Los scripts deben estar disponibles en el perfil de imagen de SO como un script de instalación o software personalizado.
targetServer	opcional	Cadena	El UUID del servidor que es el destino del despliegue del SO. Si common es verdadero, este campo puede estar vacío o ser nulo y el servidor de destino se especifica durante el despliegue del SO.

Parámetro	Necesa-rio/ Opcional	Tipo	Descripción

template	opcional	Matriz de objetos	Patrón que representa objetos reutilizables.
			Durante el despliegue del SO, esta plantilla puede representar varias instancias del objeto. Los campos **minElements** y **maxElements** pueden utilizarse para limitar el número de instancias.
			
			El ejemplo siguiente utiliza una plantilla que representan una matriz de 1 a 3 servidores NTP.
			{
			"category": "dynamic",
			"common": true,
			"description": "NTP Servers",
			"label": "NTP Servers",
			"maxElements": 3,
			"minElements": 0,
			"name": "common-ntpservers",
			"optional": true,
			"template": [{
			"autoCreateInstance": true,
			"category": "dynamic",
			"common": true,
			"description": "A NTP Server",
			"label": "NTP Server",
			"name": "ntpserver",
			"optional": true,
			"regex": "[\\w\\.]{1,64}$",
			"type": "string"
			}],
			"type": "array"
			},
			
			Una vez que se recopilan los valores ingresados por el usuario durante el despliegue del SO, se crea una instancia del archivo de valores de configuración con contenido específico para cada dispositivo en el que se despliega el SO.
			{
			"category": "dynamic",
			"common": true,
			"description": "NTP Servers",
			"label": "NTP Servers",
			"maxElements": 3,
			"minElements": 0,
			"name": "common-ntpservers",
			"optional": true,
			"content": [{
			"category": "dynamic",
			"common": true,
			"description": "A NTP Server",
			"label": "NTP Server",
			"name": "ntpserver0",
			"optional": true,
			"regex": "[\\w\\.]{1,64}$",
			"type": "string",
			"value": "192.0.2.1"
			}],
			"template": [{

Parámetro	Necesa-rio/ Opcional	Tipo	Descripción

			<pre>"category": "dynamic",
			"common": true,
			"description": "A NTP Server",
			"label": "NTP Server",
			"name": "ntpserver",
			"optional": true,
			"regex": "[\\w\\.]{1,64}$",
			"type": "string"
			}],
			"type": "array"
			}</pre> **Notas:**
			• Se *requiere* una plantilla en el nivel superior de los objetos específicos para el servidor (common=false).
			• Si **category** es `static`, se omite el campo de la plantilla.

tipo	Obligato-rio	Cadena	Tipo de datos del objeto. Puede presentar uno de los valores siguientes. • **matriz** • **assoc_array** • **boolean** • **integer** • **password** • **string** • **user_data**
value	opcional	Cadena	Un valor estático único para los valores de configuración. **Notas:** • Si se especificó **default**, este campo puede estar vacío o ser nulo; de lo contrario, especifique un valor que coincida con **type**. • Si **type** es `password`, especifique una cadena no cifrada. • Si **type** es `assoc_array` o `array`, también se debe especificar un campo **content** vacío. • Si **type** es `user_data`, especifique un parámetro de valor **value** con un formato de JSON válido. • Si **regex** está configurado, este valor se valida utilizando las expresiones regulares especificadas.

El siguiente ejemplo de valores de configuración define los valores de configuración regional para despliegues de SLES que se pueden agregar a un perfil personalizado.

```
{
    "category": "dynamic",
    "content": [{
        "category": "dynamic",
        "common": false,
        "name": "server-settings",
        "optional": false,
        "template": [{
            "autoCreateInstance": true,
            "category": "dynamic",
```

```
        "common": false,
        "content": [{
            "category": "dynamic",
            "choices": ["en_US", "pt_BR", "ja_JP"],
            "common": false,
            "description": "This parameter defines the OS language locale to use with this deployment.
                            English, Brazilian Portuguese, and Japanese are supported.",
            "label": "OS Locale",
            "name": "locale",
            "optional": false,
            "type": "string",
            "value": "en_US"
        },
        {
            "category": "dynamic",
            "choices": ["english-us", "pt_BR", "ja_JP"],
            "common": false,
            "description": "This parameter defines the keyboard locale to use with this deployment.
                            English, Brazilian Portuguese, and Japanese are supported.",
            "label": "Keyboard Locale",
            "name": "keyboardLocale",
            "optional": false,
            "type": "string",
            "value": "english-us"
        }],
        "name": "server",
        "optional": false,
        "type": "assoc_array"
    }],
    "type": "assoc_array"
},
{
    "category": "dynamic",
    "common": true,
    "description": "NTP Servers",
    "label": "NTP Servers",
    "maxElements": 3,
    "minElements": 0,
    "name": "common-ntpservers",
    "optional": true,
    "template": [{
        "category": "dynamic",
        "common": true,
        "description": "A NTP Server",
        "label": "NTP Server",
        "name": "ntpserver",
        "optional": true,
        "regex": "[\\w\\.]{1,64}$",
        "type": "string"
    }],
    "type": "array"
},
{
    "category": "static",
    "common": true,
    "description": "Directory for post-installation script logging.",
    "name": "logpath",
    "optional": false,
    "type": "string",
    "value": "/tmp/mylogger.log"
}],
```

```
    "description": "Custom configuration file for deployment of custom locale, NTP server,
                    and directory for post-installation script logs.",
    "label": "My Custom Deployment",
    "name": "myCustomDeploy",
    "optional": false,
    "type": "array"
}
```

El ejemplo siguiente es la instancia del archivo de valores de configuración que se crea en el sistema host después de definir los valores ingresados por el usuario durante el despliegue.

```
{
    "category": "dynamic",
    "content": [{
        "category": "dynamic",
        "common": false,
        "name": "server-settings",
        "optional": false,
        "content": [{
            "category": "dynamic",
            "common": false,
            "content": [{
                "category": "dynamic",
                "choices": ["en_US", "pt_BR", "ja_JP"],
                "common": false,
                "description": "This parameter defines the OS language locale to use with this deployment.
                                English, Brazilian Portuguese, and Japanese are supported.",
                "label": "OS Locale",
                "name": "locale",
                "optional": false,
                "type": "string",
                "value": "en_US"
            },
            {
                "category": "dynamic",
                "choices": ["english-us", "pt_BR", "ja_JP"],
                "common": false,
                "description": "This parameter defines the keyboard locale to use with this deployment.
                                English, Brazilian Portuguese, and Japanese are supported.",
                "label": "Keyboard Locale",
                "name": "keyboardLocale",
                "optional": false,
                "type": "string",
                "value": "english-us"
            }],
            "name": "server0",
            "optional": false,
            "type": "assoc_array",
            "targetServer": "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
        },
        {
            "category": "dynamic",
            "common": false,
            "content": [{
                "category": "dynamic",
                "choices": ["en_US", "pt_BR", "ja_JP"],
                "common": false,
                "description": "This parameter defines the OS language locale to use with this deployment.
                                English, Brazilian Portuguese, and Japanese are supported.",
                "label": "OS Locale",
                "name": "locale",
                "optional": false,
```

```
            "type": "string",
            "value": "en_US"
        },
        {
            "category": "dynamic",
            "choices": ["english-us", "pt_BR", "ja_JP"],
            "common": false,
            "description": "This parameter defines the keyboard locale to use with this deployment.
                            English, Brazilian Portuguese, and Japanese are supported.",
            "label": "Keyboard Locale",
            "name": "keyboardLocale",
            "optional": false,
            "type": "string",
            "value": "english-us"
        }],
        "name": "server1",
        "optional": false,
        "type": "assoc_array",
        "targetServer": "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB"
    }],
    "template": [{
        "category": "dynamic",
        "common": false,
        "content": [{
            "category": "dynamic",
            "choices": ["en_US", "pt_BR", "ja_JP"],
            "common": false,
            "description": "This parameter defines the OS language locale to use with this deployment.
                            English, Brazilian Portuguese, and Japanese are supported.",
            "label": "OS Locale",
            "name": "locale",
            "optional": false,
            "type": "string",
            "value": "en_US"
        },
        {
            "category": "dynamic",
            "choices": ["english-us", "pt_BR", "ja_JP"],
            "common": false,
            "description": "This parameter defines the keyboard locale to use with this deployment.
                            English, Brazilian Portuguese, and Japanese are supported.",
            "label": "Keyboard Locale",
            "name": "keyboardLocale",
            "optional": false,
            "type": "string",
            "value": "english-us"
        }],
        "name": "server",
        "optional": false,
        "type": "assoc_array"
    }],
    "type": "assoc_array"
},
{
    "category": "dynamic",
    "common": true,
    "description": "NTP Servers",
    "label": "NTP Servers",
    "maxElements": 3,
    "minElements": 0,
    "name": "common-ntpservers",
```

```
        "optional": true,
        "content": [{
            "category": "dynamic",
            "common": true,
            "description": "A NTP Server",
            "label": "NTP Server",
            "name": "ntpserver0,
            "optional": true,
            "regex": "[\\w\\.]{1,64}$",
            "type": "string",
            "value": "192.0.2.1"
        },
        {
            "category": "dynamic",
            "common": true,
            "description": "A NTP Server",
            "label": "NTP Server",
            "name": "ntpserver1",
            "optional": true,
            "regex": "[\\w\\.]{1,64}$",
            "type": "string",
            "value": "192.0.2.2"
        }],
        "template": [{
            "category": "dynamic",
            "common": true,
            "description": "A NTP Server",
            "label": "NTP Server",
            "name": "ntpserver",
            "optional": true,
            "regex": "[\\w\\.]{1,64}$",
            "type": "string"
        }],
        "type": "array"
    },
    {
        "category": "static",
        "common": true,
        "description": "Directory for post-installation script logs.",
        "name": "logpath",
        "optional": false,
        "type": "string",
        "value": "/tmp/mylogger.log"
    }],
    "description": "Custom configuration file for deployment of custom locale, NTP server,
                    and directory for post-installation script logs.",
    "label": "My Custom Deployment",
    "name": "myCustomDeploy",
    "optional": false,
    "type": "array"
}
```

Macros predefinidas

Las *macros* ofrecen la posibilidad de añadir datos de la variable (valores de configuración) a un archivo de instalación desatendida o script posterior a la instalación. Lenovo XClarity Administrator proporciona un conjunto predefinido de valores de configuración que puede utilizar.

Para inyectar macros predefinidas en un archivo de instalación desatendida o un archivo de script posterior reinstalación, use “predefinido” como prefijo para las macros predefinidas, separa los objetos mirados con

un punto rodee el nombre de la macro un símbolo de número (#), por ejemplo **#predefined.globalSettings.ipAssignment#**.

El valor de cada macro predefinida varía según la instancia de XClarity Administrator. Por ejemplo, el campo **Desplegar imágenes del SO → Valores globales → Asignación de IP** le permite especificar el modo de IP. Después de que se recopila el valor de entrada de usuario durante el despliegue del SO, el valor se representa en los valores de configuración predefinidos por la macro predefinida **#predefined.globalSettings.ipAssignment#** y la instancia del archivo JSON de valores de configuración en el nombre de objeto ipAssignment.

La siguiente tabla enumera las macros predefinido (valores de configuración) que están disponibles en XClarity Administrator.

Nombre de macro	Tipo	Descripción
predefinido	Objeto	Información acerca de todos los valores de despliegue del SO predeterminados
globalSettings	Objeto	Información acerca de los valores globales de despliegue del SO
credentials	Matriz de objetos	Información acerca de las credenciales de usuario
name	Cadena	
tipo	Cadena	Tipo de sistema operativo. Puede presentar uno de los valores siguientes. • **ESXi** • **LINUX** • **WINDOWS**
ipAssignment	Cadena	Opción de configuración de la red del host para el despliegue del sistema operativo. Puede presentar uno de los valores siguientes. • **dhcpv4** • **staticv4** • **staticv6**
isVLANMode	Cadena	Indica si se usa el modo VLAN. Puede presentar uno de los valores siguientes. • **verdadero**. Se utiliza el modo VLAN. • **falso**. No se utiliza el modo VLAN.
hostPlatforms	Objeto	Valores de despliegue de las plataformas de host
licenseKey	Cadena	Clave de licencia que se utilizará en Microsoft Windows o VMware ESXi. Si no cuenta con una clave de licencia, puede especificar este campo como nulo.
networkSettings	Matriz	Información acerca de valores de red
dns1	Cadena	Servidor de DNS preferido para el servidor de host que se usará después de desplegar el sistema operativo
dns2	Cadena	Servidor de DNS alternativo para el servidor de host que se usará después de desplegar el sistema operativo
puerta de enlace	Cadena	Puerta de enlace para el servidor de host que se usará después de desplegar el sistema operativo. Se utiliza cuando los valores de red están establecidos en estático en los valores de despliegue de SO global. **Consejo:** para determinar el modo de IP, utilice GET /osdeployment/globalSettings.

Nombre de macro	Tipo	Descripción
Nombre de host de	Cadena	Nombre de host para el servidor host. Si no se especifica un nombre de host, se asigna un nombre de host predeterminado.
ipAddress	Cadena	Dirección IP para el servidor de host que se usará después de desplegar el sistema operativo. Se utiliza cuando los valores de red están establecidos en estático en los valores de despliegue de SO global.
mtu	Larga	Unidad de transmisión máxima preferida para el host para usar después de desplegar el sistema operativo.
prefixLength	Cadena	Longitud del prefijo de la dirección IP de host que se usará después de desplegar el sistema operativo. Se utiliza cuando los valores de red están establecidos en IPv6 estático en los valores de despliegue de SO global.
selectedMAC	Cadena	Dirección MAC del servidor host vinculado a la dirección IP. La dirección MAC está configurada en AUTO de forma predeterminada. Esta configuración detecta automáticamente los puertos Ethernet que se pueden configurar y utilizar para el despliegue. La primera dirección MAC (puerto) que se detecta se utiliza manera predeterminada. Si se detecta la conectividad en otra dirección MAC, el host de XClarity Administrator se reinicia automáticamente para utilizar la dirección MAC recién detectada para el despliegue y selectedMAC se establecen en la dirección MAC recién detectada. El modo VLAN solo se admite para servidores que tienen direcciones MAC en su inventario. Si AUTO es la única dirección MAC disponible para un servidor, entonces no se pueden usar VLAN para desplegar sistemas operativos en ese servidor. **Consejo:** para obtener la dirección MAC, utilice el campo de propiedad de respuesta de **macaddress** en GET /hostPlatforms.
subnetCIDRNumber	Entero	Máscara de subred del servidor host que se va a utilizar después de desplegar el sistema operativo, en formato de Enrutamiento entre dominios sin clase (CIDR). Se utiliza cuando los valores de red están establecidos en estático en los valores de despliegue de SO global. El número CIDR suele estar precedido por una barra diagonal "/" y sigue la dirección IP. Por ejemplo, una dirección IP de 131.10.55.70 con una máscara de subred de 255.0.0.0 (que tiene 8 bits de red) se representa como 131.10.55.70/8. Para obtener más información, consulte el Sitio web del tutorial de la notación CIDR **Consejo:** para determinar el modo de IP, utilice GET /osdeployment/globalSettings.
subnetMask	Cadena	Máscara de subred del servidor host que se va a utilizar después de desplegar el sistema operativo, en notación decimal con puntos (por ejemplo, 255.0.0.0). Se utiliza cuando los valores de red están establecidos en estático en los valores de despliegue de SO global. **Consejo:** para determinar el modo de IP, utilice GET /osdeployment/globalSettings.

Nombre de macro	Tipo	Descripción
vlanId	Cadena	Identificador de VLAN para el etiquetado VLAN del sistema operativo. Este parámetro es válido solo si el modo VLAN está habilitado. Para determinar si el modo VLAN está habilitado, use GET /osdeployment/globalSettings en la documentación en línea de XClarity Administrator). **Importante:** Solo especifique un Id. de VLAN cuando se requiere una etiqueta de VLAN para que funcione en la red. El uso de etiquetas de VLAN puede afectar el enrutamiento de la red entre el sistema operativo del host y el XClarity Administrator.
selectedImage	Cadena	Identificador de perfil de la imagen del sistema operativo que va a desplegar. **Consejo:** para obtener los Id. de perfil de la imagen del sistema operativo, utilice la propiedad de respuesta de **availableImages** en GET /hostPlatforms.
storageSettings	Matriz	Ubicación de almacenamiento preferida donde desea desplegar imágenes de sistema operativo.
targetDevice	Cadena	Dispositivo objetivo. Puede presentar uno de los valores siguientes. • **localdisk**. Unidad de disco local. Se usa la primera de las unidades de disco local enumeradas en el servidor gestionado. • **M.2drive**. Unidad M.2. Se usa la primera de las unidades M.2 enumeradas en el servidor gestionado. • **usbdisk**. Hipervisor USB integrado. Esta ubicación solo es aplicable cuando se despliega una imagen de VMware ESXi en servidores gestionados. Si hay dos claves de hipervisor instaladas en el servidor gestionado, el instalador de VMware selecciona la primera clave enumerada para el despliegue. • **lunpluswwn=***LUN@WWN*. Almacenamiento SAN FC (por ejemplo, `lunpluswwn=2@50:05:07:68:05:0c:09:bb`). • **lunplusiqn=***LUN@IQN*. Almacenamiento SAN iSCSI (por ejemplo, `lunplusiqn=0@iqn.1990-01.com.lenovo:tgt1`). Especificación del *IQN* es opcional si solo se configura un destino iSCSI si no se especifica el *IQN*, se selecciona el primer destino iSCSI detectado para OSDN. Si se especifica, y se realiza una coincidencia exacta. **Nota:** Para servidores ThinkServer, este valor siempre es “localdisk.”
unattendFileId	Cadena	Identificador del archivo de instalación desatendida a utilizar en este despliegue
UUID	Cadena	UUidentificador del servidor de host donde se desplegará el sistema operativo
imageSettings	Objeto	Información acerca de cada imagen de SO y el perfil de imagen
name	Cadena	Nombre de la imagen del sistema operativo
perfil	Cadena	Nombre del perfil de imagen
otherSettings	Objeto	Valores adicionales asociados con los trabajos de despliegue del SO en ejecución actualmente
deployDataAndSoftwareLocation	Cadena	Ruta a la carga útil de software extraído, los archivos personalizados y los datos de despliegue (por ejemplo, los certificados y los registros)

Nombre de macro	Tipo	Descripción

installRepoUrl	Cadena	(Solo SLES 15 y versiones posteriores) URL para la imagen de paquete importado
		Puede utilizar están macro predefinido en la instalación desatendida personalizada para media_url en la sección adicional, por ejemplo:
		`<add-on>`
		`<add_on_products config:type="list">`
		`<listentry>`
		`<media_url>`**#predefined.otherSettings.installRepoUrl#**
		`</media_url>`
		`<product>sle-module-basesystem</product>`
		`<product_dir>/Module-Basesystem</product_dir>`
		`</listentry>`
		`</add_on_products>`
		`</add-on>`

lxcaIp	Cadena	Dirección IP de la instancia XClarity Administrator
lxcaRelease	Cadena	Versión de XClarity Administrator (por ejemplo, 2.0.0)
jobId	Cadena	El identificador del trabajo de despliegue del SO que se está ejecutando actualmente
ntpServer	Cadena	Servidor NTP que está asociado con XClarity Administrator
statusSettings	Objeto	Valores de estado de despliegue de SO
urlStatus	Cadena	HTTPS URL (incluye el puerto) que XClarity Administrator utiliza para los informes de estado
certLocation	Cadena	Carpeta que contiene los certificados que se necesitan para acceder al servicio web **urlStatus** desde el SO del host en el primer arranque
sdkLocation	Cadena	Ubicación de XClarity Administrator proporcionada por scripts e interfaces de ayuda para acceder a XClarity Administrator
timezone	Cadena	La zona horaria se establece para XClarity Administrator (por ejemplo, America/New_York)
unattendSettings	Objeto	Valores que se utilizan para rellenar el archivo de instalación desatendida. Estos valores son específicos para la versión de XClarity Administrator
networkConfig	Cadena	(Solo ESXi y RHEL) Contenido predefinido de XClarity Administrator para su uso en el tiempo de instalación desatendida. Esto configura los valores de red para el sistema operativo
preinstallConfig	Cadena	Contenido predefinido de XClarity Administrator para su uso durante la instalación previa desatendida. Esto incluye el estado de instalación previa. • En ESXi y RHEL, se usa el enlace de scripts previos a la instalación %pre. • En SLES, se usa el enlace de scripts previos a la instalación <scripts>. **Atención:** Se recomienda encarecidamente incluir estas macros en el archivo de instalación desatendida. Puede colocar el macro en el archivo de instalación desatendida en cualquier lugar después de la línea 1 (después de la etiqueta <xml>).

Nombre de macro	Tipo	Descripción
postinstallConfig	Cadena	Contenido predefinido de XClarity Administrator para su uso después de que el servidor está configurado y se inicia por primera vez. Esto incluye el estado posterior a la instalación. • En ESXi y RHEL, se usa el enlace de scripts posteriores a la instalación %post • En SLES, se usa el enlace de scripts posterior a la instalación <scripts>. • En Windows, esto utiliza la sección “valores especializados”. **Atención:** Se recomienda encarecidamente incluir esta macro en el archivo de instalación desatendida. Puede colocar el macro en el archivo de instalación desatendida en cualquier lugar después de la línea 1 (después de la etiqueta <xml>).
reportWorkloadNotComplete	Cadena	Cuando esta macro está presente, el macro postinstallConfig no informará el estado de Instalación de SO completa (17). El perfil personalizado debe informar que se completó.
storageConfig	Cadena	(Solo ESXi y RHEL) Contenido predefinido de XClarity Administrator para su uso en el tiempo de instalación desatendida. Esto configura los valores de almacenamiento para el sistema operativo.

Importación de archivos de instalación desatendida personalizados

Se puede importar archivos de instalación desatendida personalizados en el repositorio de imágenes de SO. Estos archivos se pueden utilizar posteriormente para personalizar los perfiles de las imágenes de los SO Linux y Windows.

Acerca de esta tarea

Se admite los siguientes tipos de archivo para archivos de instalación desatendida estándar.

Sistema operativo	Tipos de archivo compatibles	Más información
CentOS Linux	No admitido	
Microsoft® Windows® Azure Stack HCI	No admitido	
Microsoft Windows Hyper-V Server	No admitido	
Microsoft Windows Server	Instalación desatendida (.xml)	Para obtener más información acerca de los archivos de instalación desatendida, consulte Página Web de referencia de instalación desatendida de Windows.

Sistema operativo	Tipos de archivo compatibles	Más información
Servidor Red Hat® Enterprise Linux (RHEL)	Comenzar (.cfg)	Para obtener más información acerca de los archivos de instalación desatendida, consulte Página web de Red Hat: Automatización de la instalación con Kickstart . Considere lo siguiente cuando agregue secciones %pre, % post, %firstboot al archivo. • Puede incluir múltiples secciones %pre, %post, %firstboot al archivo desatendido; sin embargo, tenga en cuenta el orden de las secciones. • Cuando la macro recomendada **#predefined. unattendSettings.preinstallConfig#** esté presente en el archivo desatendido, XClarity Administrator agrega una sección %pre antes de todos las otras secciones %pre en el archivo. • Cuando la macro recomendada **#predefined. unattendSettings.postinstallConfig#** está presente en el archivo desatendido, XClarity Administrator agrega secciones %post y %firstboot antes de todas los otras secciones %post y %firstboot en el archivo.
Rocky Linux	Comenzar (.cfg)	Para obtener más información acerca de los archivos de instalación desatendida, consulte Página web de Red Hat: Automatización de la instalación con Kickstart . Considere lo siguiente cuando agregue secciones %pre, % post, %firstboot al archivo. • Puede incluir múltiples secciones %pre, %post, %firstboot al archivo desatendido; sin embargo, tenga en cuenta el orden de las secciones. • Cuando la macro recomendada **#predefined. unattendSettings.preinstallConfig#** esté presente en el archivo desatendido, XClarity Administrator agrega una sección %pre antes de todos las otras secciones %pre en el archivo. • Cuando la macro recomendada **#predefined. unattendSettings.postinstallConfig#** está presente en el archivo desatendido, XClarity Administrator agrega secciones %post y %firstboot antes de todas los otras secciones %post y %firstboot en el archivo.
SUSE® Linux Enterprise Server (SLES)	AutoYast (.xml)	Para obtener más información acerca de los archivos de instalación desatendida, consulte SUSE: Página web de AutoYaST.

Sistema operativo	Tipos de archivo compatibles	Más información
Ubuntu	No admitido	
VMware vSphere® Hypervisor (ESXi) con personalización de Lenovo	Comenzar (.cfg)	Solo se admite para ESXi 6.0u3 y actualizaciones posteriores y 6.5 o posterior. Para obtener más información acerca de los archivos de instalación desatendida, consulte VMware: instalación o actualización de hosts utilizando una página web de script. Considere lo siguiente cuando agregue secciones %pre, % post, %firstboot al archivo. • Puede incluir múltiples secciones %pre, %post, %firstboot al archivo desatendido; sin embargo, tenga en cuenta el orden de las secciones. • Cuando la macro recomendada **#predefined. unattendSettings.preinstallConfig#** esté presente en el archivo desatendido, XClarity Administrator agrega una sección %pre antes de todos las otras secciones %pre en el archivo. • Cuando la macro recomendada **#predefined. unattendSettings.postinstallConfig#** está presente en el archivo desatendido, XClarity Administrator agrega secciones %post y %firstboot antes de todas los otras secciones %post y %firstboot en el archivo.

Atención:

- Puede insertar macros predefinidas y personalizadas (valores de configuración) en el archivo de instalación desatendida utilizando el nombre único del objeto. Los valores predefinidos se basan dinámicamente en las instancias de XClarity Administrator. Las macros personalizadas se basan dinámicamente en la información ingresada por el cliente que se especifique durante el despliegue del SO.

  Notas:

  - Escriba el nombre con un símbolo de número (#).
  - Para objetos anidados, separe cada nombre de objeto utilizando un punto (por ejemplo, **#server_ settings.server0.locale#**).
  - Para macros personalizadas, no incluya el nombre del objeto de nivel superior. Para macros predefinidas, use “predefinido” como el prefijo del nombre de macro.
  - Cuando se crea un objeto desde una plantilla, el nombre se conecta con un número único, comenzando con 0 (por ejemplo, **server0** y **server1**).
  - Puede ver el nombre de cada macro en el cuadro de diálogo Desplegar imágenes de SO en las pestañas Valores personalizados colocando el puntero sobre el icono Ayuda () situado junto a cada configuración personalizada.
  - Para obtener una lista de macros predefinidas, consulte Macros predefinidas. Para obtener información acerca de los valores de configuración y macros personalizados, consulte Macros personalizadas.

- XClarity Administrator proporciona las siguientes macros predefinidas que se utilizan para comunicar el estado del instalador del SO, así como varios pasos de instalación críticos. Se recomienda encarecidamente incluir estas macros en el archivo de instalación desatendida (consulte Inyección de macros predefinidas y personalizadas a un archivo de instalación desatendida).
  - #predefined.unattendSettings.preinstallConfig#

– #predefined.unattendSettings postinstallConfig#

El repositorio de imágenes del SO puede almacenar un número ilimitado de archivos predefinidos y personalizados, en caso que haya espacio disponible para almacenar los archivos.

Procedimiento

Para importar archivos de instalación desatendida en el repositorio de imágenes de SO, lleve a cabo los pasos siguientes.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Gestionar imágenes de SO** para mostrar la página Desplegar sistema operativo: Gestionar imágenes de SO.

Paso 2. Haga clic en la pestaña **Archivos de instalación desatendida**.

Paso 3. Haga clic en el icono **Importar archivo** ( ). Se muestra el cuadro de diálogo Importar archivo.

Paso 4. Haga clic en la pestaña **Importación local** para cargar archivos del sistema local, o haga clic en la pestaña **Importación remota** para cargar archivos desde un servidor de archivo remoto.

Nota: Para cargar un archivo desde un servidor de archivo remoto, debe crear primero un perfil del servidor de archivo remoto pulsando el icono **Configurar servidor de archivo** ( ). Para obtener más información, consulte Configurar un servidor de archivo remoto

Paso 5. Si desea utilizar un servidor de archivo remoto, seleccione el servidor que desea utilizar desde la lista **Servidor de archivo remoto**.

Paso 6. Seleccione el tipo de sistema operativo.

Paso 7. Escriba el nombre del archivo de instalación desatendida o haga clic en **Examinar** para buscar el archivo que desea importar.

Paso 8. **Opcional:** escriba una descripción del archivo de instalación desatendida.

Consejo: utilice el campo **Descripción** para diferenciar archivos personalizados con el mismo nombre.

Paso 9. **Opcional:** seleccione un tipo de suma de comprobación para asegurarse de que el archivo que se está cargando no está dañado y, a continuación, copie y pegue el valor de suma de comprobación en el campo de texto previsto a tal fin.

Si selecciona un tipo de suma de comprobación, debe especificar un valor de suma de comprobación para comprobar la integridad y la seguridad del archivo cargado. El valor debe proceder de una fuente segura de una organización de su confianza. Si el archivo cargado coincide con el valor de suma de comprobación, es seguro realizar el despliegue. De lo contrario, deberá cargar de nuevo el archivo o comprobar el valor de suma de comprobación.

Se admiten tres tipos de suma de comprobación:
- **MD5**
- **SHA1**
- **SHA256**

Paso 10. Haga clic en **Importar**.

Consejo: el archivo se carga a través de una conexión de red segura. Por consiguiente, la fiabilidad y el rendimiento de la red afectan al tiempo que tarda en importarse el archivo.

Si cierra la pestaña del navegador web o la ventana en la que se está cargando el archivo localmente antes de que finalice el proceso, la importación fallará.

Después de finalizar

La imagen del archivo de instalación desatendida aparece en la pestaña **Archivos de instalación desatendida**, en la página Gestionar imágenes de SO.

Desde esta página puede llevar a cabo las siguientes acciones.

- Crear un archivo de instalación desatendida al hacer clic en el icono **Crear** ( ).

  El editor identifica la ubicación de los errores que se encuentran en el archivo. Tenga en cuenta que algunos mensajes solo están disponibles en inglés.
- Asociar un archivo de instalación desatendida con un archivo de valores de configuración (consulte Asociación de un archivo de instalación desatendida con un archivo de valores de configuración).
- Ver y modificar un archivo de instalación desatendida al hacer clic en el icono **Editar** ( ).

  El editor identifica la ubicación de los errores que se encuentran en el archivo. Tenga en cuenta que algunos mensajes solo están disponibles en inglés.
- Copiar un archivo de instalación desatendida al hacer clic en el icono **Copiar** ( ).

  Si copia un archivo de instalación desatendida que está asociado a un archivo de valores de configuración, el archivo de valores de configuración asociado también se copia y se crea la asociación automáticamente entre los dos archivos copiados.
- Quitar los archivos de instalación desatendida seleccionados al hacer clic en el icono **Eliminar** ( ).
- Crear un perfil del servidor de servidor de archivo pulsando el icono **Configurar servidor de archivo** ( ).

Para obtener información acerca de cómo añadir un archivo de instalación desatendida a un perfil de imagen del SO personalizado, consulte Creación de un perfil de imagen de SO personalizado.

Inyección de macros predefinidas y personalizadas a un archivo de instalación desatendida

Se puede agregar macros predefinidas y personalizadas a un archivo de instalación desatendida.

Acerca de esta tarea

Las *macros* proporcionan la capacidad de agregar datos dinámicos (valores de configuración) a un archivo de instalación. El usuario proporciona los valores de los datos al desplegar el perfil de imagen del SO.

Lenovo XClarity Administrator proporciona un conjunto de macros *predefinidas* que se puede agregar a un archivo de instalación desatendida sin asociarla a un archivo de valores de configuración personalizado. Para obtener una lista de macros predefinidas, consulte Macros predefinidas.

Se recomienda encarecidamente incluir las siguientes macros predefinidas en los archivos de instalación desatendida.

- **#predefined.unattendSettings.preinstallConfig#** y **#predefined.unattendSettings postinstallConfig#**. Se utilizan para comunicar el estado del instalador del SO, así como varios pasos de instalación críticos.

  Consulte los siguientes escenarios de ejemplo de implementación de SO para obtener más información acerca de cómo incluir las macros de configuración de la instalación.
  - Despliegue de RHEL y una aplicación Hello World PHP utilizando un archivo de instalación desatendida
  - Despliegue de SLES 12 SP3 con una configuración regional configurable y servidores NTP
  - Despliegue de VMware ESXi v6.7 con personalización de Lenovo a un disco local usando la dirección IP estática
  - Despliegue de Windows 2016 con características personalizadas
- **#predefined.unattendSettings.networkConfig#**. (Para ESXi y solo RHEL) Habilita XClarity Administrator para configurar la red. Esta macro utiliza los valores de red que están especificados en la página Desplegar imágenes de SO. Si no incluye la macro en el archivo desatendido, o si no se define la configuración de red en XClarity Administrator, debe configurar la interfaz IP como parte del archivo de instalación de forma que el host cuente con una ruta de red de vuelta a XClarity Administrator.

  Consulte los siguientes escenarios de ejemplo de implementación de SO para obtener más información acerca de cómo incluir la macro de configuración de red.
  - Despliegue de RHEL y una aplicación Hello World PHP utilizando un archivo de instalación desatendida
  - Despliegue de VMware ESXi v6.7 con personalización de Lenovo a un disco local usando la dirección IP estática
- **#predefined.unattendSettings.storageConfig#**. (Para ESXi y solo RHEL) Habilita XClarity Administrator para configurar el almacenamiento en el host. Esta macro utiliza los valores de almacenamiento que están especificados en la página Desplegar imágenes de SO. Si no incluye la macro en el archivo desatendido, o si no se define la configuración de almacenamiento en XClarity Administrator, debe especificar la configuración de almacenamiento en el archivo de instalación.

  Consulte los siguientes escenarios de ejemplo de implementación de SO para obtener más información acerca de cómo incluir la macro de configuración de almacenamiento.
  - Despliegue de RHEL y una aplicación Hello World PHP utilizando un archivo de instalación desatendida
  - Despliegue de VMware ESXi v6.7 con personalización de Lenovo a un disco local usando la dirección IP estática

Puede crear macros *personalizadas* creando un archivo de configuración y luego asociando el archivo desatendido con un archivo de valores de configuración personalizado. Al importar el archivo de valores de configuración personalizados, XClarity Administrator crea una macro para cada valor de configuración en el archivo.

Procedimiento

Lleve a cabo los pasos siguientes para agregar macros a un archivo de instalación desatendida.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Gestionar imágenes de SO** para mostrar la página Desplegar sistema operativo: Gestionar imágenes de SO.

Paso 2. Haga clic en la pestaña **Archivos de instalación desatendida**.

Paso 3. Seleccione el archivo de instalación desatendida que desee editar.

Paso 4. Haga clic en el icono **Editar** () muestra el cuadro de diálogo Editar archivo de instalación desatendida.

Paso 5. Agregue las macros predefinidas recomendadas, por ejemplo:

1. Coloque el cursor en el archivo de instalación desatendida en cualquier lugar después de la línea 1 (después de la etiqueta <xml>).
2. Expanda la lista **predefine → unattendSettings** en la lista de macros disponibles.
3. Haga clic en **preinstallConfig** y **postinstallConfig** para añadir las macros predefinidas en el archivo de instalación desatendida.

   El siguiente código se añade al archivo:

   #predefined.unattendSettings.preinstallConfig#
   #predefined.unattendSettings.postinstallConfig#

Paso 6. Agregue las macros predefinidas o personalizadas adicionales al colocar el cursor en la ubicación correcta del archivo desatendido y, a continuación, haga clic en la macro de la lista.

Paso 7. Haga clic en **Guardar**.

Asociación de un archivo de instalación desatendida con un archivo de valores de configuración

Puede asociar (enlazar) valores de configuración con un archivo de instalación y, posteriormente, añadir macros personalizadas asociadas a un archivo de instalación desatendida.

Acerca de esta tarea

Puede agregar macros predefinidas a un archivo de instalación desatendida sin asociarla a un archivo de valores de configuración personalizado.

No se puede editar los archivos de valores de configuración asociados con los archivos de instalación desatendida. Sin embargo, puede copiar un archivo asociado y, a continuación, editar la copia.

Procedimiento

Complete los pasos siguientes para asociar un archivo de instalación desatendida con un archivo de valores de configuración.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Aprovisionamiento → Gestionar imágenes de SO** para mostrar la página Desplegar sistema operativo: Gestionar imágenes de SO.

Paso 2. Haga clic en la pestaña **Archivos de instalación desatendida**.

Paso 3. Seleccione el archivo de instalación desatendida personalizado.

Paso 4. Haga clic en el icono **Asociar un archivo de configuración** () para mostrar el cuadro de diálogo Asociar un archivo de instalación desatendida.

Paso 5. Seleccione un archivo de valores de configuración para asociar con el archivo de instalación desatendida.

Paso 6. Puede agregar macros predefinidas o personalizadas para el archivo de instalación desatendida al colocar el cursor en la ubicación del editor dónde desea agrega las macros y hacer clic en las macros de la lista disponible (consulte Inyección de macros predefinidas y personalizadas a un archivo de instalación desatendida).

Se pueden insertar macros en el archivo desatendido utilizando el nombre único del objeto. Para objetos con nombre anidado, separe cada objeto utilizando un punto (por ejemplo, `server_specific_settings.server.locale`). Tenga en cuenta que no se debe incluir el nombre de la entrada superior.

Paso 7. Haga clic en **Asociar** para enlazar los archivos juntos.

Importación de scripts de instalación personalizada

Se puede importar scripts de instalación al repositorio de imágenes de SO. Estos archivos se pueden utilizar posteriormente para personalizar las imágenes de Linux y Windows.

Acerca de esta tarea

Actualmente, solo se admite el uso de scripts posteriores a la instalación.

La siguiente tabla enumera los tipos de archivo para los scripts de instalación que admite Lenovo XClarity Administrator por cada sistema operativo. Tenga en cuenta que algunas versiones del sistema de operación no son compatibles con todos los otros tipos de archivos que admite XClarity Administrator (por ejemplo, algunas versiones RHEL pueden no incluir Perl en el perfil mínimo y, por lo tanto, no se ejecutarán scripts Perl). Asegúrese de utilizar el tipo de archivo correcto para las versiones de sistema operativo que desee desplegar.

Sistema operativo	Tipos de archivo compatibles	Más información
CentOS Linux	No admitido	
Microsoft® Windows® Azure Stack HCI	No admitido	
Microsoft Windows Hyper-V Server	No admitido	
Microsoft® Windows® Server	Archivo de comandos (.cmd), PowerShell (.ps1)	La ruta de datos y archivos personalizados predeterminada es `C:\lxca`. Para obtener más información acerca de los scripts de instalación, consulte el Pagina web Agregar un script personalizado a la instalación de Windows

Sistema operativo	Tipos de archivo compatibles	Más información
Servidor Red Hat® Enterprise Linux (RHEL)	Bash (.sh), Perl (.pm o .pl), Python (.py)	La ruta de datos y archivos personalizados predeterminada es `/home/lxca`. Para obtener más información acerca de los scripts de instalación, consulte el RHEL: Página web de script posterior a la instalación.
Rocky Linux	Bash (.sh), Perl (.pm o .pl), Python (.py)	La ruta de datos y archivos personalizados predeterminada es `/home/lxca`. Para obtener más información acerca de los scripts de instalación, consulte el RHEL: Página web de script posterior a la instalación
SUSE® Linux Enterprise Server (SLES)	Bash (.sh), Perl (.pm o .pl), Python (.py)	La ruta de datos y archivos personalizados predeterminada es `/home/lxca`. Para obtener más información acerca de los scripts de instalación, consulte el SUSE: Sitio web de script de usuario personalizado
Ubuntu	No admitido	
VMware vSphere® Hypervisor (ESXi) con personalización de Lenovo	Bash (.sh), Python (.py)	La ruta de datos y archivos personalizados predeterminada es `/home/lxca`. Para obtener más información acerca de los scripts de instalación, consulte el VMware: Página Web de instalación y actualización de scripts

Nota: El repositorio de imágenes del SO puede almacenar un número ilimitado de archivos predefinidos y personalizados, en caso que haya espacio disponible para almacenar los archivos.

Después de recopilar los datos durante el despliegue del SO, XClarity Administrator crea una instancia del archivo de configuración (lo que incluye la configuración personalizada del archivo seleccionado y un subconjunto de valores predefinidos) en el sistema host que se puede utilizar en el script de instalación posterior.

Puede insertar macros predefinidas y personalizadas (valores de configuración) en el script posterior a la instalación utilizando el nombre único del objeto. Los valores predefinidos se basan dinámicamente en las instancias de XClarity Administrator. Las macros personalizadas se basan dinámicamente en la información ingresada por el cliente que se especifique durante el despliegue del SO.

Notas:

- Escriba el nombre con un símbolo de número (#).
- Para objetos anidados, separe cada nombre de objeto utilizando un punto (por ejemplo, **#server_settings.server0.locale#**).
- Para macros personalizadas, no incluya el nombre del objeto de nivel superior. Para macros predefinidas, use “predefinido” como el prefijo del nombre de macro.
- Cuando se crea un objeto desde una plantilla, el nombre se conecta con un número único, comenzando con 0 (por ejemplo, **server0** y **server1**).

- Puede ver el nombre de cada macro en el cuadro de diálogo Desplegar imágenes de SO en las pestañas Valores personalizados colocando el puntero sobre el icono Ayuda ( ) situado junto a cada configuración personalizada.
- Para obtener una lista de macros predefinidas, consulte Macros predefinidas. Para obtener información acerca de los valores de configuración y macros personalizados, consulte Macros personalizadas.

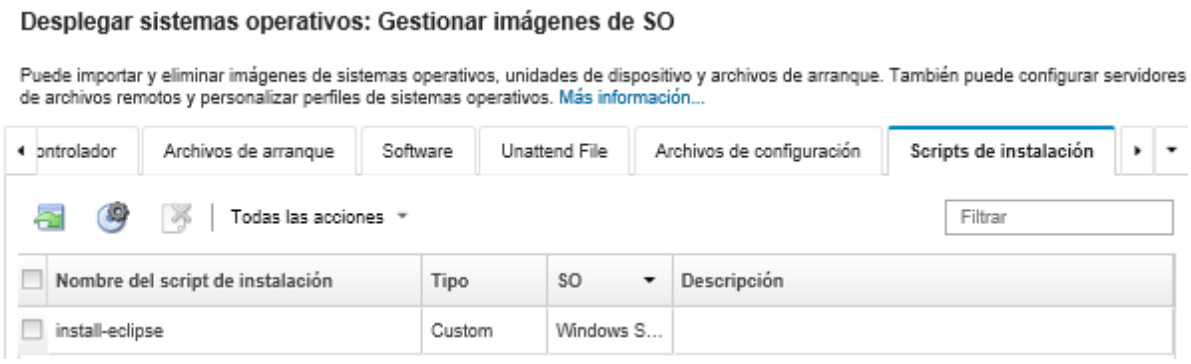
Las macros predefinidas recomendadas en el archivo de instalación desatendida informan el estado del despliegue del sistema operativo final y el estado de informe cuando descarga y ejecuta scripts posteriores a la instalación. Puede modificar los posteriores a la instalación scripts para incluir la generación de informes de estado personalizada, según el sistema operativo de destino. Para obtener más información, consulte el apartado Agregar informes de estado personalizados a los scripts de instalación.

Procedimiento

Para importar los scripts de instalación en el repositorio de imágenes del SO, lleve a cabo los pasos siguientes.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Gestionar imágenes de SO** para mostrar la página Desplegar sistema operativo: Gestionar imágenes de SO.

Paso 2. Haga clic en la pestaña **Scripts de instalación**.



Paso 3. Haga clic en el icono **Importar archivo** ( ). Se muestra el cuadro de diálogo Importar script de instalación.

Paso 4. Haga clic en la pestaña **Importación local** para cargar archivos del sistema local, o haga clic en la pestaña **Importación remota** para cargar archivos desde un servidor de archivo remoto.

Nota: Para cargar un archivo desde un servidor de archivo remoto, debe crear primero un perfil del servidor de archivo remoto pulsando el icono **Configurar servidor de archivo** ( ). Para obtener más información, consulte Configurar un servidor de archivo remoto .

Paso 5. Si desea utilizar un servidor de archivo remoto, seleccione el servidor que desea utilizar desde la lista **Servidor de archivo remoto**.

Paso 6. Seleccione el tipo de sistema operativo.

Paso 7. Escriba el nombre del archivo del script de instalación o haga clic en **Examinar** para buscar el archivo que desea importar.

Paso 8. **Opcional:** escriba una descripción para el script de instalación.

Consejo: utilice el campo **Descripción** para diferenciar archivos personalizados con el mismo nombre.

Paso 9. **Opcional:** seleccione un tipo de suma de comprobación para asegurarse de que el archivo que se está cargando no está dañado y, a continuación, copie y pegue el valor de suma de comprobación en el campo de texto previsto a tal fin.

Si selecciona un tipo de suma de comprobación, debe especificar un valor de suma de comprobación para comprobar la integridad y la seguridad del archivo cargado. El valor debe proceder de una fuente segura de una organización de su confianza. Si el archivo cargado coincide con el valor de suma de comprobación, es seguro realizar el despliegue. De lo contrario, deberá cargar de nuevo el archivo o comprobar el valor de suma de comprobación.

Se admiten tres tipos de suma de comprobación:
- **MD5**
- **SHA1**
- **SHA256**

Paso 10. Haga clic en **Importar**.

Consejo: el archivo se carga a través de una conexión de red segura. Por consiguiente, la fiabilidad y el rendimiento de la red afectan al tiempo que tarda en importarse el archivo.

Si cierra la pestaña del navegador web o la ventana en la que se está cargando el archivo localmente antes de que finalice el proceso, la importación fallará.

Después de finalizar

Los scripts de instalación que se enumeran en la pestaña **Scripts de instalación** de la página Gestionar imágenes de SO.

Desde esta página puede llevar a cabo las siguientes acciones.

- Crear un perfil del servidor de servidor de archivo pulsando el icono **Configurar servidor de archivo** ().
- Quite los scripts de instalación seleccionados al hacer clic en el icono **Eliminar** ().

Para obtener información acerca de cómo añadir un script de instalación a un perfil de imagen del SO personalizado, consulte Creación de un perfil de imagen de SO personalizado.

Agregar informes de estado personalizados a los scripts de instalación

Las macros predefinidas recomendadas en el archivo de instalación desatendida informan el estado del despliegue del sistema operativo final y el estado de informe cuando descarga y ejecuta scripts posteriores a la instalación. Puede incluir informes de estado adicionales en los scripts posteriores a la instalación.

Linux

En Linux, puede utilizar los siguientes comandos `curl` para informar el estado.

```
curl -X PUT -globoff #predefined.otherSettings.statusSettings.urlStatus#
-H "Content-Type: application/json" -d '{"deployStatus":{"id":"<status_ID>"}}'
-cert #predefined.otherSettings.statusSettings.certLocation#/cert.pem
-key #predefined.otherSettings.statusSettings.certLocation#/key.pem
-cacert #predefined.otherSettings.statusSettings.certLocation#/ca-bundle.crt
```

Donde *<status_ID>* puede ser uno de los siguientes valores.
- **44**. El despliegue de carga de trabajo tuvo éxito
- **45**. El despliegue de la carga de trabajo se está ejecutando con una advertencia
- **46**. El despliegue de carga de trabajo falló
- **47**. Mensaje de despliegue de carga de trabajo
- **48**. Error en el script posterior a la instalación personalizada

Tenga en cuenta que el comando `curl` usa macros predefinidos para la URL HTTPS que Lenovo XClarity Administrator usa para informar estados (**predefined.otherSettings.statusSettings.urlStatus**) y para la carpeta que contiene los certificados que se necesitan para acceder al servicio web urlStatus desde el SO

host en el primer inicio (**predefined.otherSettings.statusSettings.certLocation**). El siguiente ejemplo informa que el error ocurrió en el script posterior a la instalación.

El ejemplo siguiente informa de que se produjo un error en el script posterior a la instalación.

```
curl -X PUT -globoff #predefined.otherSettings.statusSettings.urlStatus#
-H "Content-Type: application/json" -d '{"deployStatus":{"id":"48"}}'
-cert #predefined.otherSettings.statusSettings.certLocation#/cert.pem
-key #predefined.otherSettings.statusSettings.certLocation#/key.pem
-cacert #predefined.otherSettings.statusSettings.certLocation#/ca-bundle.crt
```

Windows

Para Wiindows, puede importar el script `LXCA.psm1` y luego llamar los siguientes comandos para informar el estado.

- **initializeRestClient**

  Inicializa al cliente REST. Utilice la siguiente sintaxis para ejecutar este comando. Este comando se requiere antes de ejecutar los comandos de generación de informes.

  ```
  initializeRestClient
  ```

- **testLXCAConnection**

  Comprueba que los XClarity Administrator se pueden conectar con el servidor host. Utilice la siguiente sintaxis para ejecutar este comando. Este comando es opcional pero se recomienda en el script de instalación antes de ejecutar los comandos de generación de informes.

  ```
  testLXCAConnection –masterIP "#predefined.otherSettings.lxcaIp#"
  ```

- **reportWorkloadDeploymentSucceeded**

  Notifica un mensaje de finalización correcta para iniciar sesión en el registro de trabajos de XClarity Administrator. Utilice la siguiente sintaxis para ejecutar este comando.

  Consejo: si el macro **#predefined.unattendSettings.reportWorkloadNotComplete#** se incluye en un archivo de instalación desatendida personalizado o un script posterior a la instalación, incluya el comando **reportWorkloadDeploymentSucceeded** en el script posterior a la instalación para indicar una finalización exitosa. De lo contrario XClarity Administrator informa automáticamente un estado completo después de ejecutar los scripts posteriores a la instalación.

  ```
  reportWorkloadDeploymentSucceeded -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#"
  ```

- **reportWorkloadDeploymentRunningWithWarning**

  Informa de un mensaje de advertencia para iniciar sesión en el registro de trabajo XClarity Administrator. Utilice la siguiente sintaxis para ejecutar este comando.

  ```
  reportWorkloadDeploymentRunningWithWarning -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#" –WarningMessage "<message_text>"
  ```

- **reportWorkloadDeploymentFailed**

  Informa de un mensaje de error para iniciar sesión en el registro de trabajo XClarity Administrator. Utilice la siguiente sintaxis para ejecutar este comando.

  ```
  reportWorkloadDeploymentFailed -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#" -ErrorMessage "<message_text>"
  ```

- **reportCustomPostInstallScriptError**

  Informa de un mensaje de error de script posterior a la instalación para iniciar sesión en el registro de trabajo XClarity Administrator. Utilice la siguiente sintaxis para ejecutar este comando.

  ```
  reportCustomPostInstallScriptError -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#" -Message "<message_text>"
  ```

- **reportWorkloadDeploymentMessage**

  Informa de un mensaje general para iniciar sesión en el registro de trabajo XClarity Administrator sin afectar el estado del despliegue. Utilice la siguiente sintaxis para ejecutar este comando.

  ```
  reportWorkloadDeploymentMessage -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#" -Message "<message_text>"
  ```

Donde <*message_text*> es el mensaje que desea arrojar a XClarity Administrator para cada condición de estado.

Tenga en cuenta que estos comandos usan macros predefinidos para la dirección IP de la instancia XClarity Administrator (**#predefined.otherSettings.lxcaIp#**) y para el UUID del servidor de host en el que se implementará el sistema operativo (**#predefined.hostPlatforms.uuid#**).

El siguiente ejemplo es un script de instalación de PowerShell que instala Java y presenta un error si la instalación falla

```
import-module C:\windows\system32\WindowsPowerShell\v1.0\Modules\LXCA\LXCA.psm1

initializeRestClient

testLXCAConnection –masterIP "#predefined.otherSettings.lxcaIp#"

Write-Output "Reporting status to Lenovo XClarity Administator..."
   reportWorkloadDeploymentMessage -masterIP "#predefined.otherSettings.lxcaIp#"
   -UUID "#predefined.hostPlatforms.uuid#" -Message "Installing Java"

Write-Output "Install Java...."
   Invoke-Command -ScriptBlock {#predefined.otherSettings.deployDataAndSoftwareLocation#\jre-8u151-windows-x64.exe
   [INSTALLCFG=#predefined.otherSettings.deployDataAndSoftwareLocation#\java_configfile.cfg] /s}

if ($LastExitCode -ne 0) {
   reportWorkloadDeploymentFailed -masterIP "#predefined.otherSettings.lxcaIp#"
      -UUID "#predefined.hostPlatforms.uuid#" -ErrorMessage "Java could not be installed"
}

Write-Output "Completed install of Java for Administrator user."
```

Importación de software personalizado

Se puede importar software en el repositorio de imágenes de SO. Estos archivos se pueden utilizar posteriormente para personalizar las imágenes de Linux y Windows

Acerca de esta tarea

Estos archivos de software personalizado se instalan después de completar el despliegue de sistema operativo y la ejecución de los scripts de instalación posterior.

Se admite los siguientes tipos de archivo para software personalizado.

Sistema operativo	Tipos de archivo compatibles	Más información
CentOS Linux	No admitido	
Microsoft® Windows® Azure Stack HCI	No admitido	
Microsoft Windows Hyper-V Server	No admitido	

Sistema operativo	Tipos de archivo compatibles	Más información
Microsoft Windows® Server	Un archivo .zip que contenga la carga útil de software.	La ruta de archivos y datos personalizados predeterminada es `C:\lxca`.
Servidor Red Hat® Enterprise Linux (RHEL)	Un archivo .tar.gz que contenga la carga útil de software	La ruta de datos y archivos personalizados predeterminada es `/home/lxca`.
SUSE® Linux Enterprise Server (SLES)	Un archivo .tar.gz que contenga la carga útil de software	La ruta de datos y archivos personalizados predeterminada es `/home/lxca`.
Rocky Linux	Un archivo .tar.gz que contenga la carga útil de software	La ruta de datos y archivos personalizados predeterminada es `/home/lxca`.
Ubuntu	No admitido	
VMware vSphere® Hypervisor (ESXi) con personalización de Lenovo	Un archivo .tar.gz que contenga la carga útil de software	La ruta de datos y archivos personalizados predeterminada es `/home/lxca`.

Nota: El repositorio de imágenes del SO puede almacenar un número ilimitado de archivos predefinidos y personalizados, en caso que haya espacio disponible para almacenar los archivos.

Procedimiento

Para importar software en el repositorio de imágenes del SO, lleve a cabo los pasos siguientes.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Aprovisionamiento → Gestionar imágenes de SO** para mostrar la página Desplegar sistema operativo: Gestionar imágenes de SO.

Paso 2. Haga clic en la pestaña **Software**.

Paso 3. Haga clic en el icono **Importar archivo** ( ). Se muestra el cuadro de diálogo Importar script de instalación.

Paso 4. Haga clic en la pestaña **Importación local** para cargar archivos del sistema local, o haga clic en la pestaña **Importación remota** para cargar archivos desde un servidor de archivo remoto.

Nota: Para cargar un archivo desde un servidor de archivo remoto, debe crear primero un perfil del servidor de archivo remoto pulsando el icono **Configurar servidor de archivo** ( ). Para obtener más información, consulte Configurar un servidor de archivo remoto .

Paso 5. Si desea utilizar un servidor de archivo remoto, seleccione el servidor que desea utilizar desde la lista **Servidor de archivo remoto**.

Paso 6. Seleccione el tipo de sistema operativo.

Paso 7. Escriba el nombre del archivo del software o haga clic en **Examinar** para buscar el archivo que desea importar.

Paso 8. **Opcional:** escriba una descripción del archivo de software.

Consejo: utilice el campo **Descripción** para diferenciar archivos personalizados con el mismo nombre.

Paso 9. **Opcional:** seleccione un tipo de suma de comprobación para asegurarse de que el archivo que se está cargando no está dañado y, a continuación, copie y pegue el valor de suma de comprobación en el campo de texto previsto a tal fin.

Si selecciona un tipo de suma de comprobación, debe especificar un valor de suma de comprobación para comprobar la integridad y la seguridad del archivo cargado. El valor debe proceder de una fuente segura de una organización de su confianza. Si el archivo cargado coincide con el valor de suma de comprobación, es seguro realizar el despliegue. De lo contrario, deberá cargar de nuevo el archivo o comprobar el valor de suma de comprobación.

Se admiten tres tipos de suma de comprobación:
- **MD5**
- **SHA1**
- **SHA256**

Paso 10. Haga clic en **Importar**.

Consejo: el archivo se carga a través de una conexión de red segura. Por consiguiente, la fiabilidad y el rendimiento de la red afectan al tiempo que tarda en importarse el archivo.

Si cierra la pestaña del navegador web o la ventana en la que se está cargando el archivo localmente antes de que finalice el proceso, la importación fallará.

Después de finalizar

Los scripts de instalación que se enumeran en la pestaña **Software** de la página Gestionar imágenes de SO.

Desde esta página puede llevar a cabo las siguientes acciones.

- Crear un perfil del servidor de servidor de archivo pulsando el icono **Configurar servidor de archivo** ( ).
- Quitar los archivos de software seleccionados al hacer clic en el icono **Eliminar** ( ).

Para obtener información acerca de cómo añadir un archivo de software a un perfil de imagen del SO personalizado, consulte Creación de un perfil de imagen de SO personalizado.

Creación de un perfil de imagen de SO personalizado

También se puede agregar controladores de dispositivo personalizados, archivos de arranque (solo Windows), valores de configuración, archivos de instalación desatendida, scripts de instalación y software a un perfil de imagen del SO predefinido que exista en el repositorio de imágenes del SO. Al agregar archivos a una imagen de SO, Lenovo XClarity Administrator crea un perfil personalizado para dicha imagen. El perfil personalizado incluye los archivos personalizados y las opciones de instalación.

Antes de empezar

Los archivos personalizados que desee agregar deben existir en el repositorio de imágenes del SO (consulte Importar archivos de arranque, Importación de controladores de dispositivos, Importación de valores de configuración personalizada, Importación de archivos de instalación desatendida personalizados, Importación de scripts de instalación personalizada y Importación de software personalizado).

Procedimiento

Para personalizar una imagen del SO, lleve a cabo los pasos siguientes.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Gestionar imágenes de SO** para mostrar la página Desplegar sistema operativo: Gestionar imágenes de SO.

Paso 2. Haga clic en la pestaña **Imágenes del SO**.

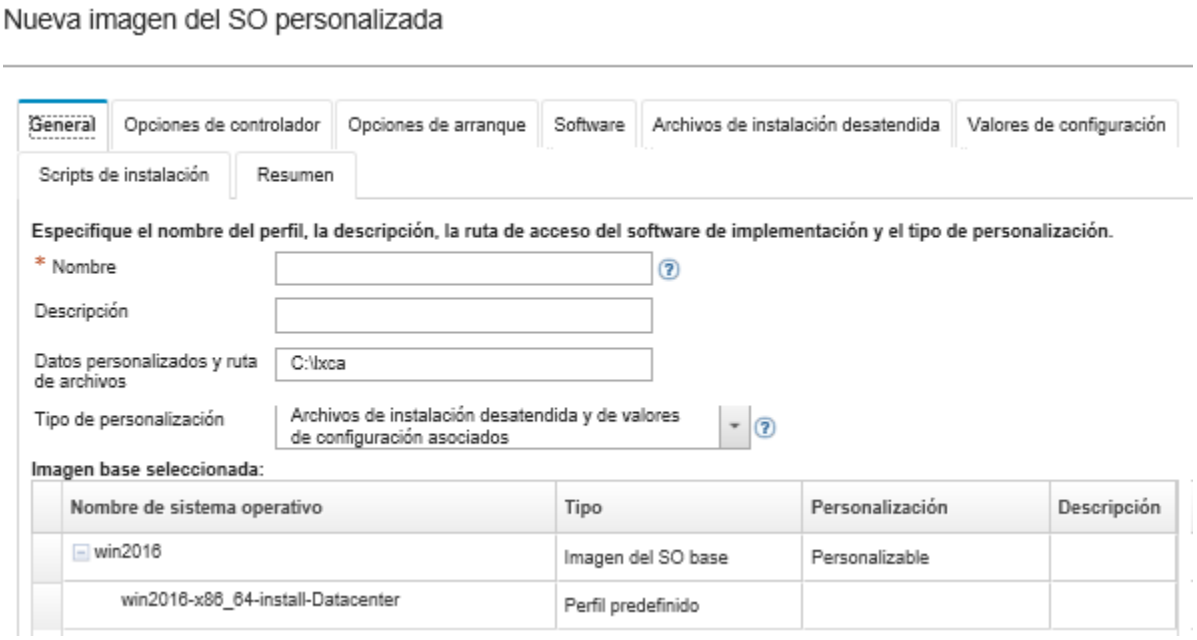
Paso 3. Seleccione el perfil de imagen del SO que desee personalizar.

La columna **Personalización** identifica las imágenes del SO que se pueden personalizar. Haga clic en el icono **Ayuda** ( ) para obtener más información acerca de la personalización de una imagen del SO específica.

- **Personalizable**. La imagen del SO admite la personalización, pero no está personalizada.
- **No personalizable**. La imagen del SO no admite la personalización.

Nota: Puede importar imágenes del SO base adicionales (en formato .iso) desde un sistema local o remoto, al hacer clic en el icono **Importar archivo** ( ).

Paso 4. Haga clic en el icono **Crear perfil personalizado** ( ). Se muestra el cuadro de diálogo Nueva imagen del SO personalizada.



Paso 5. En la pestaña **General**, especifique un nombre, una descripción, la ruta para los datos de despliegue en el host del despliegue y el tipo de personalización y archivos personalizados para el nuevo perfil personalizado de imagen del SO.

El tipo de personalización puede ser uno de los siguientes:

- **Solo archivos de instalación desatendida**
- **Solo archivos de configuración**
- **Archivos de instalación desatendida y de configuración no asociados**

- **Archivos de instalación desatendida y de configuración asociados**
- **Ninguno**

Paso 6. Haga clic en **Siguiente**.

Paso 7. En la pestaña **Controladores de dispositivos**, seleccione el controlador de dispositivo que desee agregar al perfil de imagen del SO Linux.

Para obtener una lista de los formatos compatibles, consulte Importación de controladores de dispositivos.

El archivo seleccionado se aplica después de que se completa el asistente de configuración.

Nota: Puede importar controladores de dispositivos adicionales (en formato .iso o .rpm) desde un sistema local o remoto, al hacer clic en el icono **Importar archivo** ( ).

Paso 8. Haga clic en **Siguiente**.

Paso 9. (Solo Windows) En la pestaña **Opciones de arranque**, seleccione los archivos de opciones de arranque que desee agregar al perfil de imagen del SO Windows.

Para obtener una lista de los formatos compatibles, consulte Importar archivos de arranque.

El archivo seleccionado se aplica después de que se completa el asistente de configuración.

Paso 10. Haga clic en **Siguiente**.

Paso 11. En la pestaña **Valores de configuración** (si corresponde), seleccione uno o varios archivos de configuración personalizados que desee agregar al perfil de imagen del SO. Puede seleccionar un archivo como máximo.

Paso 12. Haga clic en **Siguiente**.

Paso 13. En la pestaña **Archivos de instalación desatendida**:

a. Seleccione el archivo de instalación desatendida que desee agregar al perfil de imagen del SO.

   Para obtener una lista de los formatos compatibles, consulte Importación de archivos de instalación desatendida personalizados.

   El archivo seleccionado se aplica después de que se completa el asistente de configuración.

b. Seleccione un archivo de configuración para asociar con el archivo de instalación desatendida desde la columna **Archivo de configuración asociado**

c. Opcionalmente, seleccione macros personalizadas que están disponibles en el archivo de configuración seleccionado o agregue macros personalizados en formato .xml.

Paso 14. Haga clic en **Siguiente**.

Paso 15. En la pestaña **Scripts de instalación** (si corresponde), seleccione los scripts de instalación que desee agregar al perfil de imagen del SO Windows. Puede seleccionar como máximo un script posterior a la instalación.

Para obtener una lista de los formatos compatibles, consulte Importación de scripts de instalación personalizada.

El archivo seleccionado se aplica después de que se completa el asistente de configuración.

Nota: Se puede importar scripts de instalación adicionales (en formato .iso o .rpm) desde un sistema local o remoto, al hacer clic en el icono **Importar archivo** ( ).

Paso 16. Haga clic en **Siguiente**.

Paso 17. En la pestaña **Software**, seleccione el controlador de dispositivo que desee agregar al perfil de imagen del SO Linux.

Para obtener una lista de los formatos compatibles, consulte Importación de software personalizado.

El archivo seleccionado se aplica después de que se completa el asistente de configuración.

Nota: Puede importar software adicional (en formato .iso o .rpm) desde un sistema local o remoto, al hacer clic en el icono **Importar archivo** ().

Paso 18. Haga clic en **Siguiente**.

Paso 19. Revise los valores en la pestaña **Resumen** y haga clic en **Personalizar** para crear el perfil de imagen del SO personalizado.

Después de finalizar

El perfil de imágenes del SO personalizado se encuentra en la pestaña **Imágenes del SO**, en la página Gestionar imágenes de SO del sistema operativo base.

Desde esta página puede llevar a cabo las siguientes acciones:

- Importar un perfil de imagen del SO personalizado y aplíquelo a una imagen del SO base pulsando **Importar/Exportar perfil → Exportar imagen de perfil personalizada** (consulte Importación de un perfil de imagen del SO personalizado).
- Exportar un perfil de imagen del SO personalizado seleccionado al hacer clic en **Importar/Exportar perfil → Exportar imagen de perfil personalizada**.
- Modificar un perfil de imagen del SO personalizado seleccionado pulsando el icono **Editar** ().
- Quitar un perfil de imagen del SO personalizado seleccionado pulsando el icono **Eliminar** ().

Configuración de valores globales de despliegue del SO

Los valores globales se utilizan como valores predeterminados cuando se despliegan sistemas operativos.

Acerca de esta tarea

En la página Valores globales, puede configurar los siguientes valores:

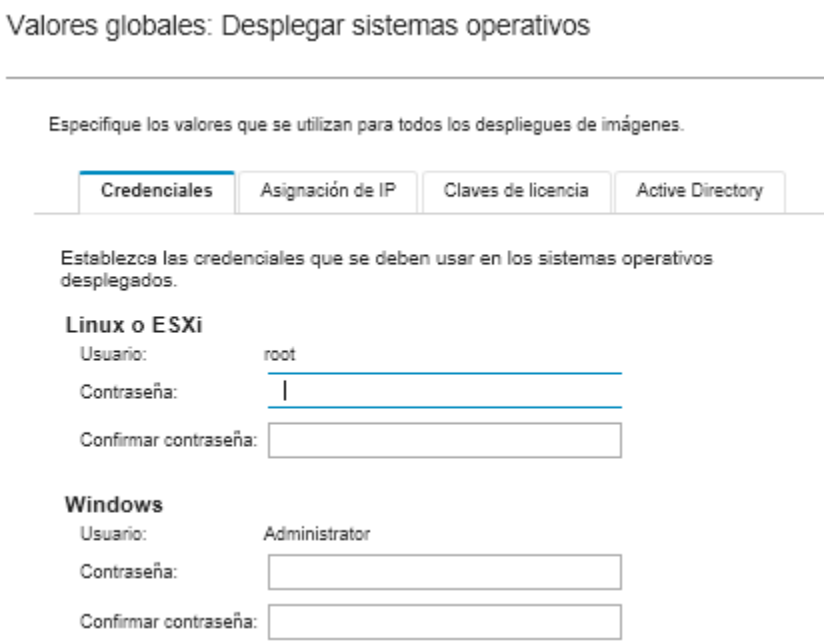
- La contraseña que la cuenta de usuario de administrador utiliza para desplegar sistemas operativos
- El método utilizado para asignar direcciones IP a los servidores
- Las claves de licencia que deben usarse para activar los sistemas operativos instalados
- Opcionalmente es posible unir un dominio de Active Directory como parte del despliegue del sistema operativo Windows.

Procedimiento

Para configurar los valores globales que se utilizarán en todos los servidores, lleve a cabo los pasos siguientes.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Aprovisionamiento → Desplegar imágenes del SO** para mostrar la página Desplegar imágenes del SO.

Paso 2. Haga clic en el icono **Valores globales** ( ) para mostrar el cuadro de diálogo Valores globales: Desplegar sistemas operativos.



Paso 3. En la pestaña **Credenciales**, introduzca la contraseña de la cuenta de administrador que debe utilizarse para iniciar sesión en el sistema operativo.

Paso 4. En la pestaña **Asignación de IP**, seleccione las siguientes opciones.

a. **Opcional:** Seleccione **Usar VLAN** para permitir la configuración de los valores de VLAN en el cuadro de diálogo Valores de red (consulte Configuración de los valores de red para servidores gestionados).

Notas: Notas:

- El etiquetado VLAN no es compatible con los despliegues de sistemas operativos Linux.
- El etiquetado VLAN no es compatible con los despliegues de sistemas operativos de dispositivos ThinkServer.
- El modo VLAN solo se admite para servidores que tienen direcciones MAC en su inventario. Si AUTO es la única dirección MAC disponible para un servidor, entonces no se pueden usar VLAN para desplegar sistemas operativos en ese servidor.

b. Seleccione el método para asignar direcciones IP al configurar el sistema operativo desplegado:

Nota: La interfaz de red de XClarity Administrator que se utiliza para la gestión debe configurarse para conectarse al controlador de la placa base utilizando el mismo método de dirección IP que elige en el cuadro de diálogo Valores globales: desplegar sistemas operativos. Por ejemplo, si XClarity Administrator esta configurado para utilizar eth0 con fines de gestión y usted elige utilizar las direcciones IPv6 estáticas asignadas manualmente al configurar el SO implementado, entonces eth0 se debe configurar con una dirección IPv6 que tenga conectividad al controlador de gestión de la placa base.

- **Asignar manualmente una dirección IPv4 estática**. Si elige asignar direcciones IPv4 estáticas, asegúrese de que configura la dirección IPv4 estática, la dirección de la puerta de enlace y la máscara de subred para el servidor antes de desplegar el sistema operativo (consulte Configuración de los valores de red para servidores gestionados).

- **Utilizar el protocolo de configuración dinámica de host (DHCP) para asignar las direcciones**. Si ya dispone de una infraestructura DHCPv4 existente en la red, puede utilizarla para asignar direcciones IP a los servidores.

  Nota: DHCP IPv6 no se admite para el despliegue de sistemas operativos.
- **Asignar manualmente una dirección IPv6 estática**. Si elige asignar direcciones IPv6 estáticas, asegúrese de que configura la dirección IPv6 estática, la dirección de la puerta de enlace y la máscara de subred para el servidor antes de desplegar el sistema operativo (consulte Configuración de los valores de red para servidores gestionados).

Paso 5. **Opcional:** En la pestaña **Claves de licencia**, especifique las claves de licencia por volumen global que desea utilizar para activar los sistemas operativos Windows instalados.

Si especifica claves de licencia por volumen global en esta pestaña, la página Desplegar imágenes del SO le permite seleccionar las claves de licencia especificadas para cualquier perfil de imagen del SO Windows.

Consejo: XClarity Administrator admite claves de licencia por volumen global para las instalaciones de Windows, así como claves de licencia minoristas individuales, tanto para Windows como para VMware ESXi. Puede especificar claves de licencia minoristas individuales como parte del procedimiento de despliegue (consulte Despliegue de la imagen de un sistema operativo).

Paso 6. **Opcional:** En la pestaña **Active Directory**, configure los valores de Active Directory para los despliegues de sistemas operativos Windows. Para obtener más información sobre la integración con Active Directory, consulte Integración con Windows Active Directory.

Paso 7. Haga clic en **Aceptar** para cerrar el cuadro de diálogo.

Configuración de los valores de red para servidores gestionados

Los valores de red son opciones de configuración específicas para cada servidor. Debe configurar los valores de red que se van a utilizar para un servidor gestionado antes de poder desplegar un sistema operativo en dicho servidor.

Acerca de esta tarea

Si va a utilizar DHCP para asignar direcciones IP de forma dinámica, debe configurar la dirección MAC.

Si utiliza direcciones IP estáticas, debe configurar los valores de red siguientes para un servidor específico antes de desplegar un sistema operativo en ese servidor. Una vez configurados estos valores, el estado de despliegue el servidor cambia a “Preparado”. (Tenga en cuenta que algunos campos no están disponibles para las direcciones IPv6 estáticas.)

- Nombre de host

  El nombre de host debe cumplir con las reglas siguientes:
  - El nombre de host de cada servidor gestionado debe ser único.
  - El nombre de host puede contener cadenas (etiquetas) separadas por un punto (.).
  - Cada etiqueta puede contener letras ASCII, dígitos y guiones (-); sin embargo, la cadena no puede comenzar ni terminar con un guion y no puede estar compuesta únicamente de dígitos.
  - La primera etiqueta puede ser 2 a 15 caracteres de longitud. Las etiquetas siguientes pueden ser de 2 a 63 caracteres de longitud.
  - La longitud máxima del nombre de host no debe superar los 255 caracteres.
- Dirección MAC del puerto en el host donde va a instalarse el sistema operativo.

  La dirección MAC está configurada en AUTO de forma predeterminada. Esta configuración detecta automáticamente los puertos Ethernet que se pueden configurar y utilizar para el despliegue. La primera

dirección MAC (puerto) que se detecta se utiliza manera predeterminada. Si se detecta la conectividad en otra dirección MAC, el host de XClarity Administrator se reinicia automáticamente para utilizar la dirección MAC recién detectada para el despliegue.

Puede determinar el estado del puerto de dirección MAC que se utiliza para el despliegue del SO desde el menú desplegable de la **Dirección MAC** en el cuadro de diálogo Valores de red. Si hay varios puertos en funcionamiento o si todos los puertos están inactivos, se utiliza AUTO de manera predeterminada.

Notas:

- No se admiten los puertos de red virtuales. No utilice un puerto de red físico para simular varios puertos de red virtual.
- Cuando el valor de red del servidor está establecido en AUTO, XClarity Administrator puede detectar automáticamente los puertos de red en las ranuras 1 a 16. Al menos un puerto de las ranuras 1 a 16 debe tener una conexión a XClarity Administrator.
- Si desea utilizar un puerto de red en la ranura 17 o superior para la dirección MAC, no puede utilizar AUTO. En su lugar, debe establecer la configuración de red del servidor en la dirección MAC del puerto específico que desee utilizar.
- Para los servidores ThinkServer, no se muestran todas las direcciones MAC del host. En la mayoría de los casos, las direcciones MAC para los adaptadores Ethernet AnyFabric se muestran en el cuadro de diálogo Editar valores de red. Las direcciones MAC para otros adaptadores Ethernet (como la LAN en placa madre) no se muestran. En los casos donde la dirección MAC de un adaptador no está disponible, utilice el método AUTO para los despliegues que no son VLAN.

- Dirección IP y Máscara de subred
- Puerta de enlace de IP
- Hasta dos servidores del sistema de nombres de dominio (DNS)
- Velocidad de la unidad de transmisión máxima (MTU)
- ID de VLAN, si está habilitado el modo IP de VLAN

Si elige utilizar VLAN, puede asignar un Id. de VLAN al adaptador de red del host que se está configurando.

Procedimiento

Para configurar valores de red para uno o varios servidores, lleve a cabo los pasos siguientes.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Desplegar imágenes de SO** para mostrar la página Desplegar sistema operativo: Desplegar imágenes de SO.

Paso 2. Seleccione uno o más servidores para configurarlos. Puede seleccionar hasta 28 servidores para su configuración simultánea.

Paso 3. Haga clic en **Cambiar selección → Valores de red** para mostrar la página Editar valores de red.

Paso 4. Rellene los campos de la tabla para cada servidor.

Consejo: en vez de completar cada fila por separado, puede actualizar todas las filas de la tabla para algunos de los campos:

a. Haga clic en **Cambiar todas las filas → Nombre de host** para establecer los nombres de host de todos los servidores, ya sea utilizando un esquema predefinido o un esquema de denominación personalizado.

b. Haga clic en **Cambiar todas las filas → Dirección IP** para asignar un rango de direcciones IP, una máscara de subred y una puerta de enlace. La dirección IP se asigna para cada servidor, empezando por la primera dirección IP y acabando por la última dirección IP que se visualiza. La máscara de subred y la dirección IP de la puerta de enlace se aplican a cada servidor.

c. Haga clic en **Cambiar todas las filas → Sistema de nombres de dominio (DNS)** para establecer los servidores DNS que el sistema operativo usará para la búsqueda DNS. Si la red define automáticamente los servidores DNS, o si no desea definir servidores DNS, seleccione **Ninguno**.

d. Haga clic en **Cambiar todas las filas → Unidad de transmisión máxima (MTU)** para establecer la MTU que se usará en el adaptador Ethernet configurado en el sistema operativo desplegado.

e. Haga clic en **Cambiar todas las filas → VLAN ID** para establecer un Id. de VLAN específico para el etiquetado VLAN del sistema operativo.

   Puede especificar un valor entre 1 y 4095. El valor predeterminado es 1, lo que significa que no se usa el modo VLAN.

   Esta opción solo está disponible cuando se habilita Usar VLAN en el cuadro de diálogo Valores globales (consulte Configuración de valores globales de despliegue del SO).

   Importante:

   - Solo especifique un Id. de VLAN cuando se requiere una etiqueta de VLAN para que funcione en la red. El **uso de etiquetas de VLAN** puede afectar el enrutamiento de la red entre el sistema operativo del host y el XClarity Administrator.
   - Los chasis o conmutadores de la parte superior del bastidor se deben configurar de forma independiente para gestionar paquetes con etiquetas de VLAN. Asegúrese de que XClarity Administrator y la red de datos estén configurados para gestionar estos paquetes correctamente.
   - El modo VLAN solo se admite para servidores que tienen direcciones MAC en su inventario. Si AUTO es la única dirección MAC disponible para un servidor, entonces no se pueden usar VLAN para desplegar sistemas operativos en ese servidor.
   - El etiquetado VLAN no es compatible con los despliegues del sistema operativo Linux; No obstante, si desea desplegar con VLAN en algunos servidores y también desplegar en otros servidores sin VLAN al mismo tiempo, puede forzar el despliegue bajo el modo VLAN estableciendo el Id. de VLAN en 1.

Paso 5. Haga clic en **Aceptar** para guardar los valores. Los valores se guardan y persisten solo en la memoria caché de almacenamiento local de su navegador web.

Resultados

Ahora, cada servidor configurado muestra **Preparado** como estado del despliegue en la página Desplegar sistema operativo: Desplegar imágenes de SO.

Elegir la ubicación de almacenamiento de los servidores gestionados

Elija la ubicación de almacenamiento preferida donde desee desplegar la imagen del sistema operativo para uno o varios servidores.

Antes de empezar

Evalúe las observaciones acerca de almacenamiento y opciones de arranque antes de seleccionar una ubicación de almacenamiento (consulte Consideraciones del despliegue del sistema operativo).

Puede desplegar un sistema operativo en los siguientes tipos de almacenamiento:

- **Unidad de disco local**

Solo se admiten discos conectados a un controlador RAID o HBA SAS/SATA.

Lenovo XClarity Administrator instala la imagen del sistema operativo en el primer disco local enumerado en el servidor RAID gestionado.

Si el RAID del servidor no está configurado correctamente o si está inactivo, puede que el disco local no esté visible en Lenovo XClarity Administrator. Para solucionar el problema, habilite la configuración del RAID mediante patrones de configuración (consulte Definición de almacenamiento local) o mediante el software de gestión de RAID del servidor.

Notas:

- Si también hay una unidad M.2 presente, la unidad de disco local debe configurarse para RAID de hardware.
- Si se habilita un adaptador SATA, el modo SATA *no debe* configurarse en “IDE”.
- Para servidores ThinkServer, los sistemas operativos se pueden desplegar solo en el disco local. El almacenamiento SAN y los hipervisores integrados no son compatibles.
- Para servidores ThinkServer, la configuración está disponible solo a través del software de gestión de RAID en el servidor.

Por ejemplo, para desplegar VMware ESXi 5.5 en una unidad de disco instalada localmente, consulte Despliegue de ESXi en una unidad de disco duro local.

- **(Solo ESXi) Hipervisor integrado (adaptador multimedia USB o SD)**

  Esta ubicación solo es aplicable cuando se despliega una imagen de VMware ESXi en servidores gestionados.

  El hipervisor integrado puede ser uno de los siguientes dispositivos:

  - La clave USB de IBM License (PN 41Y8298) o la clave USB licenciada por Lenovo que se monta en un puerto de uso específico, en uno de los siguientes servidores:
    - Flex System x222
    - Flex System x240
    - Flex System x440
    - Flex System x480
    - Flex System x880
    - System x3850 X6
    - System x3950 X6
  - El adaptador de medio SD que está instalado en los siguientes servidores:
    - Flex System x240 M5
    - System x3500 M5
    - System x3550 M5
    - System x3650 M5

    Además, la unidad se debe configurar tal como se indica a continuación:
    - Las unidades correspondientes en el adaptador multimedia deben estar definidas.
    - El modo del adaptador multimedia SD debe configurarse en **Operativo**.
    - El propietario debe estar configurado como Sistema o Solo sistema.
    - Debe haberse establecido un acceso de lectura y escritura.
    - La unidad debe tener asignado un número LUN de 0.

    Importante: Si el adaptador multimedia SD no se configura de forma correcta, el despliegue del sistema operativo en dicho adaptador desde Lenovo XClarity Administrator no se realiza correctamente.

    Puede cambiar el modo del adaptador multimedia SD a **Configuración** y configurar el adaptador multimedia a través de la CLI del controlador de gestión utilizando el comando `sdraid`. Para obtener

información adicional acerca de cómo establecer el modo del adaptador multimedia SD y configurar el adaptador desde la CLI, consulte la Documentación en línea de Integrated Management Module II.

Si hay dos claves de hipervisor instaladas en el servidor gestionado, el instalador de VMware selecciona la primera clave enumerada para el despliegue.

Nota: si intenta desplegar Microsoft Windows en un servidor gestionado que tiene instalada una clave de hipervisor se podrían producir problemas aunque no seleccione la clave del hipervisor integrada. Si se producen errores de despliegue de Windows, quite la clave del hipervisor integrada del servidor gestionado e intente desplegar de nuevo Microsoft Windows en ese servidor.

- **Unidad M.2**

  Lenovo XClarity Administrator instala la imagen del sistema operativo en la primera unidad M.2 que está configurada en el servidor gestionado.

  El almacenamiento M.2 solo se admite en servidores de ThinkSystem.

  Atención: Si un dispositivo gestionado cuenta con dos unidades locales (SSD, SAS o SATA) que no están configuradas para RAID de hardware y unidades M.2, se deben deshabilitar las unidades locales en el caso que desee usar las unidades M.2, o bien, se deben deshabilitar las unidades M.2 si desea usar las unidades locales. Puede deshabilitar los dispositivos del controlador de almacenamiento incorporado y los ROM heredados y de opción de almacenamiento de UEFI mediante el uso de patrones de configuración. Para esto, seleccione Deshabilitar disco local en la pestaña Almacenamiento local del asistente o cree un patrón de configuración desde un servidor existente y, a continuación, deshabilite los dispositivos M.2 en el patrón de UEFI extendido.

- **Almacenamiento SAN**

  Lenovo XClarity Administrator instala la imagen del sistema operativo en el destino de arranque de SAN que está configurado en el servidor gestionado.

  Se admiten los siguientes protocolos.
  - Fibre Channel
  - Fibre Channel sobre Ethernet
  - SAN iSCSI (utilizando solo el adaptador Emulex VFA 5.2 2x10 GbE SFP+ y FCoE/iSCSI SW o el adaptador Emulex VFA 5.2 ML2 2x10 GbE SFP+ y los adaptadores FCoE/iSCSI SW)

  En los servidores de bastidor gestionados, solo puede desplegar Windows o RHEL en un almacenamiento SAN. Asegúrese de que el destino de arranque de SAN esté configurado en los servidores gestionados. También puede configurar el destino de arranque de SAN FC utilizando un patrón de servidor (consulte Definición de opciones de arranque)

  Cuando despliegue VMware ESXi:

  - Los discos duros locales deben estar deshabilitados o quitados del servidor. Puede deshabilitar los discos duros locales utilizando patrones de servidor (consulte Definición de almacenamiento local)
  - Si hay disponibles varios volúmenes de SAN, solo se utilizará el primero para el despliegue.

  Asegúrese de que el volumen del SO en el que está realizando la instalación sea el único volumen visible para el sistema operativo.

  Por ejemplo, para desplegar VMware ESXi 5.5 en volúmenes SAN que están anexados a los servidores, consulte Despliegue de ESXi en un almacenamiento SAN.

Nota: Cada servidor debe tener un adaptador RAID de hardware o HBA SAS/SATA instalado y configurado. No se admite el RAID de software que generalmente se encuentra está presente en el adaptador de almacenamiento Intel SATA incorporado o el almacenamiento generalmente se especifica como JBOD. Sin embargo, si un adaptador de RAID de hardware no está presente, configurar el adaptador SATA en el **Modo de AHCI SATA** habilita el despliegue del sistema operativo o la configuración de discos no configurados en

buen estado en JBOD en algunos casos. Para obtener más información, consulte El instalador del SO no puede encontrar el disco en el que desea instalar XClarity Administrator en la documentación en línea de XClarity Administrator.

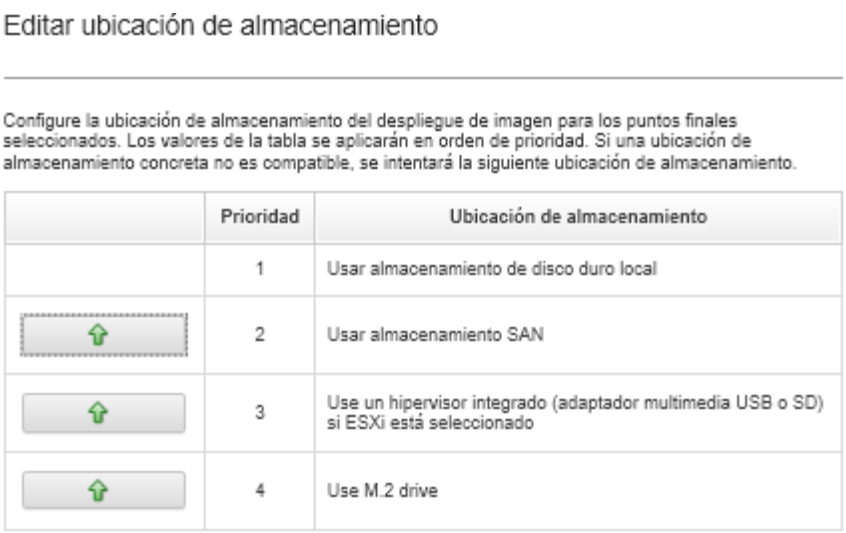
Procedimiento

Lleve a cabo los pasos siguientes para elegir la ubicación de almacenamiento para uno o varios servidores gestionados.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, pulse **Aprovisionamiento → Desplegar imágenes de SO** para mostrar la página Desplegar imágenes de SO.

Paso 2. Seleccione los servidores cuyos valores de almacenamiento desee cambiar.

Paso 3. Haga clic en **Cambiar selección → Ubicación de almacenamiento** para cambiar el orden de prioridad de las ubicaciones de almacenamiento de todos los servidores seleccionados. Si la primera ubicación de almacenamiento no es compatible, se intentará la siguiente ubicación de almacenamiento.



Puede establecer la prioridad de las ubicaciones de almacenamiento siguientes:
- **Utilizar almacenamiento de la unidad de disco local**
- **Use un hipervisor integrado (adaptador multimedia USB o SD) si ESXi está seleccionado**
- **Usar unidad M.2**
- **Usar el almacenamiento SAN**

Paso 4. Para cada servidor, en la columna **Almacenamiento** seleccione la ubicación de almacenamiento preferida donde desee desplegar la imagen del sistema operativo. Puede elegir entre los valores siguientes, que corresponden a los valores del paso anterior.
- **Unidad de disco local**
- **Hipervisor integrado**
- **Unidad M.2**
- **Almacenamiento SAN**

Si selecciona **Almacenamiento SAN**, se muestra un cuadro de diálogo para configurar el volumen SAN. Asegúrese de que se pueda acceder al volumen SAN de destino durante la implementación.

Si la ubicación de almacenamiento seleccionada no es compatible con el servidor, Lenovo XClarity Administrator intenta desplegar el sistema operativo en la ubicación de almacenamiento que siga en el orden de prioridad definido en el paso anterior.

Despliegue de la imagen de un sistema operativo

Puede utilizar Lenovo XClarity Administrator para desplegar la imagen de un sistema operativo hasta en 28 servidores al mismo tiempo.

Antes de empezar

Lea las consideraciones de despliegue del sistema operativo antes de intentar desplegar sistemas operativos en los servidores gestionados (consulte Consideraciones del despliegue del sistema operativo).

En la pestaña **imágenes del SO**, asegúrese de que el **Estado del despliegue** del sistema operativo que va a desplegar esté definido en “Preparado.” Para desplegar el sistema operativo Windows, se requiere un archivo de arranque de WinPE. Si un archivo de WinPE correspondiente no está disponible, el **Estado del despliegue** se establece en “no preparado” y no se puede desplegar el sistema operativo. Debe descargar e importar manualmente un archivo de WinPE (consulte Importar archivos de arranque).

En la pestaña **Gestionar imágenes de SO**, puede filtrar la lista de imágenes de SO haciendo clic en **Mostrar todo → Estado del despliegue**. Puede filtrar la lista para mostrar solo los servidores que tienen un estado de “Preparado,” “No preparado” y “Advertencia”. Tenga en cuenta que si el estado de despliegue de una imagen del sistema operativo es “No preparado”, el sistema operativo no se incluye en la lista de los sistemas operativos desplegables.

De forma predeterminada, se admite la configuración regional en inglés. Para especificar la configuración regional a un idioma específico, debe utilizar un archivo de configuración personalizada y un archivo de instalación desatendida. Para obtener más información, consulte Despliegue de SLES 12 SP3 con una configuración regional configurable y servidores NTP, Despliegue de Windows 2016 en japonés.

El despliegue del sistema operativo en almacenamientos conectados diferentes de RAID no es compatible.

Atención: Si el servidor tiene instalado actualmente un sistema operativo, al desplegar la imagen se sobrescribirá el sistema operativo actual.

Para los servidores con XCC2 que tienen habilitada la función de protección del sistema y la acción establecida en **Evitar el arranque del SO**, asegúrese de que la función de protección del sistema sea conforme con el dispositivo. Si la función de protección del sistema es no conforme, los dispositivos no pueden completar el proceso de arranque, lo que provoca que el despliegue del SO falle. Para aprovisionar estos dispositivos, responda manualmente el mensaje de arranque de la función de protección del sistema para permitir que los dispositivos arranquen con normalidad.

Procedimiento

Para desplegar la imagen de un sistema operativo en uno o varios servidores gestionados, lleve a cabo los pasos siguientes.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Desplegar imágenes de SO** para mostrar la página Desplegar sistema operativo: Desplegar imágenes de SO.

Consejo: para complejos escalables, el sistema operativo se despliega en la partición principal; por lo tanto, solo la partición principal está incluida en la lista de servidores.

Paso 2. Seleccione uno o varios servidores en los que desee desplegar el sistema operativo. Puede desplegar un sistema operativo en hasta 28 servidores al mismo tiempo.

Puede ordenar las columnas de la tabla para que sea más fácil encontrar servidores específicos. Además, puede filtrar la lista de dispositivos mostrados al seleccionar una opción en el menú

Mostrar, de modo que se muestren solo los dispositivos en un chasis, bastidor o grupo específico, o al ingresar texto (como un nombre o dirección IP) en el campo **Filtro**.

Consejo: puede elegir varios nodos de cálculo de varios chasis si piensa desplegar el mismo sistema operativo en todos los nodos de cálculo.

Paso 3. Haga clic en **Cambiar selección → Valores de red** para configurar los valores de red.

Para obtener más información, consulte el apartado Configuración de los valores de red para servidores gestionados.

Paso 4. Para cada servidor, seleccione el perfil de imagen del sistema operativo que se desplegará de la lista desplegable en la columna **Imagen para desplegar**.

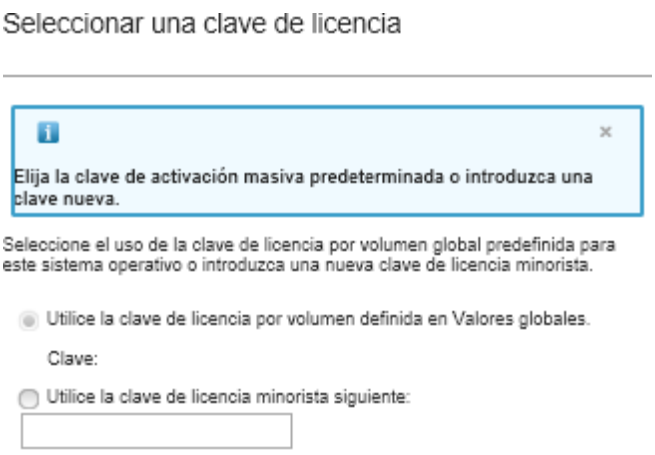
Asegúrese de seleccionar un perfil de imagen de SO compatible con el servidor seleccionado. Puede determinar la compatibilidad a partir de los atributos de perfil que se enumeran en la columna **Atributo** de la página Gestionar imágenes de SO. Para obtener información sobre atributos de perfil, consulte Perfiles de las imágenes del sistema operativo.

Paso 5. Para cada servidor, haga clic en el icono **Clave de licencia** ( ) y especifique la clave de licencia que se va a utilizar para activar el sistema operativo una vez instalado.

XClarity Administrator permite utilizar claves de licencia por volumen predeterminadas para las instalaciones de Windows, así como claves minoristas individuales, tanto para Windows como para VMware ESXi.

Para utilizar la clave de licencia por volumen global que ha especificado en el cuadro de diálogo Valores globales, seleccione **Utilizar la clave de licencia por volumen definida en Valores globales**. Para obtener más información sobre las claves de licencia por volumen global, consulte Configuración de valores globales de despliegue del SO.

Para utilizar una clave de licencia minorista individual, seleccione **Utilice la clave de licencia minorista siguiente** y, a continuación, introduzca la clave en el campo siguiente.



Paso 6. **Opcional:** si ha seleccionado un sistema operativo Windows para un servidor, puede unir el sistema operativo Windows a un dominio de Active Directory como parte del despliegue del sistema operativo haciendo clic en el icono **Carpeta** ( ) que aparece junto a la imagen del sistema operativo y seleccionando a continuación el nombre Active Directory.

Para utilizar Active Directory predeterminado que ha especificado en el cuadro de diálogo Valores globales, seleccione **Utilizar Active Directory definido en Valores globales**. Para obtener más información sobre cómo unir un dominio de Active Directory, consulte Integración con Windows Active Directory.

Para utilizar Active Directory individual, seleccione **Utilizar el siguiente Active Directory** y el dominio de Active Directory.

Paso 7. Para cada servidor, en la columna **Almacenamiento** seleccione la ubicación de almacenamiento preferida donde desee desplegar la imagen del sistema operativo.
- **Unidad de disco local**
- **Hipervisor integrado**
- **Unidad M.2**
- **Almacenamiento SAN**

Si la ubicación de almacenamiento seleccionada no es compatible con el servidor, XClarity Administrator intenta desplegar el sistema operativo en la ubicación de almacenamiento que siga en el orden de prioridad.

Nota: Solo para servidores ThinkServer, **Disco local** está disponible

Para obtener más información acerca de cómo configurar la ubicación de almacenamiento, consulte Elegir la ubicación de almacenamiento de los servidores gestionados.

Nota: Para asegurarse de que los despliegues del sistema operativo sean correctos, desconecte todos los sistemas de almacenamiento del servidor gestionado, a excepción del que haya elegido para el despliegue del sistema operativo.

Paso 8. Compruebe que el estado de despliegue de todos los servidores seleccionados sea Preparado.

Importante: asegúrese de que el estado de despliegue de todos los servidores seleccionados sea Preparado. Si el estado de un servidor es No preparado, no puede desplegar la imagen de un sistema operativo en ese servidor. Haga clic en el vínculo **No preparado** para obtener información sobre cómo resolver el problema. Si los valores de red no son válidos, haga clic en **Cambiar selección → Valores de red** para configurar los valores de red.

Paso 9. Haga clic en el icono **Desplegar imágenes** ( ) para iniciar el despliegue del sistema operativo.

Si se han añadido valores de configuración personalizada en el perfil de imagen del SO, la pestaña **Configuración personalizada** se abre la pestaña en el cuadro de diálogo Desplegar imagen del SO. Especifique una configuración personalizada, los valores comunes de servidor y la configuración específica del servidor y, a continuación, haga clic en **Siguiente** para continuar con el despliegue del SO. Tenga en cuenta que l despliegue del SO no se llevará a cabo si en la entrada no se especifica ningún valor de configuración personalizada necesaria.

Después de finalizar

Puede supervisar el estado del proceso de despliegue desde el registro de trabajos. En la barra de menús de XClarity Administrator, haga clic en **Supervisión → Trabajos**. Para obtener más información sobre el registro de trabajos, consulte Supervisión de trabajos.

También puede definir una sesión de control remoto mediante el controlador de gestión de la placa base del servidor para ver cómo va progresando la instalación. Para obtener más información sobre el control remoto, consulte Utilizar un control remoto para gestionar servidores convergidos, Flex System, NeXtScale y System x.

Se guarda la información de despliegue del sistema operativo. Puede ver la información de despliegue haciendo clic en **Aprovisionamiento → Gestionar acceso de SO** y luego colocando el cursor sobre el nombre del servidor.

Integración con Windows Active Directory

Cuando se despliega una imagen de Windows mediante Lenovo XClarity Administrator, es posible unir un dominio de Active Directory como parte del despliegue del sistema operativo.

Antes de empezar

Para unir un dominio de Active Directory durante el despliegue de una imagen de Windows, es preciso configurar tanto el servidor de gestión como el servidor de Windows Server que está ejecutando el controlador de dominio de Active Directory afectado. Para realizar esta configuración, debe contar con los requisitos de acceso siguientes:

- Una cuenta de administrador con autoridad para autenticar y unir el dominio de servidores de Active Directory. Esta cuenta debe poseer privilegios semejantes a los del grupo de administradores de dominio predeterminado y puede usar una cuenta de este grupo para efectuar la citada configuración.
- Acceso a un sistema de nombres de dominio (DNS, Domain Name Server) que se resuelva en el servidor de Active Directory que está ejecutando el controlador de dominio. Este DNS debe especificarse en la opción **Valores de red → DNS** del servidor en el que vaya a desplegar el sistema operativo.
- El administrador del servidor de Active Directory debe crear el nombre del equipo requerido en el servidor de dominio antes de desplegar el sistema operativo. El intento de unión no crea el nombre del equipo. Si no se especifica ningún nombre, la unión produce un error.
- El administrador del servidor de Active Directory debe utilizar el campo **Valores de red → Nombre de host** para especificar el nombre de host del servidor en el que va a desplegarse la imagen. Dicho nombre debe ser un nombre de equipo perteneciente a la unidad organizativa de destino.

  El nombre de host (nombre del equipo) debe ser exclusivo. Si se especifica un nombre que ya está en uso en otra instalación de Windows, la unión no se completará.

Puede unirse el dominio de Active Directory utilizando uno de los métodos siguientes:

- **Utilice un dominio de Active Directory**

Puede elegir utilizar un dominio de Active Directory específico de una lista de dominios predefinidos. Lleve a cabo los siguientes pasos para definir un dominio de Active Directory en XClarity Administrator. Si tiene pensado utilizar varios dominios, repita este paso para cada nombre de dominio.

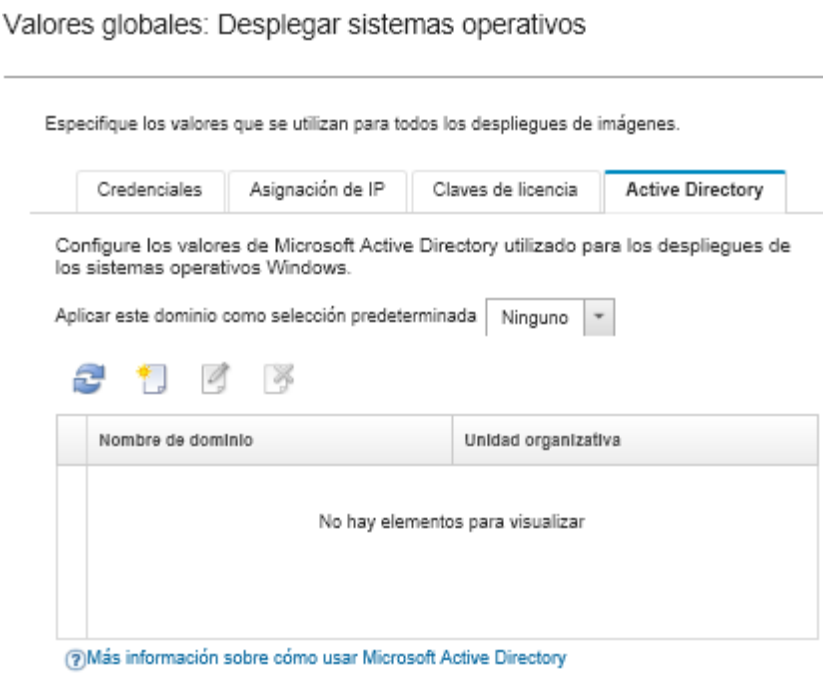
1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Desplegar imágenes de SO** para mostrar la página Desplegar imágenes de SO.
2. Haga clic en el icono **Valores globales** ( ) para mostrar el cuadro de diálogo Valores globales: Desplegar sistemas operativos.
3. Haga clic en la pestaña **Active Directory**.
4. Haga clic en el icono **Crear** ( ) para abrir el cuadro de diálogo Añadir dominio de Active Directory nuevo.
5. Especifique el nombre de dominio y la unidad de la organización.

   El despliegue del sistema operativo admite tanto la unión de un dominio como la creación en el seno de este último de unidades organizativas anidadas. Si está especificando unidades organizativas, no es necesario especificar explícitamente la OU durante la unión. Active Directory puede deducir cuál es la OU correcta a partir del nombre de dominio y del nombre del sistema.
6. Haga clic en **Aceptar**.

- **Utilice el dominio de Active Directory predeterminado**

  Puede elegir utilizar el dominio de Active Directory predeterminado que se define en valores globales. Lleve a cabo los siguientes pasos para establecer el dominio de Active Directory predeterminado en XClarity Administrator.

  1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Desplegar imágenes de SO** para mostrar la página Desplegar imágenes de SO.
  2. Haga clic en el icono **Valores globales** ( ) para mostrar el cuadro de diálogo Valores globales: Desplegar sistemas operativos.
  3. Haga clic en la pestaña **Active Directory**.



4. En el menú desplegable **Aplicar este dominio como selección predeterminada**, seleccione el dominio de Active Directory que se va a utilizar de forma predeterminada para cada despliegue de Windows.
5. Haga clic en **Aceptar**.

- **Utilice datos blob de metadatos**

  Puede utilizar metadatos de la cuenta de equipo de Active Directory (en formato blob codificado con Base64) para unirse al dominio de Active Directory para cualquier servidor. Lleve a cabo los pasos siguientes para generar datos blob de metadatos.

  1. Utilice una cuenta de administrador para iniciar sesión en el equipo. El equipo debe ser parte del dominio de Active Directory al que se está uniendo.
  2. Haga clic en **Inicio → Programas → Accesorios**. Haga clic en **Indicador de comando** y luego **Ejecutar como administrador**.
  3. Vaya al directorio C:\windows\system32.
  4. Ejecute el comando `djoin` utilizando el siguiente formato para realizar una unión de dominio fuera de línea:
     `djoin /provision /domain <AD_domain_name> /machine <hostname> /savefile blob`

     donde:

     – *<AD_domain_name>* es el nombre del dominio de Active Directory.
     – *<hostname>* es el nombre de host del servidor en el que va a desplegarse la imagen como un nombre de un perteneciente a la unidad organizativa de destino pulsando el campo **Valores de red → Nombre de host**.

     Este comando crea un archivo denominado `blob` que contiene los datos blob de metadatos. El proceso de despliegue del sistema operativo utiliza el contenido de este archivo para especificar los detalles de unión a Active Directory, así que mantenga estos datos al alcance.

     Los datos blob de metadatos son de tipo confidencial.

Para obtener información detallada sobre cómo desplegar la imagen de un sistema operativo, consulte Despliegue de la imagen de un sistema operativo.

Procedimiento

Lleve a cabo estos pasos para unir un dominio de Active Directory.

Paso 1. Importe la imagen del sistema operativo Windows al Repositorio de imágenes del SO (consulte Importación de imágenes del sistema operativo).

Paso 2. Seleccione uno o varios servidores en los que desee desplegar el sistema operativo. Puede desplegar un sistema operativo en hasta 28 servidores al mismo tiempo.

Consejo: puede elegir varios nodos de cálculo de varios chasis si piensa desplegar el mismo sistema operativo en todos los nodos de cálculo.

Paso 3. Haga clic en **Cambiar selección → Valores de red** para configurar los valores de red.

a. Haga clic en **Cambiar todas las filas → Sistema de nombres de dominio (DNS)** y especifique como mínimo un DNS que se resuelva en el dominio de Active Directory.

b. Para cada servidor, especifique un nombre de host que coincida con el nombre de un equipo existente en el dominio y la unidad organizativa que está uniendo.

Para obtener más información sobre cómo configurar valores de red, consulte Configuración de los valores de red para servidores gestionados.

Paso 4. Para cada servidor, seleccione la imagen del sistema operativo Windows que se desplegará en la columna **Imagen para desplegar**. Junto al nombre de la imagen se muestran los iconos de la carpeta y de la clave de licencia.

Paso 5. Para cada servidor, haga clic en el icono **Clave de licencia** ( ) y especifique la clave de licencia que se va a utilizar para activar el sistema operativo una vez instalado:

Paso 6. Para cada servidor, haga clic en el icono **Carpeta** ( ) y especifique el dominio de Active Directory. Puede elegir uno de los valores siguientes:

- **Utilice Active Directory definido en Valores globales** para utilizar el dominio predeterminado.
- **Utilice el siguiente Active Directory** para seleccionar un dominio específico.
- **Utilice datos de bloque de metadatos** para especificar los contenidos del archivo blob.

  Los datos blob de metadatos contienen información confidencial que no se muestra en el campo. Esta información solo está disponible hasta que se completa la operación de implementación. No es persistente.

Paso 7. Para cada servidor, en la columna **Almacenamiento** seleccione la ubicación de almacenamiento preferida donde desee desplegar la imagen del sistema operativo.

- **Unidad de disco local**
- **Hipervisor integrado**
- **Unidad M.2**
- **Almacenamiento SAN**

Si la ubicación de almacenamiento seleccionada no es compatible con el servidor, XClarity Administrator intenta desplegar el sistema operativo en la ubicación de almacenamiento que siga en el orden de prioridad.

Para obtener más información acerca de cómo configurar la ubicación de almacenamiento, consulte Elegir la ubicación de almacenamiento de los servidores gestionados.

Nota: Para asegurarse de que los despliegues del sistema operativo sean correctos, desconecte todos los sistemas de almacenamiento del servidor gestionado, a excepción del que haya elegido para el despliegue del sistema operativo.

Paso 8. Compruebe que el estado de despliegue de todos los servidores seleccionados sea Preparado.

Si el estado de un servidor es No preparado, no puede desplegar la imagen de un sistema operativo en ese servidor. Haga clic en el vínculo **No preparado** para obtener información sobre cómo resolver el problema. Si los valores de red no son válidos, haga clic en **Cambiar selección → Valores de red** para configurar los valores de red.

Paso 9. Haga clic en el icono **Desplegar imágenes** () para iniciar el despliegue del sistema operativo.

En el cuadro de diálogo Confirmación de despliegue se le piden las credenciales que deben usarse para autenticarse en el servidor de Active Directory y unir el dominio. Por motivos de seguridad, estas credenciales no se almacenan en XClarity Administrator. Debe indicar las credenciales para cada despliegue de Windows que se una al dominio.

Puede supervisar el estado del proceso de despliegue desde el registro de trabajos. En la barra de menús de XClarity Administrator, haga clic en **Supervisión → Trabajos**. Para obtener más información sobre el registro de trabajos, consulte Supervisión de trabajos.

Resultados

Una vez completado el despliegue del sistema operativo, abra un navegador web en la dirección IP que ha especificado en la página Editar valores de red y, a continuación, inicie sesión para continuar con el proceso de configuración.

Escenarios de despliegue del SO

Utilice los escenarios para ayudarle a personalizar y desplegar sistemas operativos en sus servidores gestionados.

Despliegue de RHEL con controladores personalizados de dispositivo

En este escenario se instala el sistema operativo Red Hat Enterprise Linux (RHEL) y los controladores de dispositivos adicionales que no están disponibles en el sistema operativo base. Se utiliza un perfil personalizado que incluye los controladores de dispositivos adicionales. Después de esto, el perfil personalizado se puede seleccionar en la página Desplegar imágenes de SO.

Antes de empezar

Al desplegar sistemas operativos usando Lenovo XClarity Administrator, el sistema operativo puede incluir el Ethernet, Fibre Channel y los controladores de dispositivo del adaptador de almacenamiento adecuados para su hardware. Si un controlador de dispositivo no está incluido en el sistema operativo, el adaptador no es compatible con el despliegue del SO. En XClarity Administrator versión 1.2.0 y posteriores, se puede personalizar un sistema operativo agregando controladores de dispositivos.

Puede obtener controladores de dispositivos desde Página web del repositorio de Lenovo YUM, desde un proveedor (como Red Hat) o mediante un controlador de dispositivo personalizado que generó por su cuenta. Para algunos controladores de dispositivos de Windows, puede generar un controlador de dispositivo personalizado al extraer el controlador de dispositivo del exe de instalación a su sistema local y crear un archivo .zip.

Nota: Los controladores de dispositivo RHEL deben estar en formato de imagen .iso o .rpm.

Procedimiento

Para desplegar RHEL con controladores de dispositivo personalizados, lleve a cabo los pasos siguientes.

Paso 1. Descargue el sistema operativo RHEL base desde el sitio web de Red Hat en el sistema local e importe la imagen en el repositorio de imágenes del SO. Para obtener más información, consulte Importación de imágenes del sistema operativo.

1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Gestionar imágenes de SO** para mostrar la página Desplegar sistema operativo: Gestionar imágenes de SO.
2. Haga clic en la pestaña **Imágenes del SO**.
3. Haga clic en el icono **Importar** ( ).
4. Haga clic en **Importación local**.
5. Haga clic en **Examinar** para buscar y seleccionar la imagen de RHEL que se importará (por ejemplo, `RHEL-<ver>-<date>-Server-x86_64-dvd1.iso`).
6. Haga clic en **Importar** para cargar la imagen al repositorio de imágenes de SO.
7. Espere a que se complete la importación. Esto puede tardar varios minutos.

Paso 2. Descargue los controladores de controladores personalizados al sistema local e importe los archivos al repositorio de imágenes del SO. Para obtener más información, consulte Importación de controladores de dispositivos.

1. Pulse la pestaña **Controladores de dispositivo**
2. Haga clic en el icono **Importar** ( ).
3. Haga clic en **Importación local**.
4. Seleccione `RHEL` para el sistema operativo.
5. Seleccione la versión del sistema operativo.
6. Seleccione el tipo de dispositivo.
7. Haga clic en **Examinar** para buscar y seleccionar el controlador de dispositivo que desea importar (por ejemplo, `kmod-i40e-2.0.12-1.el7.x86_64.rpm`).
8. Haga clic en **Importar** para cargar el archivo al repositorio de imágenes de SO.

Paso 3. Cree un perfil de imagen del SO personalizado que incluya los controladores de dispositivo personalizados. Para obtener más información, consulte Creación de un perfil de imagen de SO personalizado.

1. Haga clic en la pestaña **Imágenes del SO**.
2. Seleccione un perfil de imagen de SO a personalizar (por ejemplo, `Virtualization`).
3. Haga clic en el icono **Crear** ( ) para abrir el cuadro de diálogo Crear perfil personalizado.
4. En la pestaña **General**:
   a. Introduzca un nombre para el perfil (por ejemplo: `RHEL personalizado con controladores de dispositivo`).
   b. Utilice el valor predeterminado para el campo **Datos personalizados y ruta de archivo**.

c. Seleccione **Ninguno** para el tipo de personalización.
d. Haga clic en **Siguiente**.

5. En la pestaña **Opciones de controlador**, seleccione los controladores de dispositivo personalizados que se incluyen en el perfil y haga clic en **Siguiente**. De forma predeterminada, se incluyen los controladores de dispositivo de entrada.
6. En la pestaña **Software**, haga clic en **Siguiente**.
7. Haga clic en **Personalizar** para crear el perfil de imagen del SO personalizado.

Paso 4. Despliegue el perfil de imagen de SO personalizado en los servidores de destino. Para obtener más información, consulte Despliegue de la imagen de un sistema operativo.

1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Desplegar imágenes de SO** para mostrar la página Desplegar sistema operativo: Desplegar imágenes de SO.
2. En cada servidor de destino:
   a. Seleccione el servidor.
   b. Haga clic en **Cambiar selección → Valores de red** y especifique el nombre de host, la dirección IP y los valores de DNS, MTU y VLAN del servidor.

      Consejo: los valores VLAN están disponibles únicamente cuando se establece el modo VLAN en **Valores globales → Asignación de IP → Usar VLAN**.
   c. Seleccione el perfil de imagen de SO personalizado (por ejemplo, <*base_OS*>|<*timestamp*>_RHEL personalizado con controladores de dispositivo) de la lista desplegable en la columna **Imagen para desplegar**.

      Nota: Asegúrese de que todos los servidores de destino utilicen el mismo perfil personalizado.
   d. (Opcional) Haga clic en el icono **Clave de licencia** () y especifique la clave de licencia que se va a utilizar para activar el sistema operativo una vez instalado.
   e. Seleccione la ubicación de almacenamiento preferida donde desee desplegar la imagen del sistema operativo desde la columna **Almacenamiento**.

      Nota: Para asegurarse de que los despliegues del sistema operativo sean correctos, desconecte todos los sistemas de almacenamiento del servidor gestionado, a excepción del que haya elegido para el despliegue del sistema operativo.
   f. Compruebe que el estado de despliegue del servidor seleccionado sea **Preparado**.
3. Seleccione todos los servidores de destino y haga clic en el icono **Desplegar imagen** () para iniciar el despliegue del sistema operativo.
4. En la pestaña **Resumen**, revise los valores.
5. Haga clic en **Desplegar** para desplegar el sistema operativo.

Despliegue de RHEL y una aplicación Hello World PHP utilizando un archivo de instalación desatendida

En este caso, se instala el sistema operativo RHEL junto con el software personalizado (Apache HTTP, PHP y una aplicación hello-world PHP). Se utiliza un perfil de imagen de SO personalizada que incluye una instalación desatendida que registra el sistema operativo con la suscripción Lenovo RHEL interno de servicio para que pueda usar los repositorios yum, instala los paquetes de Apache y PHP, configura el firewall para permitir conexiones de Apache, crea una aplicación Hello World PHP y la copia al directorio del servidor de web de Apache y configura los archivos de configuración de Apache para admitir PHP.

Antes de empezar

Puede desplegar RHEL con software personalizado en varias formas diferentes. Este ejemplo utiliza un archivo de instalación desatendida personalizado que se incluye en el perfil de imagen del SO personalizado. También puede utilizar un script posterior a la instalación que instala un software personalizado que se importa en el repositorio y que incluye el perfil de imagen del SO personalizado. Para instalar el software utilizando un script posterior a la instalación, consulte Implementación de RHEL y una aplicación Hello World PHP mediante software personalizado y un script posterior a la instalación.

Este escenario utiliza el siguiente archivo de muestra.

- RHEL_installSoftware_customUnattend.cfg Este archivo desatendido personalizado utiliza los valores de macros predefinidos o personalizados instala y configura el software personalizado.

Procedimiento

Para desplegar RHEL con software personalizado utilizando un archivo de instalación desatendida personalizado, lleve a cabo los siguientes pasos.

Paso 1. Descargue el sistema operativo RHEL base desde el sitio web de Red Hat en el sistema local e importe la imagen en el repositorio de imágenes del SO. Para obtener más información, consulte Importación de imágenes del sistema operativo.

1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Gestionar imágenes de SO** para mostrar la página Desplegar sistema operativo: Gestionar imágenes de SO.
2. Haga clic en la pestaña **Imágenes del SO**.
3. Haga clic en el icono **Importar** ().
4. Haga clic en **Importación local**.
5. Haga clic en **Examinar** para buscar y seleccionar la imagen de RHEL que se importará (por ejemplo, `RHEL-<ver>-<date>-Server-x86_64-dvd1.iso`).
6. Haga clic en **Importar** para cargar la imagen al repositorio de imágenes de SO.
7. Espere a que se complete la importación. Esto puede tardar varios minutos.

Paso 2. Modifique el archivo RHEL de instalación desatendida (comenzar) para registrar el sistema operativo con el servicio de suscripción satélite de RHEL, instale los paquetes HTTP (Apache) y PHP y cree una aplicación Hello World PHP simple, agregue las macros predefinidas requeridas y otras macros predefinidas según corresponda, como la dirección IP, la puerta de enlace, el DNS y los valores de nombre de host y luego importe el archivo personalizado en el repositorio de imágenes del SO. Para obtener más información, consulte Importación de archivos de instalación desatendida personalizados.

Añada comandos para registrar el host con su satélite RHEL, por ejemplo:

```
rpm -Uvh http://<YOUR_SATELLITE_SERVER_IP>/pub/katello-ca-consumer-latest.noarch.rpm
subscription-manager register --org="<YOUR_ORGANIZATION>" --activationkey="RHEL_Base" --force
subscription-manager repos --enable rhel-7-server-rpms
```

Importante: En el archivo de instalación desatendida de ejemplo, especifique la dirección IP del servidor satélite y su organización, según la configuración de suscripción de servicio.

Agregue los comandos para actualizar el host y para instalar y configurar los paquetes apache y php, por ejemplo:

```
%packages
@base
@core
@fonts
@gnome-desktop
@internet-browser
```

```
@multimedia
@x11
@print-client
-gnome-initial-setup

#Add the Apache and PHP packages
httpd
mod_ssl
openssl
php
php-mysql
php-gd
%end

yum -y update

systemctl enable httpd.service

firewall-cmd --permanent --zone=public --add-service=http
firewall-cmd --permanent --zone=public --add-service=https
firewall-cmd --reload

echo "<?PHP
echo 'Hello World !! ';
?>" | tee /var/www/html/index.php

sudo cp /etc/httpd/conf/httpd.conf /etc/httpd/conf/httpd.conf.original

sudo sed -i -e 's/^[ \t]*//' /etc/httpd/conf/httpd.conf
sudo sed -i "s|IncludeOptional|#IncludeOptional|" /etc/httpd/conf/httpd.conf
sudo sed -i "s|#ServerName www.example.com:80|ServerName localhost|" /etc/httpd/conf/httpd.conf
sudo sed -i "s|DirectoryIndex index.html|DirectoryIndex index.html index.php|" /etc/httpd/conf/httpd.conf

echo "AddType application/x-httpd-php .php" | tee -a /etc/httpd/conf/httpd.conf
```

Nota: El archivo de instalación desatendida modifica los paquetes predeterminado que se están instalando con el archivo de comienzo. Especifica los paquetes Apache y PHO como parte de la sección %packages.

Solo para ESXi y RHEL, XClarity Administrator proporciona el macro **#predefined.unattendSettings.networkConfig#**, que añade a todos los valores que se definen en la interfaz de usuario del archivo de instalación desatendida y el macro **# predefined.unattendSettings.storageConfig#**, que añade todos los valores de almacenamiento que se definen en la interfaz de usuario en el archivo de instalación desatendida. El archivo de instalación desatendida de ejemplo ya contiene estas macros.

XClarity Administrator también ofrece algunas macros prácticas de nivel básico, como la inserción de controladores OOB, informes de estado, scripts posteriores a la instalación, software personalizado. Sin embargo, para aprovechar estas macros predefinidas, debe especificar las siguientes macros en el archivo desatendido personalizado. El archivo de ejemplo ya contiene las macros necesarias.

```
#predefined.unattendSettings.preinstallConfig#
#predefined.unattendSettings.postinstallConfig#
```

El archivo de muestra ya contiene las macros necesarias y las macros predefinidas adicionales para especificar dinámicamente los valores de red para el servidor y la zona horaria de destino. Para obtener más información acerca de cómo agregar macros a archivos de instalación desatendida, consulte Inyección de macros predefinidas y personalizadas a un archivo de instalación desatendida.

También puede agregar comandos para enviar mensajes personalizados al registro de trabajos en XClarity Administrator. Para obtener más información, consulte el apartado Agregar informes de estado personalizados a los scripts de instalación.

Para importar el script de instalación personalizado, lleve a cabo estos pasos. Para obtener más información, consulte el apartado Importación de scripts de instalación personalizada.

Para importar el archivo de instalación personalizada y desatendida, lleve a cabo estos pasos.

1. Haga clic en la pestaña **Archivos de instalación desatendida**.
2. Haga clic en el icono **Importar** ().
3. Haga clic en **Importación local**.
4. Seleccione `RHEL` para el sistema operativo.
5. Haga clic en **Examinar** para buscar y seleccionar el software a importar (por ejemplo, `RHEL_installSoftware_customUnattend.cfg`).
6. Haga clic en **Importar** para cargar el archivo al repositorio de imágenes de SO.

Paso 3. Cree un perfil de imagen de SO personalizado que incluya los valores de configuración de software y scripts posterior a la instalación. Para obtener más información, consulte Creación de un perfil de imagen de SO personalizado.

1. Haga clic en la pestaña **Imágenes del SO**.
2. Seleccione un perfil de imagen de SO a personalizar (por ejemplo, `Basic`).
3. Haga clic en el icono **Crear** () para abrir el cuadro de diálogo Crear perfil personalizado.
4. En la pestaña **General**:
   a. Introduzca un nombre para el perfil (por ejemplo: `Custom RHEL with software using custom unattend`).
   b. Utilice el valor predeterminado para el campo **Datos personalizados y ruta de archivo**.
   c. Seleccione **Solo archivos de instalación desatendida** en el tipo de personalización.
   d. Haga clic en **Siguiente**.
5. En la pestaña **Opciones de controlador**, haga clic en **Siguiente**. De forma predeterminada, se incluyen los controladores de dispositivo de entrada.
6. En la pestaña **Software**, haga clic en **Siguiente**.
7. En la pestaña **Archivos de instalación desatendida**, seleccione el archivo de instalación desatendida personalizado (por ejemplo, `RHEL_installSoftware_customUnattend.cfg`) y haga clic en **Siguiente**.
8. En la pestaña **Scripts de instalación**, haga clic en **Siguiente**.
9. En la pestaña **Resumen**, revise los valores.
10. Haga clic en **Personalizar** para crear el perfil de imagen del SO personalizado.

Paso 4. Despliegue el perfil de imagen de SO personalizado en los servidores de destino. Para obtener más información, consulte Despliegue de la imagen de un sistema operativo.

1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Desplegar imágenes de SO** para mostrar la página Desplegar sistema operativo: Desplegar imágenes de SO.
2. En cada servidor de destino:
   a. Seleccione el servidor.
   b. Haga clic en **Cambiar selección → Valores de red** y especifique el nombre de host, la dirección IP y los valores de DNS, MTU y VLAN del servidor.

Consejo:

- Los valores VLAN están disponibles únicamente cuando el modo VLAN se establece en **Valores globales → Asignación de IP → Usar VLAN**.
- Los valores de red que especifique en el cuadro de diálogo Valores de red se agregan al archivo desatendido en el tiempo de ejecución usando la macro **#predefined. hostPlatforms.networkSettings.<*setting*>#**.

c. Seleccione el perfil de imagen de SO personalizado (por ejemplo, <*base_OS*>| <*timestamp*>_RHEL personalizado con software utilizando un archivo de instalación desatendida personalizado) de la lista desplegable en la columna **Imagen para desplegar**.

Nota: Asegúrese de que todos los servidores de destino utilicen el mismo perfil personalizado.

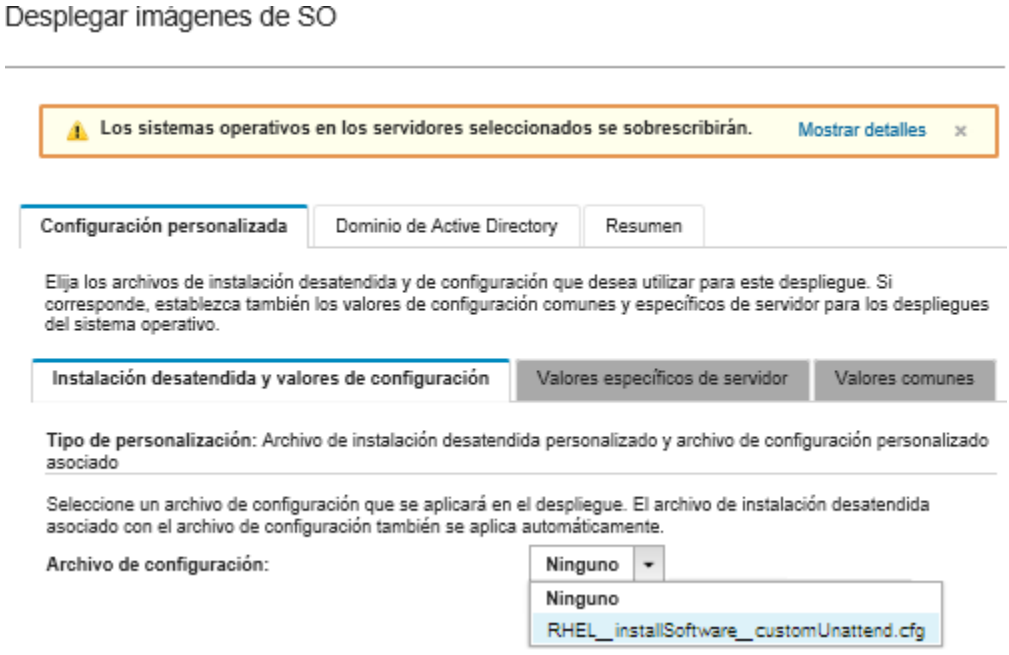
d. (Opcional) Haga clic en el icono **Clave de licencia** ( ) y especifique la clave de licencia que se va a utilizar para activar el sistema operativo una vez instalado.

e. Seleccione la ubicación de almacenamiento preferida donde desee desplegar la imagen del sistema operativo desde la columna **Almacenamiento**.

Nota: Para asegurarse de que los despliegues del sistema operativo sean correctos, desconecte todos los sistemas de almacenamiento del servidor gestionado, a excepción del que haya elegido para el despliegue del sistema operativo.

f. Compruebe que el estado de despliegue del servidor seleccionado sea **Preparado**.

3. Seleccione todos los servidores de destino y haga clic en el icono **Desplegar imagen** ( ) para iniciar el despliegue del sistema operativo.
4. En la pestaña Configuración personalizada, haga clic en la subpestaña **Valores de instalación desatendida** y de configuración y seleccione el archivo de instalación desatendida personalizada (por ejemplo, RHEL_installSoftware_customUnattend.cfg).



5. En la pestaña **Resumen**, revise los valores.
6. Haga clic en **Desplegar** para desplegar el sistema operativo.

Implementación de RHEL y una aplicación Hello World PHP mediante software personalizado y un script posterior a la instalación

En este caso, se instala el sistema operativo RHEL junto con el software personalizado (Apache HTTP, PHP y una aplicación hello-world PHP). Se utiliza un perfil de imagen de SO personalizada que incluye un software personalizado y un script posterior a la instalación que registra el sistema operativo con la suscripción Lenovo RHEL interno de servicio para que pueda usar los repositorios yum, instala los paquetes de Apache y PHP, configura el firewall para permitir conexiones de Apache, crea una aplicación Hello World PHP y la copia al directorio del servidor de web de Apache y configura los archivos de configuración de Apache para admitir PHP. Los paquetes de software personalizado se exportan al host durante el despliegue y se disponen para usarlos en el script posterior a la instalación.

Antes de empezar

Puede desplegar RHEL y una aplicación Hello World PHP en varias formas diferentes. Este ejemplo utiliza un script posterior a la instalación que instala un software personalizado que se importa en el repositorio y que incluye el perfil de imagen del SO personalizado. También puede usar un archivo de instalación atendida personalizado que se incluye en el perfil de imagen del SO personalizado. Para instalar el software utilizando un archivo de instalación atendida personalizada, consulte Despliegue de RHEL y una aplicación Hello World PHP utilizando un archivo de instalación desatendida.

Este escenario utiliza los siguientes archivos de muestra.

- httpd.conf. Este es el archivo de instalación de Apache HTTP.
- hello_world.php Esta es la aplicación Hello World PHP.
- RHEL_installSoftware_customScript.sh Este script posterior a la instalación instala y configura el software personalizado.

Notas:

- Los scripts de instalación de RHEL pueden estar en uno de los siguientes formatos: Bash (.sh), Perl (.pm o .pl), Python (.py)
- Los archivos de software y scripts de instalación se instalan en la ruta de datos y archivos personalizada que especifica durante el despliegue. La ruta de datos y archivos personalizados predeterminada es `/home/lxca`.

Procedimiento

Para desplegar RHEL con software personalizado utilizando un script posterior a la instalación lleve a cabo los siguientes pasos.

Paso 1. Descargue el sistema operativo RHEL base desde el sitio web de Red Hat en el sistema local e importe la imagen en el repositorio de imágenes del SO. Para obtener más información, consulte Importación de imágenes del sistema operativo.

1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Gestionar imágenes de SO** para mostrar la página Desplegar sistema operativo: Gestionar imágenes de SO.
2. Haga clic en la pestaña **Imágenes del SO**.
3. Haga clic en el icono **Importar** ().
4. Haga clic en **Importación local**.
5. Haga clic en **Examinar** para buscar y seleccionar la imagen de RHEL que se importará (por ejemplo, `RHEL-<ver>-<date>-Server-x86_64-dvd1.iso`).
6. Haga clic en **Importar** para cargar la imagen al repositorio de imágenes de SO.
7. Espere a que se complete la importación. Esto puede tardar varios minutos.

Paso 2. Descargue el software personalizado en el sistema local e importe los archivos al repositorio de imágenes del SO. Para obtener más información, consulte Importación de software personalizado.

Consejo: para importar un software personalizado a XClarity Administrator, los archivos deben estar contenidos en un archivo tar.gz. En este ejemplo, comprima los archivos de software `httpd.conf` e `index.php` en un archivo tar.gz denominado `RHEL_installSoftware_customsw.tar.gz` antes de continuar

1. Haga clic en la pestaña **Software**.
2. Haga clic en el icono **Importar** ().
3. Haga clic en **Importación local**.
4. Seleccione `RHEL` para el sistema operativo.
5. Haga clic en **Examinar** para buscar y seleccionar el software a importar (por ejemplo, `RHEL_installSoftware_customsw.tar.gz`).
6. Haga clic en **Importar** para cargar el archivo al repositorio de imágenes de SO.

Paso 3. Cree un código posterior a la instalación personalizado e importe el archivo al repositorio de imágenes del SO.

Añada comandos para registrar el host con el satélite RHEL, por ejemplo:

```
rpm -Uvh http://satellite.labs.lenovo.com/pub/katello-ca-consumer-latest.noarch.rpm
subscription-manager register --org="Default_Organization" --activationkey="RHEL_Base" --force
subscription-manager repos --enable rhel-7-server-rpms A
```

Añada un comando para actualizar el host y para instalar y configurar los paquetes apache y php, por ejemplo:

```
yum -y update
yum -y install httpd mod_ssl openssl php php-mysql php-gd

systemctl enable httpd.service

firewall-cmd --permanent --zone=public --add-service=http
firewall-cmd --permanent --zone=public --add-service=https
firewall-cmd --reload
```

Agregue los comandos para añadir nuestra aplicación PHP al serversatellite web, por ejemplo:

```
cp #predefined.otherSettings.deployDataAndSoftwareLocation#/lxca/index.php /var/www/html/index.php
```

Añada los comandos para configurar Apache HTTP, por ejemplo:

```
cp /etc/httpd/conf/httpd.conf /etc/httpd/conf/httpd.conf.original
cp #predefined.otherSettings.deployDataAndSoftwareLocation#/httpd.conf /etc/httpd/conf/httpd.conf
```

Tenga en cuenta que estos comandos utilizan macros predefinidas de la ruta de acceso para los datos extraídos y archivos de software (**predefined.otherSettings.deployDataAndSoftwareLocation**).

También puede agregar comandos para enviar mensajes personalizados al registro de trabajos en XClarity Administrator. Para obtener más información, consulte el apartado Agregar informes de estado personalizados a los scripts de instalación.

Para importar el script de instalación personalizado, lleve a cabo estos pasos. Para obtener más información, consulte Importación de scripts de instalación personalizada.

1. Haga clic en la pestaña **Scripts de instalación**.
2. Haga clic en el icono **Importar** ().

3. Haga clic en **Importación local**.
4. Seleccione `RHEL` para el sistema operativo.
5. Haga clic en **Examinar** para buscar y seleccionar el script de instalación posterior para importar (por ejemplo, `RHEL_installSoftware_customScript.sh`).
6. Haga clic en **Importar** para cargar el archivo al repositorio de imágenes de SO.

Paso 4. Cree un perfil de imagen de SO personalizado que incluya los valores de configuración de software y scripts posterior a la instalación. Para obtener más información, consulte Creación de un perfil de imagen de SO personalizado.

1. Haga clic en la pestaña **Imágenes del SO**.
2. Seleccione un perfil de imagen de SO a personalizar (por ejemplo, `Basic`).
3. Haga clic en el icono **Crear** () para abrir el cuadro de diálogo Crear perfil personalizado.
4. En la pestaña **General**:
   a. Introduzca un nombre para el perfil (por ejemplo: `Custom RHEL with software using post-installation script`).
   b. Utilice el valor predeterminado para el campo **Datos personalizados y ruta de archivo**.
   c. Seleccione **Ninguno** para el tipo de personalización.
   d. Haga clic en **Siguiente**.
5. En la pestaña **Opciones de controlador**, haga clic en **Siguiente**. De forma predeterminada, se incluyen los controladores de dispositivo de entrada.
6. En la pestaña **Software**, seleccione los archivos de instalación de software (por ejemplo, `httpd.conf` e `index.php`) y haga clic en **Siguiente**.
7. En la pestaña **Scripts de instalación**, seleccione los scripts de instalación (por ejemplo, `RHEL_installSoftware_customScript.sh`) y haga clic en **Siguiente**.
8. En la pestaña **Resumen**, revise los valores.
9. Haga clic en **Personalizar** para crear el perfil de imagen del SO personalizado.

Paso 5. Despliegue el perfil de imagen de SO personalizado en los servidores de destino. Para obtener más información, consulte Despliegue de la imagen de un sistema operativo.

1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Desplegar imágenes de SO** para mostrar la página Desplegar sistema operativo: Desplegar imágenes de SO.
2. En cada servidor de destino:
   a. Seleccione el servidor.
   b. Haga clic en **Cambiar selección → Valores de red** y especifique el nombre de host, la dirección IP y los valores de DNS, MTU y VLAN del servidor.

      Consejo: los valores VLAN están disponibles únicamente cuando se establece el modo VLAN en **Valores globales → Asignación de IP → Usar VLAN**.
   c. Seleccione el perfil de imagen de SO personalizado (por ejemplo, <*base_OS*>| <*timestamp*>`_Custom RHEL with software using post-installation script`) de la lista desplegable en la columna **Imagen para desplegar**.

      Nota: Asegúrese de que todos los servidores de destino utilicen el mismo perfil personalizado.
   d. Seleccione la ubicación de almacenamiento preferida donde desee desplegar la imagen del sistema operativo desde la columna **Almacenamiento**.

Nota: Para asegurarse de que los despliegues del sistema operativo sean correctos, desconecte todos los sistemas de almacenamiento del servidor gestionado, a excepción del que haya elegido para el despliegue del sistema operativo.

e. Compruebe que el estado de despliegue del servidor seleccionado sea **Preparado**.

3. Seleccione todos los servidores de destino y haga clic en el icono **Desplegar imagen** () para iniciar el despliegue del sistema operativo.
4. En la pestaña **Resumen**, revise los valores.
5. Haga clic en **Desplegar** para desplegar el sistema operativo.

Despliegue de SLES 12 SP3 con paquetes personalizados y zona horaria

Este escenario instala el sistema operativo SLES 12 SP3 (en inglés) y varios paquetes de SLES opcionales. También le solicita su zona horaria. Se utiliza un perfil de imagen de SO personalizado que incluye un archivo de configuración personalizada y un archivo de instalación desatendida. Este perfil personalizado se puede seleccionar en la página Desplegar imágenes de SO. A continuación, se puede seleccionar los paquetes de SLE que desea desplegar y se puede especificar la zona horaria en la pestaña **Configuración personalizada**. Los valores seleccionados se sustituyen por las macros personalizadas en el proceso de instalación desatendida personalizada y el instalador de AutoYaST para SLES utiliza estos valores de archivo de instalación desatendida para configurar el sistema operativo.

Antes de empezar

Este escenario utiliza los siguientes archivos de muestra.

- SLES_installPackages_customConfig.json. Este archivo de configuración consulta por la zona horaria y los paquetes de SLES opcionales (Linux, Apache, MySQL, paquetes de software PHP, paquetes del servidor de correo SLES y paquetes del servidor de archivos SLES) para instalar.
- SLES_installPackages_customUnattend.xml Este archivo de instalación desatendida utiliza los valores de macros predefinidas y macros personalizadas que se definen en el archivo de configuración.

Procedimiento

Para desplegar SLES 12 SP3 en servidores utilizando un perfil de imagen de SO personalizado, lleve a cabo los pasos siguientes.

Paso 1. Descargue el sistema operativo SLES base desde el sitio web de SUSE en el sistema local e importe la imagen en el repositorio de imágenes de SO. Para obtener más información, consulte Importación de imágenes del sistema operativo.

1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Gestionar imágenes de SO** para mostrar la página Desplegar sistema operativo: Gestionar imágenes de SO.
2. Haga clic en la pestaña **Imágenes del SO**.
3. Haga clic en el icono **Importar** ().
4. Haga clic en **Importación local**.
5. Haga clic en **Examinar** para buscar y seleccionar la imagen de SLES 12 SP3 que se importará (por ejemplo, `SLE-12-SP3-Server-DVD-x86_64-GM-DVD1.iso`).
6. Haga clic en **Importar** para cargar la imagen al repositorio de imágenes de SO.
7. Espere a que se complete la importación. Esto puede tardar varios minutos.

Paso 2. Cree un archivo de valores de configuración personalizados e importe el archivo al repositorio de imágenes de SO.

El archivo de valores de configuración es un archivo JSON que describen los datos que se deben recopilar dinámicamente durante el proceso de despliegue del SO. En este caso, queremos especificar los paquetes de SLES opcionales que se pueden instalar (lo que incluye SLES Linux, Apache, MySQL, el paquete de software PHP, el paquete del servidor de correo SLES y el paquete de servidor de archivo SLES) y una zona horaria que se utilizará para cada despliegue del SO. Para obtener más información sobre cómo crear y desplegar archivos de valores de configuración, consulte Macros personalizadas.

Para importar el archivo de valores de configuración, lleve a cabo estos pasos. Para obtener más información, consulte Importación de valores de configuración personalizada.

1. Haga clic en la pestaña **Archivos de configuración**.
2. Haga clic en el icono **Importar** ( ).
3. Haga clic en **Importación local**.
4. Seleccione `SLES` para el sistema operativo.
5. Haga clic en **Examinar** para buscar y seleccionar el archivo de valores de configuración a importar (por ejemplo, `SLES_installPackages_customConfig.json`).
6. Haga clic en **Importar** para cargar el archivo al repositorio de imágenes de SO.

   Nota: Al importar un archivo de valores de configuración personalizados, XClarity Administrator genera macros personalizadas para cada valor de configuración en el archivo. Puede añadir las macros al archivo de instalación desatendida. Durante el despliegue del SO, las macros se sustituyen con los valores reales.

Paso 3. Modifique el archivo de instalación desatendida de SLES para especificar los valores dinámicos de los paquetes SLES opcionales y la zona horaria y, a continuación, importe el archivo personalizado en el repositorio de imágenes del SO. Para obtener más información, consulte Importación de archivos de instalación desatendida personalizados.

En la sección **<general>**, agregue la información de la zona horaria, por ejemplo:

```
<timezone>
   <hwclock></hwclock>
   <timezone></timezone>
</timezone>
```

En la sección **<patterns>**, añada tres etiquetas de patrón. Las etiquetas se utilizan los macros personalizados para la configuración del paquete de SLES opcional. Por ejemplo:

```
<patterns config:type="list">
   <pattern>32bit</pattern>
   <pattern>Basis-Devel</pattern>
   <pattern>Minimal</pattern>
   <pattern>WBEM</pattern>
   <pattern>apparmor</pattern>
   <pattern>base</pattern>
   <pattern>documentation</pattern>
   <pattern>fips</pattern>
   <pattern>gateway_server</pattern>
   <pattern>ofed</pattern>
   <pattern>printing</pattern>
   <pattern>sap_server</pattern>
   <pattern>x11</pattern>
   <pattern></pattern>
   <pattern></pattern>
   <pattern></pattern>
</patterns>
```

Notas:

- Las etiquetas están en el archivo de instalación desatendida de muestra.
- Cuando se emprende una instalación desatendida personalizada, XClarity Administrator no proporciona varias de las características prácticas comunes que se obtienen cuando se utiliza un archivo de instalación desatendida predefinida. Por ejemplo, los destinos **<DiskConfiguration>**, **<ImageInstall>**, **<ProductKey>** y **<UserAccounts>** para el administrador, **<Interfaces>** para redes y la lista **<package>** de funciones de instalación se deben especificar en el archivo de instalación desatendida personalizada que se está cargando.

Para importar el archivo de instalación personalizada y desatendida, lleve a cabo estos pasos.

1. Haga clic en la pestaña **Archivos de instalación desatendida**.
2. Haga clic en el icono **Importar** ().
3. Haga clic en **Importación local**.
4. Seleccione `SLES` para el sistema operativo.
5. Haga clic en **Examinar** para buscar y seleccionar el archivo de Instalación desatendida a importar (por ejemplo, `SLES_installPackages_customUnattend.xml`).
6. Haga clic en **Importar** para cargar el archivo al repositorio de imágenes de SO.

   Nota: Se muestra una advertencia de que faltan macros predefinidas en el archivo de instalación. Puede hacer caso omiso de las advertencias por ahora. Usted agregará las macros predefinidas en el siguiente paso
7. Haga clic en **Cerrar** en el cuadro de diálogo de advertencia al abrir el cuadro de diálogo Editar archivo de instalación desatendida.

Paso 4. Asocie el archivo de instalación desatendida personalizada con el archivo de valores de configuración personalizado y añada las macros predefinidas y personalizadas (valores) del archivo de valores de configuración en el archivo de instalación desatendida. Para obtener más información, consulte Asociación de un archivo de instalación desatendida con un archivo de valores de configuración, Inyección de macros predefinidas y personalizadas a un archivo de instalación desatendida.

Consejo: opcionalmente, puede asociar el archivo de instalación desatendida personalizado con los valores de configuración personalizados y añadir macros cuando importe el archivo de instalación desatendida

1. Desde el cuadro de diálogo Editar archivo de instalación desatendida, seleccione el archivo de valores de configuración para asociar el archivo de instalación desatendida desde la lista desplegable **Asociar un archivo de configuración** (por ejemplo, `SLES_installPackages_customConfig`).
2. Añada las macros predefinidas necesarias para el archivo de instalación desatendida.
   a. Seleccione **Predefinido** desde la lista desplegable **Macros disponibles**.
   b. Coloque el cursor en el archivo de instalación desatendida en cualquier lugar después de la línea 1 (después de la etiqueta **<xml>**).
   c. Expanda la lista **predefined → unattendSettings** en la lista de macros predefinidas disponibles.
   d. Haga clic en las macros **preinstallConfig** y **postinstallConfig** para añadir las macros en el archivo de instalación desatendida.

   Por ejemplo:

```
#predefined.unattendSettings.preinstallConfig#
#predefined.unattendSettings.postinstallConfig#
<profile xmlns="http://www.suse.com/1.0/yast2ns" xmlns:config="http://www.suse.com/1.0/configns">
```

3. Agregue la macro personalizada para especificar la zona horaria.
   a. Seleccione **Personalizada** desde la lista desplegable **Macros disponibles**.
   b. Coloque el cursor después de la etiqueta **<hwclock>** y haga clic en **timezone** para agregar la macro de zona horaria.
   c. Coloque el cursor después de la etiqueta **<timezone>** y haga clic en **timezone** para agregar la macro de zona horaria.

   Por ejemplo:

```
<timezone>
   <hwclock>#timezone#</hwclock>
   <timezone>#timezone#</timezone>
</timezone>
```

4. Agregue la macro personalizada para especificar los paquetes de SLES opcionales.
   a. Expanda la lista **server-settings → node** en la lista de macros personalizadas disponibles.
   b. Coloque el cursor en una de las etiquetas **<pattern>** vacías y haga clic en **fileserver**.
   c. Coloque el cursor en una de las etiquetas **<pattern>** vacías y haga clic en **lampserver**.
   d. Coloque el cursor en una de las etiquetas **<pattern>** vacías y haga clic en **mailserver**.

   Por ejemplo:

```
<patterns config:type="list">
   <pattern>32bit</pattern>
   <pattern>Basis-Devel</pattern>
   <pattern>Minimal</pattern>
   <pattern>WBEM</pattern>
   <pattern>apparmor</pattern>
   <pattern>base</pattern>
   <pattern>documentation</pattern>
   <pattern>fips</pattern>
   <pattern>gateway_server</pattern>
   <pattern>ofed</pattern>
   <pattern>printing</pattern>
   <pattern>sap_server</pattern>
   <pattern>x11</pattern>
   <pattern>#server-settings.node.fileserver#</pattern>
   <pattern>#server-settings.node.lampserver#</pattern>
   <pattern>#server-settings.node.mailserver#</pattern>
</patterns>
```

5. Haga clic en **Guardar** para vincular los archivos y guardar los cambios en el archivo de instalación desatendida.

Paso 5. Cree un perfil de imagen de SO personalizado que incluya los valores de configuración y de instalación desatendida personalizados. Para obtener más información, consulte Creación de un perfil de imagen de SO personalizado.

1. Haga clic en la pestaña **Imágenes del SO**.
2. Seleccione un perfil de imagen de SO a personalizar (por ejemplo, `Basic`).
3. Haga clic en el icono **Crear** () para abrir el cuadro de diálogo Crear perfil personalizado.
4. En la pestaña **General**:
   a. Introduzca un nombre para el perfil (por ejemplo: `SLES personalizado con paquetes opcionales`).
   b. Utilice el valor predeterminado para el campo **Datos personalizados y ruta de archivo**.
   c. Seleccione **Archivos de instalación desatendida y de valores de configuración asociados** para el tipo de personalización.
   d. Haga clic en **Siguiente**.

5. En la pestaña **Opciones de controlador**, haga clic en **Siguiente**. De forma predeterminada, se incluyen los controladores de dispositivo de entrada.
6. En la pestaña **Software**, haga clic en **Siguiente**.
7. En la pestaña **Archivos de instalación desatendida**, seleccione el archivo de instalación desatendida a importar (por ejemplo, `SLES_installPackages_customUnattend.xml`) y haga clic en **Siguiente**.

   El archivo de valores de configuración asociado se selecciona automáticamente.
8. En la pestaña **Scripts de instalación**, haga clic en **Siguiente**.
9. En la pestaña **Resumen**, revise los valores.
10. Haga clic en **Personalizar** para crear el perfil de imagen del SO personalizado.

Paso 6. Despliegue el perfil de imagen de SO personalizado en los servidores de destino. Para obtener más información, consulte Despliegue de la imagen de un sistema operativo.

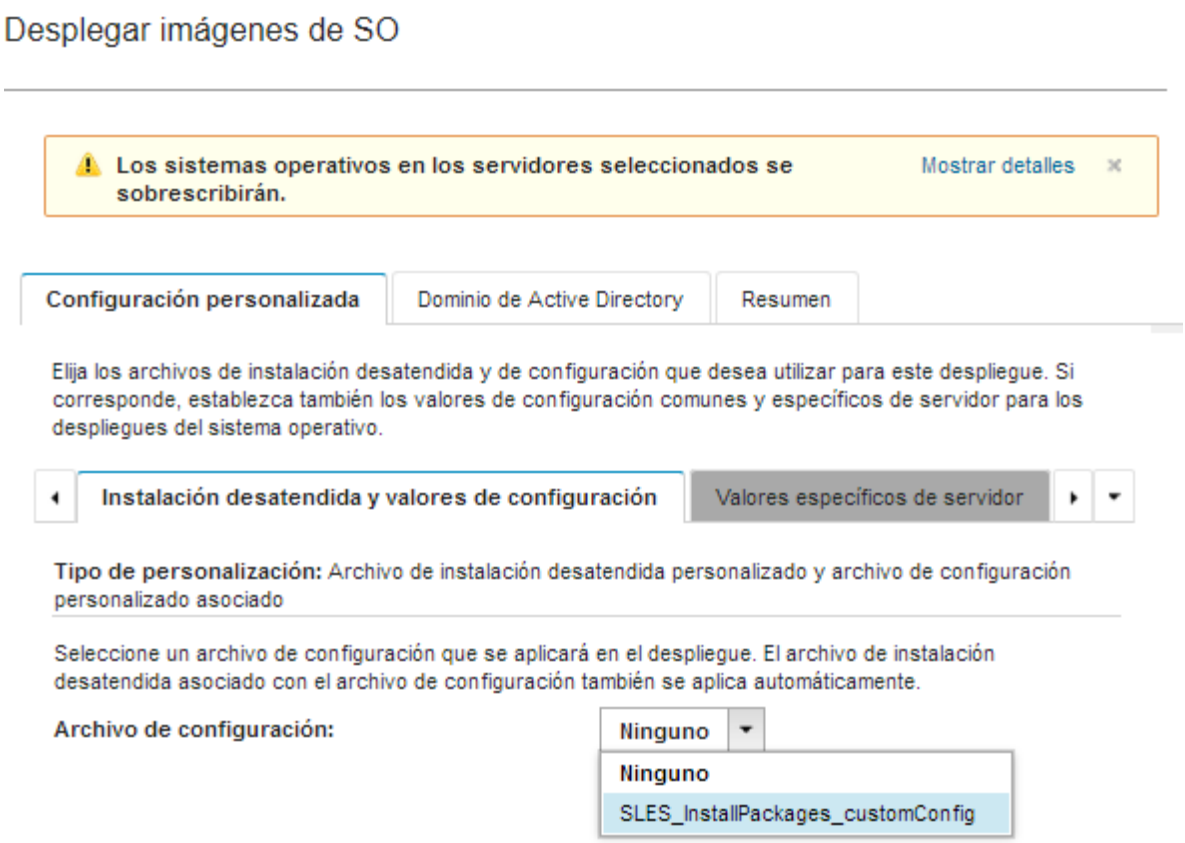
1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Desplegar imágenes de SO** para mostrar la página Desplegar sistema operativo: Desplegar imágenes de SO.
2. En cada servidor de destino:
   a. Seleccione el servidor.
   b. Haga clic en **Cambiar selección → Valores de red** y especifique el nombre de host, la dirección IP y los valores de DNS, MTU y VLAN del servidor.

      Consejo: los valores VLAN están disponibles únicamente cuando se establece el modo VLAN en **Valores globales → Asignación de IP → Usar VLAN**.
   c. Seleccione el perfil de imagen de SO personalizado (por ejemplo, <*base_OS*>|<*timestamp*>`_SLES personalizado con paquetes opcionales`) de la lista desplegable en la columna **Imagen para desplegar**.

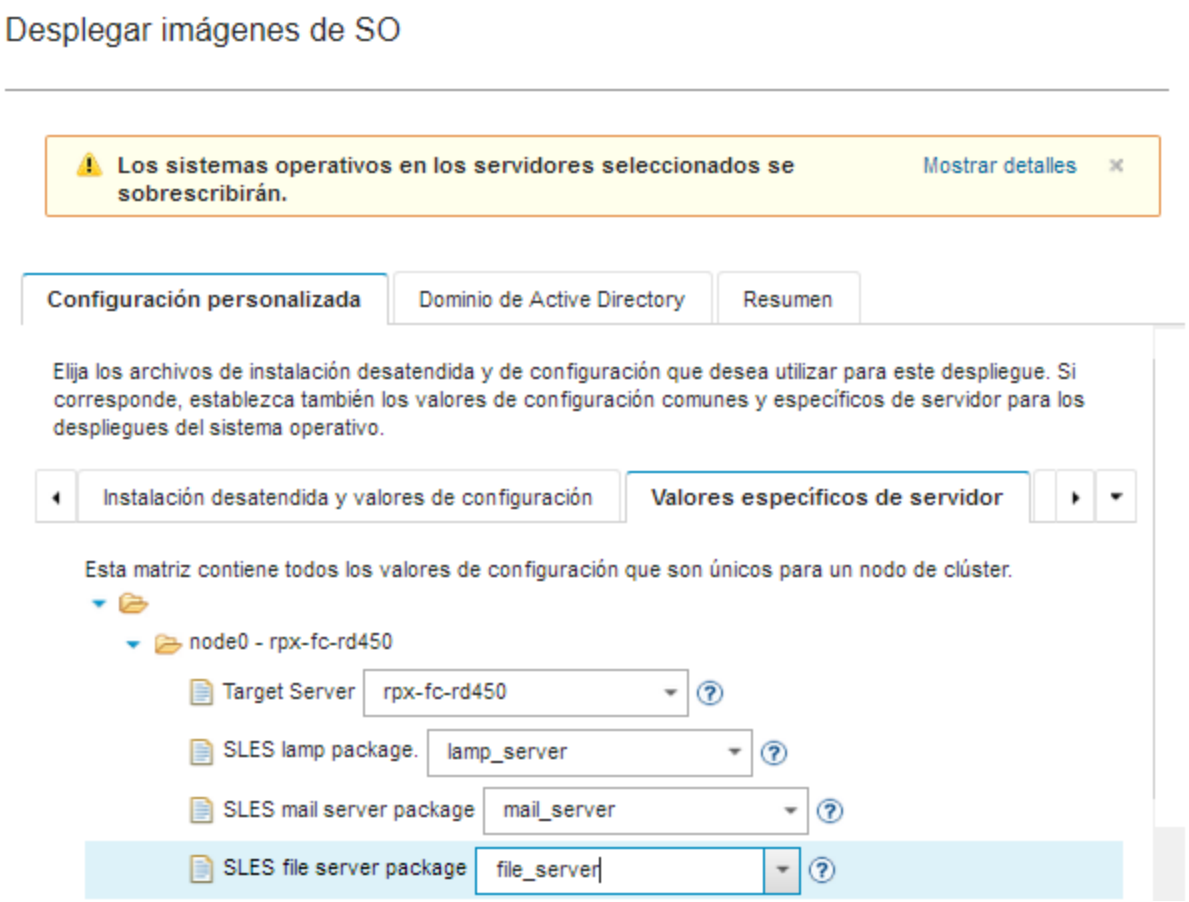
      Nota: Asegúrese de que todos los servidores de destino utilicen el mismo perfil personalizado.
   d. Seleccione la ubicación de almacenamiento preferida donde desee desplegar la imagen del sistema operativo desde la columna **Almacenamiento**.

      Nota: Para asegurarse de que los despliegues del sistema operativo sean correctos, desconecte todos los sistemas de almacenamiento del servidor gestionado, a excepción del que haya elegido para el despliegue del sistema operativo.
   e. Compruebe que el estado de despliegue del servidor seleccionado sea **Preparado**.
3. Seleccione todos los servidores de destino y haga clic en el icono **Desplegar imagen** () para iniciar el despliegue del sistema operativo.
4. En la pestaña **Configuración personalizada**, haga clic en la subpestaña **Valores de instalación desatendida** y de configuración y seleccione el archivo de valores de configuración personalizada (por ejemplo, `SLES_installPackages_customConfig`).

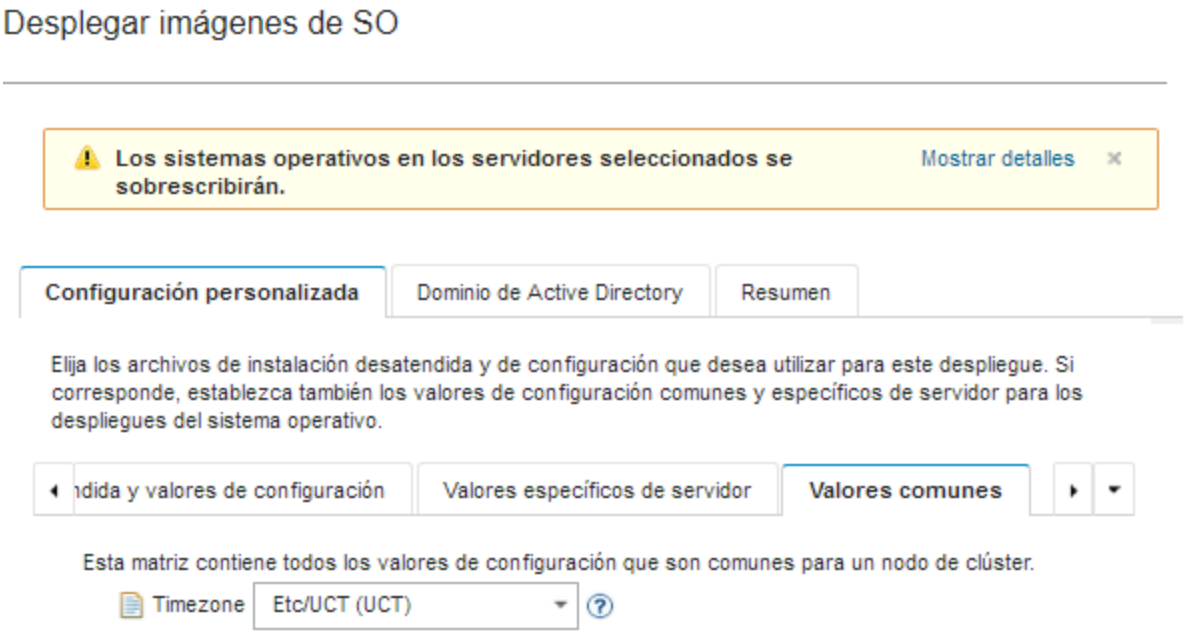
   Nota: El archivo de instalación desatendida personalizado asociado se selecciona automáticamente.



5. En la subpestaña **Valores específicos del servidor**, seleccione el servidor de destino y los paquetes de SLES opcionales que desee desplegar.



6. En la subpestaña **Valores comunes**, seleccione la zona horaria a establecer en todos los servidores de destino.



7. En la pestaña **Resumen**, revise los valores.
8. Haga clic en **Desplegar** para desplegar el sistema operativo.

Despliegue de SLES 12 SP3 con software personalizado

En este caso se instala el sistema operativo SLES 12 SP3 junto con software personalizado (Java y Eclipse IDE). Se utiliza un perfil personalizado que incluye el software personalizado y scripts de instalación posterior para instalar y configurar el software personalizado. Los paquetes de software personalizado se copian al host durante el despliegue y se disponen para usarlos en el script de instalación posterior.

Antes de empezar

Este escenario utiliza los siguientes archivos de muestra.

- jre-8u151-linux-x64.tar.gz. Este es el archivo de instalación de Java para Eclipse.
- eclipse-4.6.3-3.1.x86_64.tar.gz Este es el archivo de instalación para Eclipse IDE.
- SLES_installSoftware_customScript.sh Este script posterior a la instalación crea un usuario para lanzar Eclipse e instala Eclipse IDE y Java.

Notas:

- Los scripts de instalación de SLES pueden estar en uno de los siguientes formatos: Bash (.sh), Perl (.pm o .pl), Python (.py)
- Los archivos de software y scripts de instalación se instalan en la ruta de datos y archivos personalizada que especifica durante el despliegue. La ruta de datos y archivos personalizados predeterminada es `/home/lxca`.
- Para SLES 12 SP3, IDE Eclipse requiere el compilador GCC, que se incluye en el perfil básico. En este caso, se crea un perfil de imagen del SO personalizado utilizando el perfil básico como base. Si elige utilizar otro perfil, debe asegurarse de que el perfil incluya el compilador GCC.

Procedimiento

Para desplegar SLES 12 SP3 con software personalizado, lleve a cabo los pasos siguientes.

Paso 1. Descargue el sistema operativo SLES 12 SP3 base desde el sitio web de SUSE en el sistema local e importe la imagen en el repositorio de imágenes del SO. Para obtener más información, consulte Importación de imágenes del sistema operativo.

1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Gestionar imágenes de SO** para mostrar la página Desplegar sistema operativo: Gestionar imágenes de SO.
2. Haga clic en la pestaña **Imágenes del SO**.
3. Haga clic en el icono **Importar** ( ).
4. Haga clic en **Importación local**.
5. Haga clic en **Examinar** para buscar y seleccionar la imagen de SLES 12 SP3 que se importará (por ejemplo, `SLE-12-SP3-Server-DVD-x86_64-GM-DVD1.iso`).
6. Haga clic en **Importar** para cargar la imagen al repositorio de imágenes de SO.
7. Espere a que se complete la importación. Esto puede tardar varios minutos.

Paso 2. Descargue el software personalizado en el sistema local e importe los archivos al repositorio de imágenes del SO. Para obtener más información, consulte Importación de software personalizado.

1. Haga clic en la pestaña **Software**.
2. Haga clic en el icono **Importar** ( ).
3. Haga clic en **Importación local**.
4. Seleccione `SLES` para el sistema operativo.

5. Haga clic en **Examinar** para buscar y seleccionar el software a importar (por ejemplo, `jre-8u151-linux-x64.tar.gz`).
6. Haga clic en **Importar** para cargar el archivo al repositorio de imágenes de SO.
7. Haga clic en el icono **Importar** () nuevamente.
8. Haga clic en **Importación local**.
9. Seleccione `SLES` para el sistema operativo.
10. Haga clic en **Examinar** para buscar y seleccionar el software a importar (por ejemplo, `eclipse-4.6.3-3.1.x86_64.tar.gz`).
11. Haga clic en **Importar** para cargar el archivo al repositorio de imágenes de SO.

Paso 3. Cree un código posterior a la instalación personalizado e importe el archivo al repositorio de imágenes del SO.

Añada comandos para crear un usuario para iniciar Eclipse para este archivo, por ejemplo:

```
echo "Create a user called lenovo..."
egrep "lenovo" /etc/passwd >/dev/null
pass=$(perl -e 'print crypt($ARGV[0], "password")' "PasswOrd")
useradd -m -p $pass lenovo
[ $? -eq 0 ] &amp;amp;&amp;amp; echo "User has been created." || curl -X PUT
--globoff #predefined.otherSettings.statusSettings.urlStatus# -H "Content-Type: application/json"
-d '{"deployStatus":{"id":"46","parameters":["'"Could not create lenovo user"'"]}}'
--cert #predefined.otherSettings.statusSettings.certLocation#/cert.pem
--key #predefined.otherSettings.statusSettings.certLocation#/key.pem
--cacert #predefined.otherSettings.statusSettings.certLocation#/ca-bundle.crt
```

Añada los comandos para instalar el software, por ejemplo:

```
#Install Java for eclipse
echo "Installing Java JRE 8...."
rpm -ivh #predefined.otherSettings.deployDataAndSoftwareLocation#/jre-8u151-linux-x64.rpm

#Install eclipse
echo "Installing Eclipse IDE..."
rpm -ivh #predefined.otherSettings.deployDataAndSoftwareLocation#/eclipse-4.6.3-3.1.x86_64.rpm
```

Tenga en cuenta que estos comandos utilizan macros predefinidas de URL HTTPS que XClarity Administrator utiliza en los informes de estado (**predefined.otherSettings.statusSettings.urlStatus**), para la carpeta que contiene los certificados que se necesitan para acceder al servicio web urlStatus desde el SO host en el primer inicio (**predefined.otherSettings.statusSettings.certLocation**) y la ruta de acceso a los datos extraídos y archivos de software (**predefined.otherSettings.deployDataAndSoftwareLocation**).

También puede agregar comandos para enviar mensajes personalizados al registro de trabajos en XClarity Administrator, tal como se muestra en el archivo de muestra. Para obtener más información, consulte el apartado Agregar informes de estado personalizados a los scripts de instalación.

Para importar el script de instalación personalizado, lleve a cabo estos pasos. Para obtener más información, consulte Importación de scripts de instalación personalizada.

1. Haga clic en la pestaña **Scripts de instalación**.
2. Haga clic en el icono **Importar** ().
3. Haga clic en **Importación local**.
4. Seleccione `SLES` para el sistema operativo.

5. Haga clic en **Examinar** para buscar y seleccionar el script de instalación posterior para importar (por ejemplo, `SLES_installSoftware_customScript.sh`).
6. Haga clic en **Importar** para cargar el archivo al repositorio de imágenes de SO.

Paso 4. Cree un perfil de imagen de SO personalizado que incluya los valores de configuración de software y scripts posterior a la instalación. Para obtener más información, consulte Creación de un perfil de imagen de SO personalizado.

1. Haga clic en la pestaña **Imágenes del SO**.
2. Seleccione un perfil de imagen de SO a personalizar (por ejemplo, `Basic`).
3. Haga clic en el icono **Crear** () para abrir el cuadro de diálogo Crear perfil personalizado.
4. En la pestaña **General**:
   a. Introduzca un nombre para el perfil (por ejemplo: `SLES personalizado con software`).
   b. Utilice el valor predeterminado para el campo **Datos personalizados y ruta de archivo**.
   c. Seleccione **Ninguno** para el tipo de personalización.
   d. Haga clic en **Siguiente**.
5. En la pestaña **Opciones de controlador**, haga clic en **Siguiente**. De forma predeterminada, se incluyen los controladores de dispositivo de entrada.
6. En la pestaña **Software**, seleccione los archivos de instalación del software (por ejemplo `jre-8u151-linux-x64.tar.gz` y `eclipse-4.6.3-3.1.x86_64.tar.gz`) y, a continuación, haga clic en **Siguiente**.
7. En la pestaña **Scripts de instalación**, seleccione los scripts de instalación (por ejemplo, `SLES_installSoftware_customScript.sh`) y haga clic en **Siguiente**.
8. En la pestaña **Resumen**, revise los valores.
9. Haga clic en **Personalizar** para crear el perfil de imagen del SO personalizado.

Paso 5. Despliegue el perfil de imagen de SO personalizado en los servidores de destino. Para obtener más información, consulte Despliegue de la imagen de un sistema operativo.

1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Desplegar imágenes de SO** para mostrar la página Desplegar sistema operativo: Desplegar imágenes de SO.
2. En cada servidor de destino:
   a. Seleccione el servidor.
   b. Haga clic en **Cambiar selección → Valores de red** y especifique el nombre de host, la dirección IP y los valores de DNS, MTU y VLAN del servidor.

      Consejo: los valores VLAN están disponibles únicamente cuando se establece el modo VLAN en **Valores globales → Asignación de IP → Usar VLAN**.
   c. Seleccione el perfil de imagen de SO personalizado (por ejemplo, <*base_OS*>| <*timestamp*>_`SLES personalizado con software`) de la lista desplegable en la columna **Imagen para desplegar**.

      Nota: Asegúrese de que todos los servidores de destino utilicen el mismo perfil personalizado.
   d. Seleccione la ubicación de almacenamiento preferida donde desee desplegar la imagen del sistema operativo desde la columna **Almacenamiento**.

      Nota: Para asegurarse de que los despliegues del sistema operativo sean correctos, desconecte todos los sistemas de almacenamiento del servidor gestionado, a excepción del que haya elegido para el despliegue del sistema operativo.
   e. Compruebe que el estado de despliegue del servidor seleccionado sea **Preparado**.

3. Seleccione todos los servidores de destino y haga clic en el icono **Desplegar imagen** () para iniciar el despliegue del sistema operativo.
4. En la pestaña **Resumen**, revise los valores.
5. Haga clic en **Desplegar** para desplegar el sistema operativo.

Despliegue de SLES 12 SP3 con una configuración regional configurable y servidores NTP

Este escenario instala el sistema operativo SLES 12 SP3 con inglés, portugués de Brasil o japonés habilitado en el teclado y la configuración regional del sistema operativo. También configura la dirección IP para hasta tres servidores NTP. Se usa un perfil personalizado de imagen de SO que incluye un archivo de instalación desatendida (con macros predefinidas y personalizadas), además de un archivo de valores de configuración para seleccionar la configuración regional y del servidor NTP. Este perfil personalizado se puede seleccionar en la página Desplegar imágenes de SO. Después, la configuración regional y del servidor NTP se pueden especificar en la pestaña **Configuración personalizada**. Los valores especificados se sustituyen por las macros personalizadas contenidas en el archivo de instalación desatendida personalizada y el instalador de AutoYaST para SLES utiliza estos valores de archivo de instalación desatendida para configurar el sistema operativo.

Antes de empezar

Este escenario utiliza los siguientes archivos de muestra.

- SLES_locale_customConfig.json. Este archivo de configuración personalizada solicita el idioma a instalar para la configuración regional del SO y del teclado tanto para SLES como para el servidor NTP.
- SLES_locale_customUnattend.xml. Este archivo de instalación desatendida personalizada utiliza los valores de las macros personalizadas que se definen en el archivo de configuración.

Procedimiento

Para desplegar SLES 12 SP3 utilizando un perfil de imagen del SO personalizado, lleve a cabo los pasos siguientes.

Paso 1. Descargue el sistema operativo SLES base desde el sitio web de SUSE en el sistema local e importe la imagen en el repositorio de imágenes de SO. Para obtener más información, consulte Importación de imágenes del sistema operativo.

1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Gestionar imágenes de SO** para mostrar la página Desplegar sistema operativo: Gestionar imágenes de SO.
2. Haga clic en la pestaña **Imágenes del SO**.
3. Haga clic en el icono **Importar** ().
4. Haga clic en **Importación local**.
5. Haga clic en **Examinar** para buscar y seleccionar la imagen de SLES 12 SP3 que se importará (por ejemplo, `SLE-12-SP3-Server-DVD-x86_64-GM-DVD1.iso`).
6. Haga clic en **Importar** para cargar la imagen al repositorio de imágenes de SO.
7. Espere a que se complete la importación.

Paso 2. Cree un archivo de valores de configuración personalizados e importe el archivo al repositorio de imágenes de SO.

El archivo de valores de configuración es un archivo JSON que describen los datos que se deben recopilar dinámicamente durante el proceso de despliegue del SO. En este caso, buscamos especificar la configuración regional del sistema operativo (en_US, ja_JP, pt_BR), la configuración

regional de teclado (inglés-EE. UU., japonés o portugués-br) y hasta tres direcciones IP del servidor NTP que se utilizará para cada despliegue del SO. Para obtener más información sobre cómo crear y desplegar archivos de valores de configuración, consulte Macros personalizadas.

Para importar el archivo de valores de configuración, lleve a cabo estos pasos. Para obtener más información, consulte Importación de valores de configuración personalizada.

1. Haga clic en la pestaña **Archivos de configuración**.
2. Haga clic en el icono **Importar** ().
3. Haga clic en **Importación local**.
4. Seleccione `SLES` para el sistema operativo.
5. Haga clic en **Examinar** para buscar y seleccionar el archivo de valores de configuración a importar (por ejemplo, `SLES_locale_customConfig.json`).
6. Haga clic en **Importar** para cargar el archivo al repositorio de imágenes de SO

   Nota: Al importar un archivo de valores de configuración personalizados, XClarity Administrator genera macros personalizadas para cada valor de configuración en el archivo. Puede añadir las macros al archivo de instalación desatendida. Durante el despliegue del SO, las macros se sustituyen con los valores reales.

Paso 3. Modifique el archivo de instalación desatendida de SLES para especificar los valores dinámicos de la configuración local del sistema operativo y del teclado, además de las direcciones IP del servidor NTP; a continuación, importe el archivo personalizado en el repositorio de imágenes del SO. Para obtener más información, consulte Importación de archivos de instalación desatendida personalizados.

Inmediatamente después de la etiqueta <profile>, agregue la información del servidor NTP y de red: El siguiente ejemplo incluye etiquetas para los dos servidores NTP. La dirección IP se agregará como macros en un paso posterior.

```
<ntp-client>
   <configure_dhcp config:type="boolean">false</configure_dhcp>
   <peers config:type="list">
      <peer>
         <address></address>
         <initial_sync config:type="boolean">true</initial_sync>
         <options></options>
         <type>server</type>
      </peer>
      <peer>
         <address></address>
         <initial_sync config:type="boolean">true</initial_sync>
         <options></options>
         <type>server</type>
      </peer>
   </peers>
   <start_at_boot config:type="boolean">true</start_at_boot>
   <start_in_chroot config:type="boolean">true</start_in_chroot>
</ntp-client>
```

En la sección <general>, agregue la información de configuración regional del teclado y del sistema operativo, como se muestra en el siguiente ejemplo. Los valores locales del teclado y del sistema operativo se agregan como macros en un paso posterior.

```
<keyboard>
   <keymap></keymap>
</keyboard>
<language></language>
```

Nota: Cuando se emprende una instalación desatendida personalizada, XClarity Administrator no proporciona varias de las características prácticas comunes que se obtienen cuando se utiliza un archivo de instalación desatendida predefinida. Por ejemplo, los destinos **<DiskConfiguration>**, **<ImageInstall>**, **<ProductKey>** y **<UserAccounts>** para el administrador, **<Interfaces>** para redes y la lista **<package>** de funciones de instalación se deben especificar en el archivo de instalación desatendida personalizada que se está cargando.

Para importar el archivo de instalación personalizada y desatendida, lleve a cabo estos pasos.

1. Haga clic en la pestaña **Archivos de instalación desatendida**.
2. Haga clic en el icono **Importar** ( ).
3. Haga clic en **Importación local**.
4. Seleccione `SLES` para el sistema operativo.
5. Haga clic en **Examinar** para buscar y seleccionar el archivo de Instalación desatendida a importar (por ejemplo, `SLES_locale_customUnattend.xml`).
6. Haga clic en **Importar** para cargar el archivo al repositorio de imágenes de SO

Paso 4. Asocie el archivo de instalación desatendida personalizada con el archivo de valores de configuración personalizado y añada las macros predefinidas y personalizadas (valores) del archivo de valores de configuración en el archivo de instalación desatendida. Para obtener más información, consulte Asociación de un archivo de instalación desatendida con un archivo de valores de configuración, Inyección de macros predefinidas y personalizadas a un archivo de instalación desatendida

Consejo: opcionalmente, puede utilizar el archivo de instalación desatendida personalizado con los valores de configuración personalizados y añadir macros cuando importe el archivo de instalación desatendida.

1. En la pestaña **Archivos de instalación desatendida**, seleccione el archivo de instalación desatendida personalizada (por ejemplo, `SLES_locale_customUnattend.xml`).
2. Haga clic en el icono **Asociar un archivo de configuración** ( ) para mostrar el cuadro de diálogo Asociar un archivo de instalación desatendida.
3. Seleccione el archivo de valores de configuración para asociar con el archivo de instalación desatendida (por ejemplo, `SLES_locale_customConfig`).
4. Añada las macros predefinidas necesarias para el archivo de instalación desatendida.
   a. Seleccione **Predefinido** desde la lista desplegable **Macros disponibles**.
   b. Coloque el cursor en el archivo de instalación desatendida en cualquier lugar después de la línea 1 (después de la etiqueta **<xml>**).
   c. Expanda la lista **predefined → unattendSettings** en la lista de macros predefinidas disponibles.
   d. Haga clic en las macros **preinstallConfig** y **postinstallConfig** para añadir las macros.

   Por ejemplo:

```
<?xml version="1.0"?>
<!DOCTYPE profile SYSTEM "/usr/share/YaST2/include/autoinstall/profile.dtd">
   #predefined.unattendSettings.preinstallConfig#
   #predefined.unattendSettings.postinstallConfig#
<profile xmlns="http://www.suse.com/1.0/yast2ns" xmlns:config="http://www.suse.com/1.0/configns">
```

5. Agregue la macro personalizada para especificar la configuración local del sistema operativo.
   a. Seleccione **Personalizada** desde la lista desplegable **Macros disponibles**
   b. Coloque el cursor después de la etiqueta **<language>**.

c. Expanda **server-settings → node** en la lista de macros personalizadas disponibles y, a continuación, haga clic en **locale** para agregar la macro de configuración regional de sistema operativo.

Por ejemplo:

```
<language>#server-settings.node.locale#</language>
```

6. Agregue la macro personalizada para especificar la configuración local del teclado.
   a. Coloque el cursor después de la etiqueta **<keymap>**.
   b. Expanda **server-settings → node** en la lista de macros personalizadas disponibles y, a continuación, haga clic en **keyboardLocale** para agregar la macro de configuración regional del teclado.

   Por ejemplo:

```
<keyboard>
   <keymap>#server-settings.node.keyboardLocale#</keymap>
</keyboard>
```

7. Agregue la macro personalizada para especificar las direcciones IP del servidor NTP.

   En este caso, el archivo de valores personalizados de la configuración utiliza una plantilla para especificar entre cero y tres servidores NTP. Cuando utiliza plantillas en el archivo de configuración, los macros que están asociados con la plantilla no se muestran en el cuadro de diálogo Asociar un archivo de instalación desatendida. En su lugar, debe editar el archivo de instalación desatendida y agregar los macros y las etiquetas correspondientes de forma manual.

   Por ejemplo, para incluir tres servidores NTP, agregaría las siguientes etiquetas y macros al archivo de instalación. Estas etiquetas y macros ya existen en el archivo de instalación de muestra para este escenario.

```
<ntp-client>
   <configure_dhcp config:type="boolean">false</configure_dhcp>
   <peers config:type="list">
      <peer>
         <address>#server-settings.ntpserver1#</address>
         <initial_sync config:type="boolean">true</initial_sync>
         <options></options>
         <type>server</type>
      </peer>
      <peer>
         <address>#server-settings.ntpserver2#</address>
         <initial_sync config:type="boolean">true</initial_sync>
         <options></options>
         <type>server</type>
      </peer>
      <peer>
         <address>#server-settings.ntpserver3#</address>
         <initial_sync config:type="boolean">true</initial_sync>
         <options></options>
         <type>server</type>
      </peer>
   </peers>
   <start_at_boot config:type="boolean">true</start_at_boot>
    <start_in_chroot config:type="boolean">true</start_in_chroot>
</ntp-client>
```

8. Haga clic en **Asociar** para vincular los archivos y guardar los cambios en el archivo de instalación desatendida.

Paso 5. Cree un perfil de imagen de SO personalizado que incluya los valores de configuración y de instalación desatendida personalizados. Para obtener más información, consulte Creación de un perfil de imagen de SO personalizado.

1. Haga clic en la pestaña **Imágenes del SO**.
2. Seleccione un perfil de imagen de SO a personalizar (por ejemplo, `Basic`).
3. Haga clic en el icono **Crear** () para abrir el cuadro de diálogo Crear perfil personalizado.
4. En la pestaña **General**:
   a. Ingrese un nombre para el perfil (por ejemplo, `SLES personalizado para configuración regional de SO y teclado y servidor NTP`).
   b. Utilice el valor predeterminado para el campo **Datos personalizados y ruta de archivo**.
   c. Seleccione **Archivos de instalación desatendida y de valores de configuración asociados** para el tipo de personalización.
   d. Haga clic en **Siguiente**.
5. En la pestaña **Opciones de controlador**, haga clic en **Siguiente**. De forma predeterminada, se incluyen los controladores de dispositivo de entrada.
6. En la pestaña **Software**, haga clic en **Siguiente**.
7. En la pestaña **Archivos de instalación desatendida**, seleccione el archivo de instalación desatendida a importar (por ejemplo, `SLES_locale_customUnattend.xml`) y haga clic en **Siguiente**.

   El archivo de valores de configuración asociado se selecciona automáticamente.
8. En la pestaña **Scripts de instalación**, haga clic en **Siguiente**.
9. En la pestaña **Resumen**, revise los valores.
10. Haga clic en **Personalizar** para crear el perfil de imagen del SO personalizado.

Paso 6. Despliegue el perfil de imagen de SO personalizado en el servidor de destino. Para obtener más información, consulte Despliegue de la imagen de un sistema operativo.

1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Desplegar imágenes de SO** para mostrar la página Desplegar sistema operativo: Desplegar imágenes de SO.
2. En cada servidor de destino:
   a. Seleccione el servidor.
   b. Haga clic en **Cambiar selección → Valores de red** y especifique el nombre de host, la dirección IP y los valores de DNS, MTU y VLAN del servidor.

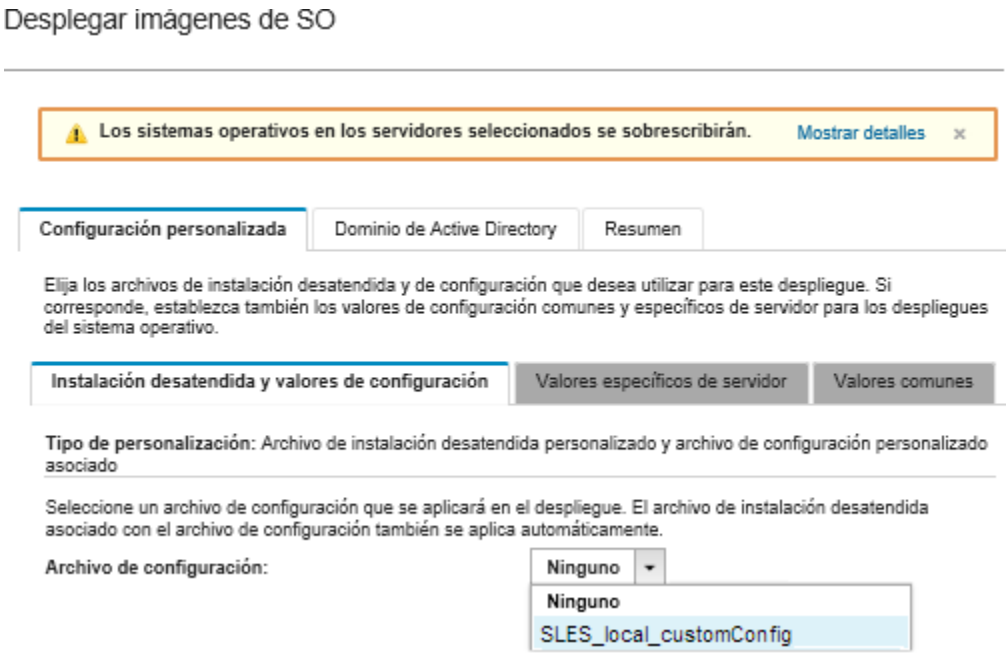
      Consejo: los valores VLAN están disponibles únicamente cuando se establece el modo VLAN en **Valores globales → Asignación de IP → Usar VLAN**.
   c. Seleccione el perfil de imagen de SO personalizado (por ejemplo, <*base_OS*>| <*timestamp*>`_SLES personalizado para SO, configuración local de teclado y servidor NTP`) de la lista desplegable en la columna **Imagen para desplegar**

      Nota: Asegúrese de que todos los servidores de destino utilicen el mismo perfil personalizado.
   d. Seleccione la ubicación de almacenamiento preferida donde desee desplegar la imagen del sistema operativo desde la columna **Almacenamiento**.

      Nota: Para asegurarse de que los despliegues del sistema operativo sean correctos, desconecte todos los sistemas de almacenamiento del servidor gestionado, a excepción del que haya elegido para el despliegue del sistema operativo.
   e. Compruebe que el estado de despliegue del servidor seleccionado sea **Preparado**.

3. Seleccione todos los servidores de destino y haga clic en el icono **Desplegar imagen** ( ) para iniciar el despliegue del sistema operativo.
4. En la pestaña **Configuración personalizada**, haga clic en la subpestaña **Valores de instalación desatendida** y de configuración y seleccione el archivo de valores de configuración personalizada (por ejemplo, `SLES_locale_customConfig`).

   Nota: El archivo de instalación desatendida personalizado asociado se selecciona automáticamente.



5. En la subpestaña **Valores específicos del servidor**, seleccione el servidor de destino, configuración regional de sistema operativo y la configuración regional de teclado.
6. En la subpestaña **Valores comunes**, haga clic en **Añadir** para especificar la dirección IP de hasta tres servidores NTP.
7. En la pestaña **Resumen**, revise los valores.
8. Haga clic en **Desplegar** para desplegar el sistema operativo.

Despliegue de VMware ESXi v6.7 con personalización de Lenovo a un disco local usando la dirección IP estática

Este escenario instala el sistema operativo VMware ESXi v6.7 con personalización de Lenovo en el disco local mediante la dirección IP estática del servidor host. Se utiliza un perfil de imagen de SO personalizado que incluye un archivo de instalación desatendida con macros predefinidas. Este perfil personalizado se puede seleccionar en la página Desplegar imágenes de SO. Los valores conocidos se sustituyen por las macros predefinidas en el archivo de instalación desatendida personalizado y el instalador de comienzo de VMware ESXi utiliza estos valores de archivo de instalación desatendida para configurar el sistema operativo.

Antes de empezar

Este escenario utiliza los siguientes archivos de muestra.

- ESXi_staticIP_customUnattend.cfg. Este archivo desatendido personalizado utiliza valores de macros predefinidas.

Procedimiento

Para desplegar VMware ESXi v6.7 utilizando un perfil de imagen de SO personalizado, lleve a cabo los pasos siguientes.

Paso 1. Descargue el sistema operativo VMware vSphere® Hypervisor (ESXi) con personalización de Lenovo desde el sitio web de Soporte de VMware - página web de descargas en el sistema local e importe la imagen en el repositorio de imágenes del SO. Para obtener más información, consulte Importación de imágenes del sistema operativo.

1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Gestionar imágenes de SO** para mostrar la página Desplegar sistema operativo: Gestionar imágenes de SO.
2. Haga clic en la pestaña **Imágenes del SO**.
3. Haga clic en el icono **Importar** ().
4. Haga clic en **Importación local**.
5. Haga clic en **Examinar** para buscar y seleccionar la imagen de ESXi que se importará (por ejemplo, `ESXi6.7-7535516-RC-Lenovo_20180126_Async.iso`).
6. Haga clic en **Importar** para cargar la imagen al repositorio de imágenes de SO.
7. Espere a que se complete la importación.

Paso 2. Modificar el archivo de ESXi desatendido (comienzo) para añadir las macros predefinidas necesarias y otras macros predefinidas donde corresponda, como la dirección IP, la puerta de enlace, los valores de DNS y de nombre de host y luego importar el archivo en el repositorio de imágenes del SO. Para obtener más información, consulte Importación de archivos de instalación desatendida personalizados.

Solo para ESXi y RHEL, XClarity Administrator proporciona la macro **#predefined.unattendSettings.networkConfig#**, que añade a todos los valores de red que se definen en la interfaz de usuario al archivo de instalación desatendida. Ya que este ejemplo especifica un valor (**--addvmportgroup**) que no se define en la interfaz de usuario, la macro **#predefinedunattendSettings.storageConfig#** no se utiliza en el archivo de instalación desatendida de muestra. En su lugar, se añaden individualmente los valores de red en el archivo y se utilizan las macros **#predefined.hostPlatforms.networkSettings.**<*setting*>**#**.

Solo para ESXi y RHEL, XClarity Administrator proporciona la macro **#predefined.unattendSettings.storageConfig#**, que añade a todos los valores de almacenamiento que se definen en la interfaz de usuario al archivo de instalación desatendida. Ya que este ejemplo especifica valores (**--novmfsondisk** y **–ignoressd**) que no se definen en la interfaz de usuario, la macro **#predefinedunattendSettings.storageConfig#** no se utiliza en el archivo de instalación desatendida de muestra. En su lugar, los valores de almacenamiento se agregan individualmente y **--firstdisk=local** está codificado en el archivo.

Nota: XClarity Administrator ofrece algunas macros prácticas de nivel básico, como la inserción de controladores OOB, informes de estado, scripts posteriores a la instalación, software personalizado. Sin embargo, para aprovechar estas macros predefinidas, debe especificar las siguientes macros en el archivo desatendido personalizado. El archivo de ejemplo ya contiene las macros necesarias. Tenga en cuenta que debido a que se incluye la sección %firstboot, el orden de estas macros predefinidas importa. Para obtener más información, consulte Importación de archivos de instalación desatendida personalizados.

```
#predefined.unattendSettings.preinstallConfig#
#predefined.unattendSettings.postinstallConfig#
```

El archivo de muestra ya contiene las macros necesarias y las macros predefinidas adicionales para especificar dinámicamente los valores de red para el servidor de destino. Para obtener más

información acerca de cómo agregar macros a archivos de instalación desatendida, consulte Inyección de macros predefinidas y personalizadas a un archivo de instalación desatendida.

Para obtener más información acerca de las macros predefinidos disponibles, consulte Macros predefinidas.

Para importar el archivo de instalación personalizada y desatendida, lleve a cabo estos pasos.

1. Haga clic en la pestaña **Archivos de instalación desatendida**.
2. Haga clic en el icono **Importar** ().
3. Haga clic en **Importación local**.
4. Seleccione `ESXi` para el sistema operativo.
5. Haga clic en **Examinar** para buscar y seleccionar el archivo de Instalación desatendida a importar (por ejemplo, `ESXi_staticIP_customUnattend.cfg`).
6. Haga clic en **Importar** para cargar el archivo al repositorio de imágenes de SO

Paso 3. Cree un perfil de imagen del SO personalizado que incluya el archivo de instalación desatendida personalizado. Para obtener más información, consulte Creación de un perfil de imagen de SO personalizado.

1. Haga clic en la pestaña **Imágenes del SO**.
2. Seleccione un perfil de imagen de SO a personalizar (por ejemplo, `Virtualization`).
3. Haga clic en el icono **Crear** () para abrir el cuadro de diálogo Crear perfil personalizado.
4. En la pestaña **General**:
   a. Introduzca un nombre para el perfil (por ejemplo: `ESXi personalizada con IP estática`).
   b. Utilice el valor predeterminado para el campo **Datos personalizados y ruta de archivo**.
   c. Seleccione **Solo archivos de instalación desatendida** en el tipo de personalización.
   d. Haga clic en **Siguiente**.
5. En la pestaña **Archivos de instalación desatendida**, seleccione el archivo de instalación desatendida a importar (por ejemplo, `ESXi_staticIP_customUnattend.cfg`) y haga clic en **Siguiente**.
6. En la pestaña **Resumen**, revise los valores.
7. Haga clic en **Personalizar** para crear el perfil de imagen del SO personalizado.

Paso 4. Despliegue el perfil de imagen de SO personalizado en el servidor de destino. Para obtener más información, consulte Despliegue de la imagen de un sistema operativo.

1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Desplegar imágenes de SO** para mostrar la página Desplegar sistema operativo: Desplegar imágenes de SO.
2. En cada servidor de destino:
   a. Seleccione el servidor.
   b. Haga clic en **Cambiar selección → Valores de red** y especifique el nombre de host, la dirección IP y los valores de DNS, MTU y VLAN del servidor.

      Consejo:

      - Los valores VLAN están disponibles únicamente cuando el modo VLAN se establece en **Valores globales → Asignación de IP → Usar VLAN**.
      - Los valores de red que especifique en el cuadro de diálogo Valores de red se agregan al archivo desatendido en el tiempo de ejecución usando la macro **#predefined. hostPlatforms.networkSettings.**<*setting*>**#**.

c. Seleccione el perfil de imagen de SO personalizado (por ejemplo, <*base_OS*>| <*timestamp*>_ESXi personalizada con IP estática) de la lista desplegable en la columna **Imagen para desplegar**.

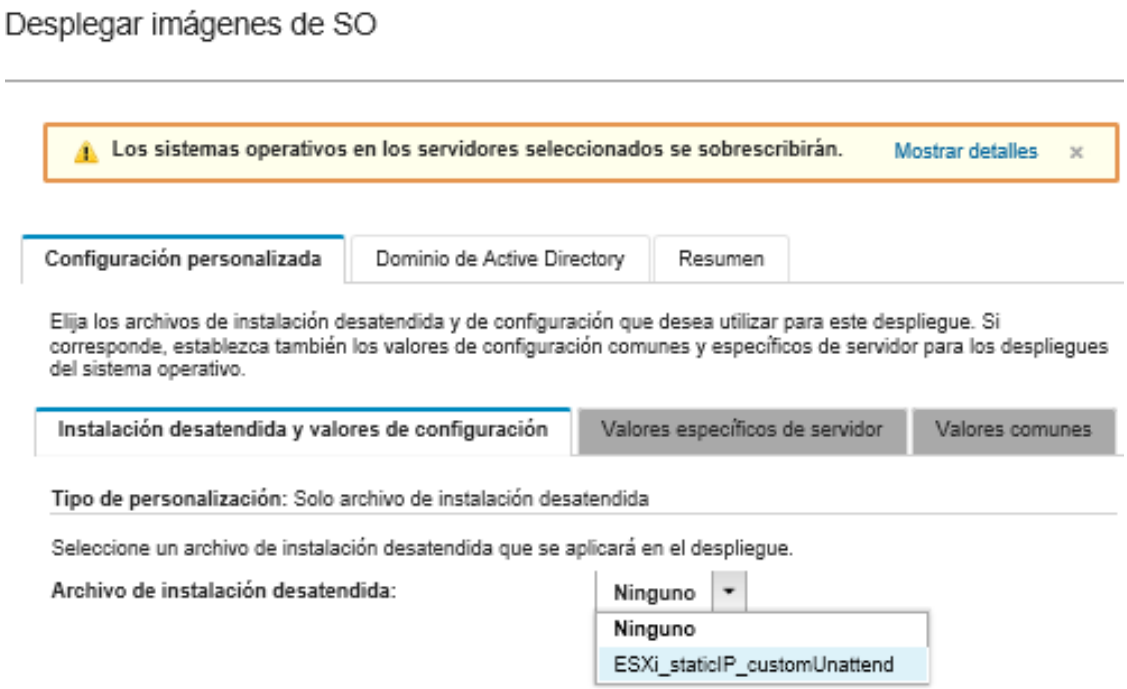
   Nota: Asegúrese de que todos los servidores de destino utilicen el mismo perfil personalizado.

d. (Opcional) Haga clic en el icono **Clave de licencia** ( ) y especifique la clave de licencia que se va a utilizar para activar el sistema operativo una vez instalado.

e. Compruebe que el estado de despliegue del servidor seleccionado sea **Preparado**.

Nota: Ya que se especificó **--firstdisk=local** en el archivo de instalación desatendida, no necesita especificar la ubicación de almacenamiento preferida en la columna **Almacenamiento**. Se ignora la configuración de la interfaz de usuario.

3. Seleccione todos los servidores de destino y haga clic en el icono **Desplegar imagen** ( ) para iniciar el despliegue del sistema operativo.
4. En la pestaña **Configuración personalizada**, haga clic en la subpestaña **Valores de instalación desatendida y de configuración** y seleccione el archivo de instalación desatendida personalizada (por ejemplo, ESXi_staticIP_customUnattend.cfg).



5. En la pestaña **Resumen**, revise los valores.
6. Haga clic en **Desplegar** para desplegar el sistema operativo.

Despliegue de VMware ESXi v6.7 con personalización de Lenovo con configuración regional configurable y credenciales de segundo usuario

Este escenario instala el sistema operativo VMware ESXi v6.7 con personalización de Lenovo con un idioma configurarle habilitado para la configuración regional de teclado y credenciales de segundo usuario de ESXi. Este ejemplo también utiliza la configuración básica de red y de almacenamiento que se define en la interfaz de usuario. Se usa un perfil de imagen de SO personalizado que incluye un archivo de instalación desatendida (con macros predefinidas y personalizadas), además de un archivo de valores de configuración para seleccionar la contraseña. Este perfil personalizado se puede seleccionar en la página Desplegar

imágenes de SO. A continuación, puede especificar la contraseña en la pestaña **Configuración personalizada**. El valor especificado se sustituye por la macro personalizada en el archivo de instalación desatendida personalizado y el instalador de ESXi utiliza estos valores de archivo de instalación desatendida para configurar el sistema operativo.

Antes de empezar

Este escenario utiliza los siguientes archivos de muestra.

- ESXi_locale_customConfig.json. Este archivo de configuración personalizada pedirá las credenciales para el segundo usuario de ESXi y la configuración regional de teclado.
- ESXi_locale_customUnattend.cfg. Este archivo de instalación desatendida personalizada utiliza los valores en macros predefinidas y personalizadas que se definen en el archivo de configuración.

Procedimiento

Para desplegar VMware ESXi v6.7 utilizando un perfil de imagen de SO personalizado, lleve a cabo los pasos siguientes.

Paso 1. Descargue el sistema operativo VMware vSphere® Hypervisor (ESXi) con personalización de Lenovo desde el sitio web de Soporte de VMware - página web de descargas en el sistema local e importe la imagen en el repositorio de imágenes del SO. Para obtener más información, consulte Importación de imágenes del sistema operativo.

1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Gestionar imágenes de SO** para mostrar la página Desplegar sistema operativo: Gestionar imágenes de SO.
2. Haga clic en la pestaña **Imágenes del SO**.
3. Haga clic en el icono **Importar** ( ).
4. Haga clic en **Importación local**.
5. Haga clic en **Examinar** para buscar y seleccionar la imagen de ESXi que se importará (por ejemplo, `ESXi6.7-7535516-RC-Lenovo_20180126_Async.iso`).
6. Haga clic en **Importar** para cargar la imagen al repositorio de imágenes de SO.
7. Espere a que se complete la importación.

Paso 2. Cree un archivo de valores de configuración personalizados e importe el archivo al repositorio de imágenes de SO.

El archivo de valores de configuración es un archivo JSON que describen los datos que se deben recopilar dinámicamente durante el proceso de despliegue del SO. En este caso, queremos elegir la configuración regional de teclado y el Id. de usuario y contraseña que se utilizará para un segundo usuario de ESXi en cada despliegue del SO. Para obtener más información sobre cómo crear y desplegar archivos de valores de configuración, consulte Macros personalizadas.

Para importar el archivo de valores de configuración, lleve a cabo estos pasos. Para obtener más información, consulte Importación de valores de configuración personalizada.

1. Haga clic en la pestaña **Archivos de configuración**.
2. Haga clic en el icono **Importar** ( ).
3. Haga clic en **Importación local**.
4. Seleccione `ESXi` para el sistema operativo.
5. Haga clic en **Examinar** para buscar y seleccionar el archivo de valores de configuración a importar (por ejemplo, `ESXi_locale_customConfig.json`).

6. Haga clic en **Importar** para cargar el archivo al repositorio de imágenes de SO

   Nota: Al importar un archivo de valores de configuración personalizados, XClarity Administrator genera macros personalizadas para cada valor de configuración en el archivo. Puede añadir las macros al archivo de instalación desatendida. Durante el despliegue del SO, las macros se sustituyen con los valores reales.

Paso 3. Modifique el archivo de instalación desatendida de ESXi (comienzo) para especificar la configuración local del sistema operativo y el teclado, además de las credenciales de usuario para el segundo usuario de ESXi; y luego importe el archivo personalizado en el repositorio de imágenes del SO. Para obtener más información, consulte Importación de archivos de instalación desatendida personalizados.

Agregue comandos para establecer la configuración local del teclado, por ejemplo:

```
# Set the keyboard locale
keyboard ''
```

Agregue comandos para crear un segundo usuario de ESXi. En el siguiente ejemplo, *<user_id>* y *<password>* serán reemplazados con macros personalizadas en el paso siguiente.

```
#Create second user
/usr/lib/vmware/auth/bin/adduser -D -h /tmp <user_id>
echo <password> | /usr/lib/vmware/auth/bin/passwd <user_id> --stdin
/bin/vim-cmd vimsvc/auth/entity_permission_add vim.Folder:ha-folder-root <user_id> false Admin true
```

Para importar el archivo de instalación personalizada y desatendida, lleve a cabo estos pasos.

1. Haga clic en la pestaña **Archivos de instalación desatendida**.
2. Haga clic en el icono **Importar** ().
3. Haga clic en **Importación local**.
4. Seleccione `ESXi` para el sistema operativo.
5. Haga clic en **Examinar** para buscar y seleccionar el archivo de Instalación desatendida a importar (por ejemplo, `ESXi_locale_customUnattend.cfg`).
6. Haga clic en **Importar** para cargar el archivo al repositorio de imágenes de SO

Paso 4. Asocie el archivo de instalación desatendida personalizada con el archivo de valores de configuración personalizado y añada las macros predefinidas y personalizadas (valores) del archivo de valores de configuración en el archivo de instalación desatendida. Para obtener más información, consulte Asociación de un archivo de instalación desatendida con un archivo de valores de configuración, Inyección de macros predefinidas y personalizadas a un archivo de instalación desatendida

Consejo:

- Opcionalmente, puede asociar el archivo de instalación desatendida personalizado con los valores de configuración personalizados y añadir macros cuando importe el archivo de instalación desatendida
- XClarity Administrator ofrece algunas macros prácticas de nivel básico, como la inserción de controladores OOB, informes de estado, scripts posteriores a la instalación, software personalizado. Sin embargo, para aprovechar estas macros predefinidas, debe especificar las siguientes macros en el archivo desatendido personalizado. El archivo de ejemplo ya contiene las macros necesarias. Tenga en cuenta que debido a que se incluye la sección %firstboot, el orden de estas macros predefinidas importa. Para obtener más información, consulte Importación de archivos de instalación desatendida personalizados.

  ```
  #predefined.unattendSettings.preinstallConfig#
  #predefined.unattendSettings.postinstallConfig#
  ```

- XClarity Administrator también proporciona macros que entre tanto de las configuraciones de red y de almacenamiento que se definen en la interfaz de usuario. Estos son útiles cuando se desistan solo valores básicos para el despliegue. El archivo de ejemplo ya contiene las macros necesarias.
  ```
  #predefined.unattendSettings.networkConfig#
  #predefined.unattendSettings.storageConfig#
  ```

Para obtener más información acerca de cómo agregar macros a archivos de instalación desatendida, consulte Inyección de macros predefinidas y personalizadas a un archivo de instalación desatendida. Para obtener más información acerca de las macros predefinidos disponibles, consulte Macros predefinidas.

Para agregar el archivo de instalación desatendida predefinido con el archivo de valores de configuración personalizado, complete estos pasos.

1. En la pestaña **Archivos de instalación desatendida**, seleccione el archivo de instalación desatendida personalizada (por ejemplo, `ESXi_locale_customUnattend.cfg`).
2. Haga clic en el icono **Asociar un archivo de configuración** () para mostrar el cuadro de diálogo Asociar un archivo de instalación desatendida.
3. Seleccione el archivo de valores de configuración para asociar con el archivo de instalación desatendida (por ejemplo, `ESXi_locale_customConfig`).
4. Seleccione **Personalizada** desde la lista desplegable **Macros disponibles**.
5. Agregue la macro personalizada para especificar la configuración regional de teclado colocando el cursor entre las comillas después de teclado y luego haciendo clic en **keyboard_locale**.

   Por ejemplo:

   ```
   # Set the keyboard locale
   keyboard '#keyboard_locale#'
   ```
6. Agregue la macro personalizada para especificar el identificador del segundo usuario colocando el cursor en cada ubicación donde desea añadir el Id. de usuario y luego haciendo clic en **second_user_id**. En el archivo de ejemplo, reemplace cada vez instancia de *<user_id>* con la macro personalizada.

   Por ejemplo:

   ```
   #Create second user
   /usr/lib/vmware/auth/bin/adduser -D -h /tmp #second_user_id#
   echo <password> | /usr/lib/vmware/auth/bin/passwd #second_user_id# --stdin
   /bin/vim-cmd vimsvc/auth/entity_permission_add vim.Folder:ha-folder-root #second_user_id# false Admin true
   ```
7. Agregue la macro personalizada para especificar la contraseña del segundo usuario colocando el cursor en la ubicación donde desea añadir la contraseña de usuario y luego haciendo clic en **second_user_password**. En el archivo de ejemplo, reemplace *<password>* con la macro personalizada.

   Por ejemplo:

   ```
   #Create second user
   /usr/lib/vmware/auth/bin/adduser -D -h /tmp #second_user_id#
   echo #second_user_password# | /usr/lib/vmware/auth/bin/passwd #second_user_id# --stdin
   /bin/vim-cmd vimsvc/auth/entity_permission_add vim.Folder:ha-folder-root #second_user_id# false Admin true
   ```
8. Haga clic en **Asociar** para vincular los archivos y guardar los cambios en el archivo de instalación desatendida.

Paso 5. Cree un perfil de imagen de SO personalizado que incluya los valores de configuración y de instalación desatendida personalizados. Para obtener más información, consulte Creación de un perfil de imagen de SO personalizado.

1. Haga clic en la pestaña **Imágenes del SO**.
2. Seleccione un perfil de imagen de SO a personalizar (por ejemplo, `Virtualization`).
3. Haga clic en el icono **Crear** () para abrir el cuadro de diálogo Crear perfil personalizado.
4. En la pestaña **General**:
   a. Introduzca un nombre para el perfil (por ejemplo, `ESXi personalizada usando configuración regional y credenciales de segundo usuario`).
   b. Utilice el valor predeterminado para el campo **Datos personalizados y ruta de archivo**.
   c. Seleccione **Archivos de instalación desatendida y de valores de configuración asociados** para el tipo de personalización.
   d. Haga clic en **Siguiente**.
5. En la pestaña **Archivos de instalación desatendida**, seleccione el archivo de instalación desatendida a importar (por ejemplo, `ESXi_locale_customUnattend.cfg`) y haga clic en **Siguiente**.

   El archivo de valores de configuración asociado se selecciona automáticamente.
6. En la pestaña **Resumen**, revise los valores.
7. Haga clic en **Personalizar** para crear el perfil de imagen del SO personalizado.

Paso 6. Despliegue el perfil de imagen de SO personalizado en el servidor de destino. Para obtener más información, consulte Despliegue de la imagen de un sistema operativo.

1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Desplegar imágenes de SO** para mostrar la página Desplegar sistema operativo: Desplegar imágenes de SO.
2. En cada servidor de destino:
   a. Seleccione el servidor.
   b. Haga clic en **Cambiar selección → Valores de red** y especifique el nombre de host, la dirección IP y los valores de DNS, MTU y VLAN del servidor.

      Consejo:

      - Los valores VLAN están disponibles únicamente cuando el modo VLAN se establece en **Valores globales → Asignación de IP → Usar VLAN**.
      - Los valores de red que especifique en el cuadro de diálogo Valores de red se agregan al archivo desatendido en el tiempo de ejecución usando la macro **#predefined. hostPlatforms.networkConfig#**.

   c. Seleccione el perfil de imagen de SO personalizado (por ejemplo, <*base_OS*>| <*timestamp*>`_ESXi personalizada usando configuración regional y credenciales de segundo usuario`) de la lista desplegable en la columna **Imagen para desplegar**.

      Nota: Asegúrese de que todos los servidores de destino utilicen el mismo perfil personalizado.

   d. (Opcional) Haga clic en el icono **Clave de licencia** () y especifique la clave de licencia que se va a utilizar para activar el sistema operativo una vez instalado.
   e. Seleccione la ubicación de almacenamiento preferida donde desee desplegar la imagen del sistema operativo desde la columna **Almacenamiento**.

      Notas:

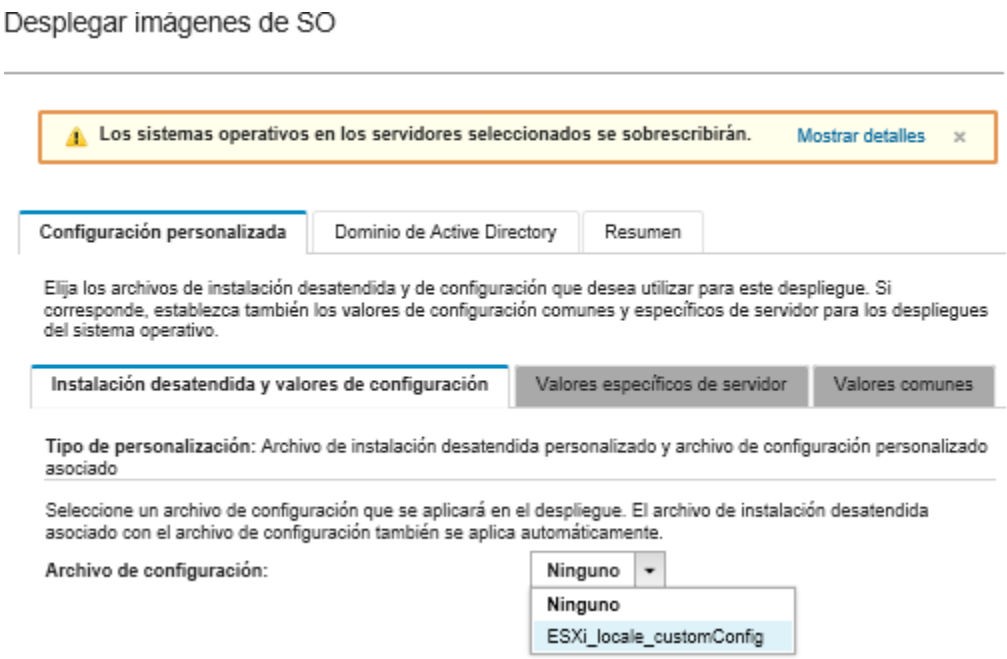
      - Para asegurarse de que los despliegues del sistema operativo sean correctos, desconecte todos los sistemas de almacenamiento del servidor gestionado, a excepción del que haya elegido para el despliegue del sistema operativo.

- Los valores de almacenamiento que especifique en el cuadro de diálogo Valores de almacenamiento se agregan al archivo desatendido en el tiempo de ejecución usando la macro **#predefined.hostPlatforms.storageConfig#**.

f. Compruebe que el estado de despliegue del servidor seleccionado sea **Preparado**.

3. Seleccione todos los servidores de destino y haga clic en el icono **Desplegar imagen** ( ) para iniciar el despliegue del sistema operativo.
4. En la pestaña **Configuración personalizada**, haga clic en la subpestaña **Valores de instalación desatendida** y de configuración y seleccione el archivo de valores de configuración personalizada (por ejemplo, `ESXi_locale_customConfig`).

   Nota: El archivo de instalación desatendida personalizado asociado se selecciona automáticamente.



5. En la subpestaña **Valores específicos del servidor**, seleccione el servidor de destino, la configuración regional de sistema operativo y las credenciales para segundo usuario de ESXi.
6. En la pestaña **Resumen**, revise los valores.
7. Haga clic en **Desplegar** para desplegar el sistema operativo.

Despliegue de Windows 2016 con características personalizadas

En este caso se instala el sistema operativo de Windows 2016 y varias funciones adicionales. Se utiliza un perfil personalizado que incluye un archivo de instalación desatendida. Después de esto, el perfil personalizado se puede seleccionar en la página Desplegar imágenes de SO.

Antes de empezar

Este escenario utiliza los siguientes archivos de muestra.

- Windows_installFeatures_customUnattend.xml. Este archivo de instalación desatendida personalizado instala las funciones WindowsMediaPlayer y BitLocker y utiliza macros predefinidos para valores dinámicos.

Procedimiento

Para desplegar Windows 2016 con funciones personalizadas, lleve a cabo los pasos siguientes.

Paso 1. Descargue el sistema operativo Windows 2016 en japonés en el sistema local e importe la imagen en el repositorio de imágenes de SO. Para obtener más información, consulte Importación de imágenes del sistema operativo.

1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Gestionar imágenes de SO** para mostrar la página Desplegar sistema operativo: Gestionar imágenes de SO.
2. Haga clic en la pestaña **Imágenes del SO**.
3. Haga clic en el icono **Importar** ().
4. Haga clic en **Importación local**.
5. Haga clic en **Examinar** para buscar y seleccionar la imagen de SO que desee importar (por ejemplo, `ja_windows_server_2016_x64_dvd_9720230.iso`).
6. Haga clic en **Importar** para cargar la imagen al repositorio de imágenes de SO.
7. Espere a que se complete la importación. Esto puede tardar varios minutos.

Paso 2. Descargue el archivo de paquete para Windows 2016 en el sistema local e importe la imagen en el repositorio de imágenes del SO. Para obtener más información, consulte Importación de controladores de dispositivos.

El archivo de paquete contiene los controladores de dispositivo más recientes y archivos de arranque de WinPE que se pueden agregar a los perfiles de imágenes del SO personalizados. En este caso se utiliza un archivo de arranque personalizado, por lo que no se utilizará el archivo de arranque del paquete.

1. Haga clic en la pestaña **Archivos de controlador**.
2. Haga clic en **Descargas → Archivos de paquete de Windows** para ir a la página Web del soporte de Lenovo y descargar el archivo de paquete de Windows 2016 en el sistema local.
3. Haga clic en el icono **Importar** ().
4. Haga clic en **Importación local**.
5. Haga clic en **Examinar** para buscar y seleccionar la imagen del SO que desee importar (por ejemplo, `bundle_win2016_20180126130051.zip`).
6. Haga clic en **Importar** para cargar el archivo al repositorio de imágenes de SO.
7. Espere a que se complete la importación. Esto puede tardar varios minutos.

Paso 3. Modifique el archivo de instalación desatendida de Windows para instalar funciones adicionales (como WindowsMediaPlayer y BitLocker) e importar el archivo personalizado en el repositorio de imágenes del SO.

En la sección “Reparación” del archivo de instalación desatendida de Windows, añada las funciones de Windows que desea instalar, por ejemplo

```
<servicing>
   <package action="configure">
      <assemblyIdentity name="Microsoft-Windows-Foundation-Package" version="10.0.14393.0"
                        processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
                        language=""></assemblyIdentity>
      <selection name="Microsoft-Hyper-V" state="true"></selection>
      <selection name="MultipathIo" state="true"></selection>
      <selection name="FailoverCluster-PowerShell" state="true"></selection>
      <selection name="FailoverCluster-FullServer" state="true"></selection>
      <selection name="FailoverCluster-CmdInterface" state="true"></selection>
      <selection name="FailoverCluster-AutomationServer" state="true"></selection>
      <selection name="FailoverCluster-AdminPak" state="true"></selection>
```

```
        <selection name="MicrosoftWindowsPowerShellRoot" state="true"></selection>
        <selection name="MicrosoftWindowsPowerShell" state="true"></selection>
        <selection name="ServerManager-Core-RSAT" state="true"></selection>
        <selection name="WindowsMediaPlayer" state="true"></selection>
        <selection name="BitLocker" state="true"></selection>
    </package>
</servicing>
```

Notas:

- Las etiquetas están en el archivo de instalación desatendida de muestra.
- Cuando se emprende una instalación desatendida personalizada, XClarity Administrator no proporciona varias de las características prácticas comunes que se obtienen cuando se utiliza un archivo de instalación desatendida predefinida. Por ejemplo, los destinos `<DiskConfiguration>`, `<ImageInstall>`, `<ProductKey>` y `<UserAccounts>` para administrador, `<Interfaces>` para redes y la lista `<package>` de características de instalación se deben especificar en el archivo de instalación desatendida personalizada que se está cargando.

Para importar el archivo de instalación personalizada y desatendida, lleve a cabo estos pasos. Para obtener más información, consulte el apartado Importación de archivos de instalación desatendida personalizados.

1. Haga clic en la pestaña **Archivos de instalación desatendida**.
2. Haga clic en el icono **Importar** ().
3. Haga clic en **Importación local**.
4. Seleccione `Windows` para el sistema operativo.
5. Haga clic en **Examinar** para buscar y seleccionar el archivo de instalación desatendida personalizado (por ejemplo, `Windows_installFeatures_customUnattend.xml`).
6. Haga clic en **Importar** para cargar el archivo al repositorio de imágenes de SO.

XClarity Administrator ofrece algunas macros prácticas de nivel básico, como la inserción de controladores OOB, informes de estado, scripts posteriores a la instalación y software personalizado. Sin embargo, para aprovechar estas macros predefinidas, debe especificar las siguientes macros en el archivo desatendido personalizado.

- `#predefined.unattendSettings.preinstallConfig#`
- `#predefined.unattendSettings.postinstallConfig#`

El archivo de muestra ya contiene el código para instalar las funciones adicionales, los macros requeridos y otras macros que se necesitan para la entrada dinámica. Para obtener más información acerca de cómo agregar macros a archivos de instalación desatendida, consulte Inyección de macros predefinidas y personalizadas a un archivo de instalación desatendida.

Para obtener más información acerca de las macros predefinidos disponibles, consulte Macros predefinidas.

Paso 4. Cree un perfil de imagen del SO personalizado que incluya el archivo de instalación desatendida. Para obtener más información, consulte Creación de un perfil de imagen de SO personalizado.

1. Haga clic en la pestaña **Imágenes del SO**.
2. Seleccione el perfil a personalizar (por ejemplo, `win2016-x86_64-install-Datacenter_Virtualization`).
3. Haga clic en el icono **Crear** () para abrir el cuadro de diálogo Crear perfil personalizado.
4. En la pestaña **General**:

a. Introduzca un nombre para el perfil (por ejemplo: `Windows personalizado con características`).
b. Utilice el valor predeterminado para el campo **Datos personalizados y ruta de archivo**.
c. Seleccione **Solo archivos de instalación desatendida** en el tipo de personalización.
d. Haga clic en **Siguiente**.

5. En la pestaña **Opciones de controlador**, haga clic en **Siguiente**. De forma predeterminada, se incluyen los controladores de dispositivo de entrada.
6. En la pestaña **Opciones de arranque** y haga clic en **Siguiente**. El archivo de arranque WinPE predefinido se selecciona de forma predeterminada.
7. En la pestaña **Software**, haga clic en **Siguiente**.
8. En la pestaña **Archivos de instalación desatendida**, seleccione el archivo de instalación desatendida personalizado (por ejemplo, `Windows_installFeatures_customUnattend.xml`) y haga clic en **Siguiente**.
9. En la pestaña **Scripts de instalación**, haga clic en **Siguiente**.
10. En la pestaña **Resumen**, revise los valores.
11. Haga clic en **Personalizar** para crear el perfil de imagen del SO personalizado

Paso 5. Despliegue el perfil de imagen de SO personalizado en los servidores de destino. Para obtener más información, consulte Despliegue de la imagen de un sistema operativo.

1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Desplegar imágenes de SO** para mostrar la página Desplegar sistema operativo: Desplegar imágenes de SO.
2. En cada servidor de destino:
   a. Seleccione el servidor.
   b. Haga clic en **Cambiar selección → Valores de red** y especifique el nombre de host, la dirección IP, la máscara de subred, la puerta de enlace y los valores de DNS, MTU y VLAN del servidor.

      Consejo: los valores VLAN están disponibles únicamente cuando se establece el modo VLAN en **Valores globales → Asignación de IP → Usar VLAN**.
   c. Seleccione el perfil de imagen de SO personalizado (por ejemplo, <*base_OS*>| <*timestamp*>`_Windows personalizado con características`) de la lista desplegable en la columna **Imagen para desplegar**.

      Nota: Asegúrese de que todos los servidores de destino utilicen el mismo perfil personalizado.
   d. (Opcional) Haga clic en el icono **Clave de licencia** () y especifique la clave de licencia que se va a utilizar para activar el sistema operativo una vez instalado.
   e. Seleccione la ubicación de almacenamiento preferida donde desee desplegar la imagen del sistema operativo desde la columna **Almacenamiento**.

      Nota: Para asegurarse de que los despliegues del sistema operativo sean correctos, desconecte todos los sistemas de almacenamiento del servidor gestionado, a excepción del que haya elegido para el despliegue del sistema operativo
   f. Compruebe que el estado de despliegue del servidor seleccionado sea **Preparado**.
3. Seleccione todos los servidores de destino y haga clic en el icono **Desplegar imagen** () para iniciar el despliegue del sistema operativo.

4. En la pestaña **Configuración personalizada**, haga clic en la subpestaña **Valores de instalación desatendida y de configuración** y seleccione el archivo de instalación desatendida personalizada (por ejemplo, `Windows_installFeatures_customUnattend.xml`).
5. (Opcional) En la pestaña **Dominio de Active Directory**, especifique la información necesaria para unir un dominio de Active Directory como parte de un despliegue de imagen de Windows (consulte Integración con Windows Active Directory).
6. En la pestaña **Resumen**, revise los valores.
7. Haga clic en **Desplegar** para desplegar el sistema operativo.

Despliegue de Windows 2016 con software personalizados

En este caso se instala el sistema operativo Windows 2016 junto con software personalizado (Java y Eclipse IDE). Se utiliza un perfil personalizado que incluye el software personalizado y scripts de instalación posterior para instalar y configurar el software personalizado. Los paquetes de software personalizado se copian al host durante el despliegue y se disponen para usarlos en el script de instalación posterior.

Antes de empezar

Este escenario utiliza los siguientes archivos de muestra.

- jre-8u151-windows-x64-with-configfile.zip. Este es el archivo de instalación de Java para Eclipse.
- eclipse-java-oxygen-1a-win32-x86_64.zip Este es el archivo de instalación para Eclipse IDE.
- Windows_installSoftware_customScript.ps1 Este script posterior a la instalación crea un usuario para iniciar Eclipse este script posterior a la instalación e instala IDE Eclipse y Java.

Notas:

- Los scripts de instalación de Windows pueden estar en uno de los siguientes formatos: Archivo de comandos (.cmd), PowerShell (.ps1)
- Los archivos de software y scripts de instalación se instalan en la ruta de datos y archivos personalizada que especifica durante el despliegue. La ruta de datos y archivos personalizados predeterminada es `C:\lxca`.

Procedimiento

Para desplegar Windows 2016 con software personalizados, lleve a cabo los pasos siguientes.

Paso 1. Descargue el sistema operativo Windows 2016 en japonés en el sistema local e importe la imagen en el repositorio de imágenes de SO. Para obtener más información, consulte Importación de imágenes del sistema operativo.

1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Gestionar imágenes de SO** para mostrar la página Desplegar sistema operativo: Gestionar imágenes de SO.
2. Haga clic en la pestaña **Imágenes del SO**.
3. Haga clic en el icono **Importar** ().
4. Haga clic en **Importación local**.
5. Haga clic en **Examinar** para buscar y seleccionar la imagen de SO que desee importar (por ejemplo, `ja_windows_server_2016_x64_dvd_9720230.iso`).
6. Haga clic en **Importar** para cargar la imagen al repositorio de imágenes de SO.
7. Espere a que se complete la importación. Esto puede tardar varios minutos.

Paso 2. Descargue el archivo de paquete para Windows 2016 en el sistema local e importe la imagen en el repositorio de imágenes del SO. Para obtener más información, consulte Importación de controladores de dispositivos.

El archivo de paquete contiene los controladores de dispositivo más recientes y archivos de arranque de WinPE que se pueden agregar a los perfiles de imágenes del SO personalizados. En este caso se utiliza un archivo de arranque personalizado, por lo que no se utilizará el archivo de arranque del paquete.

1. Haga clic en la pestaña **Archivos de controlador**.
2. Haga clic en **Descargas → Archivos de paquete de Windows** para ir a la página Web del soporte de Lenovo y descargar el archivo de paquete de Windows 2016 en el sistema local.
3. Haga clic en el icono **Importar** ().
4. Haga clic en **Importación local**.
5. Haga clic en **Examinar** para buscar y seleccionar la imagen del SO que desee importar (por ejemplo, `bundle_win2016_20180126130051.zip`).
6. Haga clic en **Importar** para cargar el archivo al repositorio de imágenes de SO.
7. Espere a que se complete la importación. Esto puede tardar varios minutos.

Paso 3. Descargue el software personalizado en el sistema local e importe los archivos al repositorio de imágenes del SO. Para obtener más información, consulte Importación de software personalizado.

1. Haga clic en la pestaña **Software**.
2. Haga clic en el icono **Importar** ().
3. Haga clic en **Importación local**.
4. Seleccione `Windows` para el sistema operativo.
5. Haga clic en **Examinar** para buscar y seleccionar el archivo de valores de configuración a importar (por ejemplo, `jre-8u151-windows-x64-with-configfile.zip`).
6. Haga clic en **Importar** para cargar el archivo al repositorio de imágenes de SO.
7. Haga clic en el icono **Importar** () nuevamente.
8. Haga clic en **Importación local**.
9. Seleccione `Windows` para el sistema operativo.
10. Haga clic en **Examinar** para buscar y seleccionar el archivo de valores de configuración a importar (por ejemplo, `eclipse-java-oxygen-1a-win32-x86_64.zip`).
11. Haga clic en **Importar** para cargar el archivo al repositorio de imágenes de SO.

Paso 4. Cree un código posterior a la instalación personalizado e importe el archivo al repositorio de imágenes del SO.

Añada los comandos para instalar el software, por ejemplo:

```
Write-Output "Install Java..."
Invoke-Command -ScriptBlock
        {#predefined.otherSettings.deployDataAndSoftwareLocation#\jre-8u151-windows-x64.exe
        [INSTALLCFG=#predefined.otherSettings.deployDataAndSoftwareLocation#\java_configfile.cfg]
        /s}

Write-Output "Install Eclipse..."
$eclipseDir="C:\Users\Administrator\Desktop\eclipse"
New-Item -ItemType directory -Path $eclipseDir
Expand-Archive -LiteralPath
        "#predefined.otherSettings.deployDataAndSoftwareLocation#\eclipse-java-oxygen-1a-win32-x86_64.zip"
        -DestinationPath $eclipseDir
```

Tenga en cuenta que este comando utiliza la macro predefinida de la ruta de acceso para los datos extraídos y archivos de software (**predefined.otherSettings.deployDataAndSoftwareLocation**).

También puede agregar comandos para enviar mensajes personalizados al registro de trabajos en XClarity Administrator, tal como se muestra en el archivo de muestra. Para obtener más información, consulte el apartado Agregar informes de estado personalizados a los scripts de instalación.

Para importar el script de instalación personalizado, lleve a cabo estos pasos. Para obtener más información, consulte Importación de scripts de instalación personalizada

1. Haga clic en la pestaña **Scripts de instalación**.
2. Haga clic en el icono **Importar** ( ).
3. Haga clic en **Importación local**.
4. Seleccione `Windows` para el sistema operativo.
5. Haga clic en **Examinar** para buscar y seleccionar el archivo de Instalación desatendida a importar (por ejemplo, `Windows_installSoftware_customScript.ps1`).
6. Haga clic en **Importar** para cargar el archivo al repositorio de imágenes de SO.

Paso 5. Cree un perfil de imagen del SO personalizado que incluya el archivo de instalación desatendida personalizado. Para obtener más información, consulte Creación de un perfil de imagen de SO personalizado.

1. Haga clic en la pestaña **Imágenes del SO**.
2. Seleccione un perfil de imagen de SO a personalizar (por ejemplo, `Datacenter virtualization`).
3. Haga clic en el icono **Crear** ( ) para abrir el cuadro de diálogo Crear perfil personalizado.
4. En la pestaña **General**:
   a. Introduzca un nombre para el perfil (por ejemplo: `Windows personalizado con software`).
   b. Utilice el valor predeterminado para el campo **Datos personalizados y ruta de archivo**.
   c. Seleccione **Ninguno** para el tipo de personalización.
   d. Haga clic en **Siguiente**.
5. En la pestaña **Opciones de controlador**, haga clic en **Siguiente**. De forma predeterminada, se incluyen los controladores de dispositivo de entrada.
6. En la pestaña **Opciones de arranque** y haga clic en **Siguiente**. El archivo de arranque WinPE predefinido se selecciona de forma predeterminada.
7. En la pestaña **Software**, seleccione los archivos de instalación del software (por ejemplo `jre-8u151-windows-x64-with-configfile.zip`y `eclipse-java-oxygen-1a-win32-x86_64.zip`) y, a continuación, haga clic en **Siguiente**.
8. En la pestaña **Scripts de instalación**, seleccione los scripts de instalación (por ejemplo, `Windows_installSoftware_customScript.ps1`) y haga clic en **Siguiente**.
9. En la pestaña **Resumen**, revise los valores.
10. Haga clic en **Personalizar** para crear el perfil de imagen del SO personalizado.

Paso 6. Despliegue el perfil de imagen de SO personalizado en los servidores de destino. Para obtener más información, consulte Despliegue de la imagen de un sistema operativo.

1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Desplegar imágenes de SO** para mostrar la página Desplegar sistema operativo: Desplegar imágenes de SO.
2. En cada servidor de destino:
   a. Seleccione el servidor.

b. Haga clic en **Cambiar selección → Valores de red** y especifique el nombre de host, la dirección IP y los valores de DNS, MTU y VLAN del servidor.

   Consejo: los valores VLAN están disponibles únicamente cuando se establece el modo VLAN en **Valores globales → Asignación de IP → Usar VLAN**.

c. Seleccione el perfil de imagen de SO personalizado (por ejemplo, <*base_OS*>| <*timestamp*>_`Windows personalizado con software`) de la lista desplegable en la columna **Imagen para desplegar**.

   Nota: Asegúrese de que todos los servidores de destino utilicen el mismo perfil personalizado.

d. (Opcional) Haga clic en el icono **Clave de licencia** () y especifique la clave de licencia que se va a utilizar para activar el sistema operativo una vez instalado.

e. Seleccione la ubicación de almacenamiento preferida donde desee desplegar la imagen del sistema operativo desde la columna **Almacenamiento**.

   Nota: Para asegurarse de que los despliegues del sistema operativo sean correctos, desconecte todos los sistemas de almacenamiento del servidor gestionado, a excepción del que haya elegido para el despliegue del sistema operativo.

f. Compruebe que el estado de despliegue del servidor seleccionado sea **Preparado**.

3. Seleccione todos los servidores de destino y haga clic en el icono **Desplegar imagen** () para iniciar el despliegue del sistema operativo.
4. En la pestaña **Resumen**, revise los valores.
5. Haga clic en **Desplegar** para desplegar el sistema operativo.

Despliegue de Windows 2016 en japonés

En este escenario se instala el sistema operativo Windows 2016 para varios servidores con japonés habilitado en el teclado y la configuración regional del sistema operativo. Se utiliza un perfil personalizado que incluye archivos personalizados de arranque y de instalación desatendida de WinPE. Después de esto, el perfil personalizado se puede seleccionar en la página Desplegar imágenes de SO.

Antes de empezar

Este escenario utiliza los siguientes archivos de muestra.

- `WinPE_64_ja.zip`. Este archivo de arranque de Windows personalizado (WinPE) instala la configuración regional de japonés.
- Windows_locale_customUnattend.xml. Este archivo de instalación desatendida personalizada utiliza el archivo de WinPE para instalar japonés.

Notas: El archivo de instalación desatendida personalizado de ejemplo asume lo siguiente:

- El servidor solo tiene un disco visible (disco 0) y no tiene una partición del sistema en el mismo.
- Se usa el modo de IPv4 estática y se establece una dirección IP estática (que se usa en la sección de instalación desatendida como una macro predefinida).

Procedimiento

Para desplegar Windows 2016 en japonés en servidores de destino con un perfil de SO personalizado, lleve a cabo los pasos siguientes.

Paso 1. Descargue el sistema operativo Windows 2016 en japonés en el sistema local e importe la imagen en el repositorio de imágenes de SO. Para obtener más información, consulte Importación de imágenes del sistema operativo.

1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Gestionar imágenes de SO** para mostrar la página Desplegar sistema operativo: Gestionar imágenes de SO.
2. Haga clic en la pestaña **Imágenes del SO**.
3. Haga clic en el icono **Importar** ().
4. Haga clic en **Importación local**.
5. Haga clic en **Examinar** para buscar y seleccionar la imagen de SO que desee importar (por ejemplo, `ja_windows_server_2016_x64_dvd_9720230.iso`).
6. Haga clic en **Importar** para cargar la imagen al repositorio de imágenes de SO.
7. Espere a que se complete la importación. Esto puede tardar varios minutos.

Paso 2. Descargue el archivo de paquete para Windows 2016 en el sistema local e importe la imagen en el repositorio de imágenes del SO. Para obtener más información, consulte Importación de controladores de dispositivos.

El archivo de paquete contiene los controladores de dispositivo más recientes y archivos de arranque de WinPE que se pueden agregar a los perfiles de imágenes del SO personalizados. En este caso se utiliza un archivo de arranque personalizado, por lo que no se utilizará el archivo de arranque del paquete.

1. Haga clic en la pestaña **Archivos de controlador**.
2. Haga clic en **Descargas → Archivos de paquete de Windows** para ir a la página Web del soporte de Lenovo y descargar el archivo de paquete de Windows 2016 en el sistema local.
3. Haga clic en el icono **Importar** ().
4. Haga clic en **Importación local**.
5. Haga clic en **Examinar** para buscar y seleccionar la imagen del SO que desee importar (por ejemplo, `bundle_win2016_20180126130051.zip`).
6. Haga clic en **Importar** para cargar el archivo al repositorio de imágenes de SO.
7. Espere a que se complete la importación. Esto puede tardar varios minutos.

Paso 3. Cree un archivo de arranque de WinPE personalizado que use la configuración regional japonesa durante la instalación de WinPe e importe el archivo en el repositorio de imágenes del SO.

XClarity Administrator utiliza un archivo de arranque predefinido previo a la instalación de Windows (WinPE) para instalar el sistema operativo Windows. La configuración regional que se utiliza con el archivo predefinido de arranque es inglés (en-US). Si desea cambiar la configuración regional que se utiliza durante la instalación de Windows, puede crear un archivo de arranque personalizado de WinPE con la configuración regional deseada y asignar ese archivo de arranque personalizado a su perfil personalizado.

Para obtener información acerca de cómo insertar configuraciones regionales en WinPE, consulte Windows WinPE: página web de añadido de complementos.

Importante: Si especifica una configuración regional distinta a inglés en el archivo de arranque de WinPE, no cambie la configuración regional del sistema operativo final que se está desplegando. Solo se cambia la configuración regional que se muestra durante la instalación y la configuración de Windows.

Para crear un archivo de arranque de WinPE personalizado que incluya la configuración regional japonesa, lleve a cabo estos pasos. Para obtener más información, consulte el apartado Creación de un archivo de arranque (WinPE).

1. Mediante un Id. de usuario con autoridad de administrador, ejecute el comando “Deployment and Imaging Tools Environment” de Windows ADK. Se muestra una sesión de comando.
2. En la sesión de comando, cámbiese al directorio donde se descargaron los archivos `genimage.cmd` y `starnet.cmd` (por ejemplo, `C:\customwim`).
3. Ejecute el siguiente comando para asegurarse de que el host no contenga imágenes montadas previamente:
   ```
   dism /get-mountedwiminfo
   ```
   Si hay imágenes montadas, ejecute el siguiente comando para desecharlas:
   ```
   dism /unmount-wim /MountDir:C:\<mount_path> /Discard
   ```
4. Si agrega controladores de dispositivos a un perfil de Windows personalizado, copie los archivos originales del controlador de dispositivo, en formato .inf, al sistema del host en el directorio `C:\drivers`.
5. Ejecute el siguiente comando para generar el archivo de arranque, en formato .wim y espere unos minutos para que se complete el comando.
   ```
   genimage.cmd amd64 <ADK_Version>
   ```
   Donde <*ADK_Version*> es uno de los siguientes valores.
   - **8.1**. Para Windows 2012 R2
   - **10**. Para Windows 2016

   Este comando crea el archivo de arranque llamado `C:\WinPE_64\media\Boot\WinPE_64.wim`.
6. Ejecute el siguiente comando para montar el archivo de arranque:
   ```
   DISM /Mount-Image /ImageFile:C:\WinPE_64\media\Boot\WinPE_64.wim /index:1 /MountDir:C:\WinPE_64\mount
   ```
7. Si agrega controladores de dispositivos predefinidos directamente al archivo de arranque, lleve a cabo los pasos siguientes.
   a. Cree la siguiente estructura de directorio, donde <*os_release*> es `2012R2` o `2016`
      ```
      drivers\<os_release>\
      ```
   b. Copie los controladores de dispositivo, en formato .inf, a un directorio dentro de dicha ruta, por ejemplo:
      ```
      drivers\<os_release>\<driver1>\<driver1_files>
      ```
   c. Copie el directorio `drivers` al directorio de montaje, por ejemplo:
      ```
      C:\WinPE_64\mount\drivers
      ```
8. **Opcional:** Personalice el archivo de opciones de arranque con opciones adicionales, como carpetas, archivos, scripts de inicio, paquetes de idioma y aplicaciones. Para obtener más información acerca de la personalización de los archivos de arranque, consulte Sitio web de WinPE: Montaje y personalización.
9. Añada los paquetes de japonés, por ejemplo.
10. Vea los paquetes instalados para asegurarse de que los paquetes japonés específicos estén instalados.
    ```
    Dism /Add-Package /Image:"C:\WinPE_64\mount"
    /PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment
    and Deployment Kit\Windows Preinstallation Environment\amd64\WinPE_OCs\ja-jp\lp.cab"
    /PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
    Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-DismCmdlets_ja-jp.cab"
    /PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
    Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-NetFx_ja-jp.cab"
    /PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
    Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-PowerShell_ja-jp.cab"
    ```

```
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-RNDIS_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-Scripting_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-StorageWMI_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-WDS-Tools_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-WMI_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\WinPE-FontSupport-JA-JP.cab"
```

11. Revise la Configuración internacional en la imagen.
    `Dism /Get-Packages /Image:"C:\WinPE_64\mount"`
12. Desmonte la imagen ejecutando el siguiente comando.
    `DISM /Unmount-Image /MountDir:C:\WinPE_64\mount /commit`
13. Comprima el contenido del directorio `C:\WinPE_64\media` en un archivo zip llamado `WinPE_64_ja.zip`.
14. Importe el archivo .zip a XClarity Administrator (consulte Importar archivos de arranque).
    a. Haga clic en la pestaña **Archivos de arranque**.
    b. Haga clic en el icono **Importar** ().
    c. Haga clic en **Importación local**.
    d. Seleccione `Windows` para el sistema operativo.
    e. Haga clic en **Examinar** para buscar y seleccionar el archivo de arranque personalizada (por ejemplo, `WinPE_64_ja.zip`).
    f. Haga clic en **Importar** para cargar el archivo al repositorio de imágenes de SO.

Paso 4. Modifique el archivo de instalación desatendida de Windows para especificar que el japonés está incluido en la imagen del SO e importe el archivo personalizado en el repositorio de imágenes de SO.

En el paso “windowsPE” de la instalación de Windows, añada japonés como el idioma del sistema operativo y de configuración regional, por ejemplo:

```
<settings pass="windowsPE">
   <component name="Microsoft-Windows-International-Core-WinPE" processorArchitecture="amd64"
              publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
              xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
              xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      <SetupUILanguage>
         <UILanguage>ja-JP</UILanguage>
      </SetupUILanguage>
      <SystemLocale>ja-JP</SystemLocale>
      <UILanguage>ja-JP</UILanguage>
      <UserLocale>ja-JP</UserLocale>
      <InputLocale>0411:00000411</InputLocale>
   </component>
</settings>
```

Nota: Cuando se emprende una instalación desatendida personalizada, XClarity Administrator no proporciona varias de las características prácticas comunes que se obtienen cuando se utiliza un archivo de instalación desatendida predefinida. Por ejemplo, los destinos `<DiskConfiguration>`, `<ImageInstall>`, `<ProductKey>` y `<UserAccounts>` para administrador, `<Interfaces>` para redes y la lista `<package>` de características de instalación se deben especificar en el archivo de instalación desatendida personalizada que se está cargando.

XClarity Administrator ofrece algunas macros prácticas de nivel básico, como la inserción de controladores OOB, informes de estado, scripts posteriores a la instalación, software personalizado. Sin embargo, para aprovechar estas macros predefinidas, debe especificar las siguientes macros en el archivo desatendido personalizado.

- `#predefined.unattendSettings.preinstallConfig#`
- `#predefined.unattendSettings.postinstallConfig#`

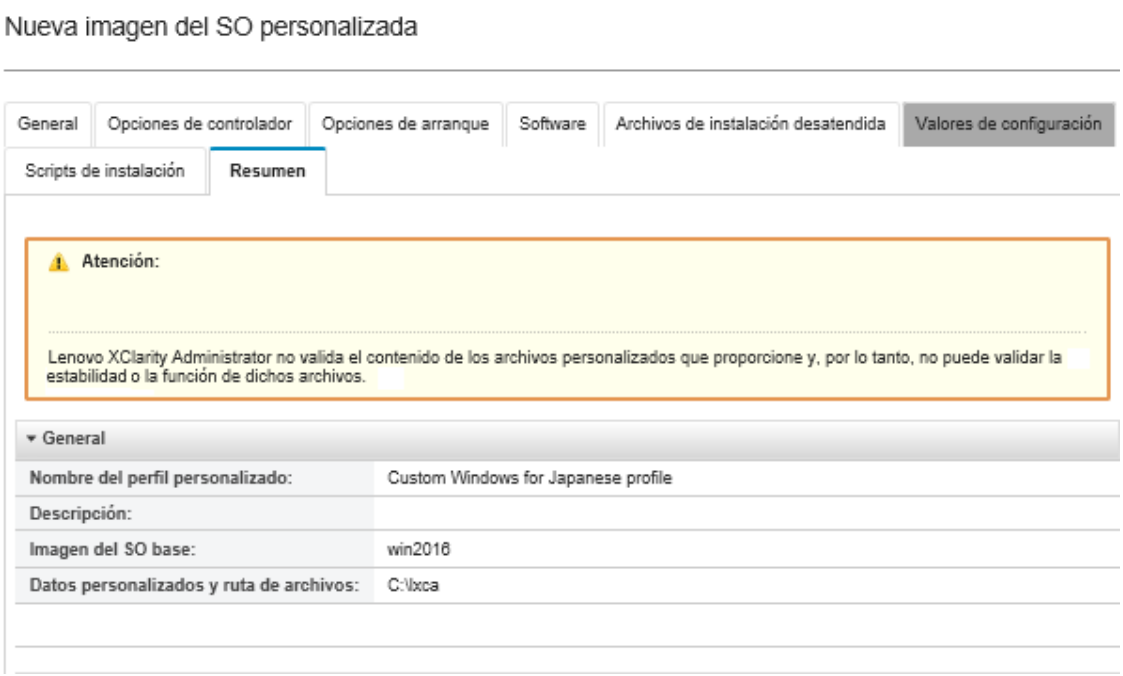
El archivo de ejemplo ya contiene las macros necesarias. Para obtener más información acerca de cómo agregar macros a archivos de instalación desatendida, consulte Inyección de macros predefinidas y personalizadas a un archivo de instalación desatendida. Para obtener más información acerca de las macros predefinidos disponibles, consulte Macros predefinidas.

Para importar el archivo de instalación personalizada y desatendida, lleve a cabo estos pasos. Para obtener más información, consulte el apartado Importación de archivos de instalación desatendida personalizados.

1. Haga clic en la pestaña **Archivos de instalación desatendida**.
2. Haga clic en el icono **Importar** ( ).
3. Haga clic en **Importación local**.
4. Seleccione `Windows` para el sistema operativo.
5. Haga clic en **Examinar** para buscar y seleccionar el archivo de instalación desatendida personalizado (por ejemplo, `Windows_locale_customUnattend.xml`).
6. Haga clic en **Importar** para cargar el archivo al repositorio de imágenes de SO.

Paso 5. Cree un perfil de imagen de SO personalizado incluido en el archivo de arranque personalizado (WinPE) y en el archivo de instalación desatendida. Para obtener más información, consulte Creación de un perfil de imagen de SO personalizado.

1. Haga clic en la pestaña **Imágenes del SO**.
2. Seleccione el perfil a personalizar (por ejemplo, `win2016-x86_64-install-Datacenter_Virtualization`).
3. Haga clic en el icono **Crear** ( ) para abrir el cuadro de diálogo Crear perfil personalizado.
4. En la pestaña **General**:
   a. Introduzca un nombre para el perfil (por ejemplo: `Perfil personalizado de Windows en japonés`).
   b. Utilice el valor predeterminado para el campo **Datos personalizados y ruta de archivo**.
   c. Seleccione **Solo archivos de instalación desatendida** en el tipo de personalización.
   d. Haga clic en **Siguiente**.
5. En la pestaña **Opciones de controlador**, haga clic en **Siguiente**. De forma predeterminada, se incluyen los controladores de dispositivo de entrada.
6. En la pestaña **Archivos de arranque**, seleccione el archivo de arranque personalizado (por ejemplo, `WinPE_64_ja`) y haga clic en **Siguiente**.
7. En la pestaña **Software**, haga clic en **Siguiente**.
8. En la pestaña **Archivos de instalación desatendida**, seleccione el archivo de instalación desatendida personalizado (por ejemplo, `Windows_locale_customUnattend.xml`) y haga clic en **Siguiente**.
9. En la pestaña **Scripts de instalación**, haga clic en **Siguiente**.
10. En la pestaña **Resumen**, revise los valores.



11. Haga clic en **Personalizar** para crear el perfil de imagen del SO personalizado.

Paso 6. Despliegue el perfil de imagen de SO personalizado en los servidores de destino. Para obtener más información, consulte Despliegue de la imagen de un sistema operativo.

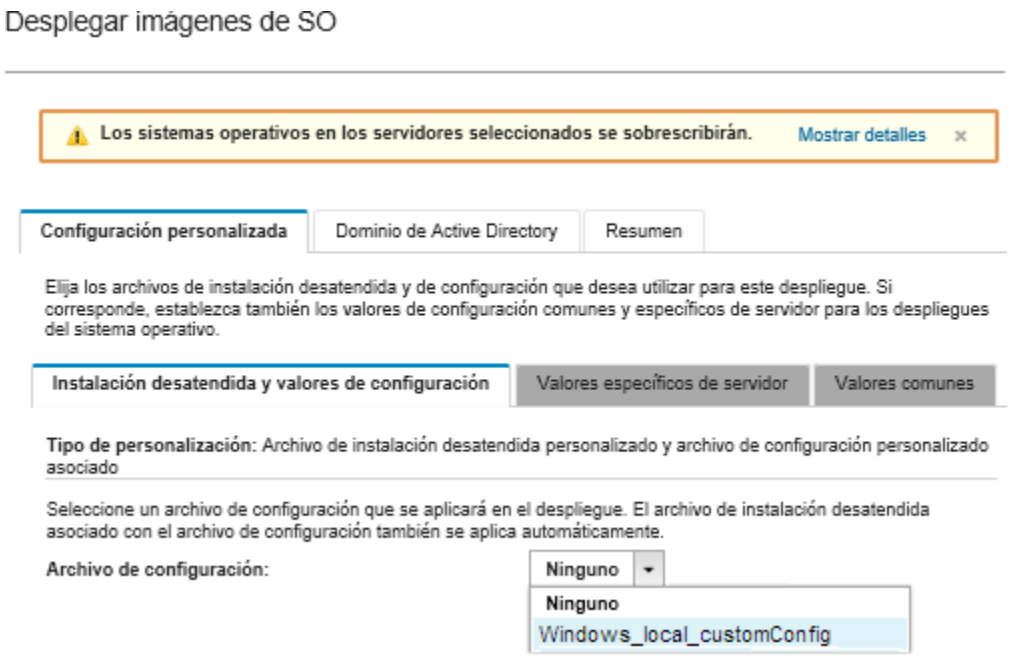
1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Desplegar imágenes de SO** para mostrar la página Desplegar sistema operativo: Desplegar imágenes de SO.
2. En cada servidor de destino:
   a. Seleccione el servidor.
   b. Haga clic en **Cambiar selección → Valores de red** y especifique el nombre de host, la dirección IP, la máscara de subred, la puerta de enlace y los valores de DNS, MTU y VLAN del servidor.

      Consejo: los valores VLAN están disponibles únicamente cuando se establece el modo VLAN en **Valores globales → Asignación de IP → Usar VLAN**.
   c. Seleccione el perfil de imagen de SO personalizado (por ejemplo, <*base_OS*>| <*timestamp*>_`Windows personalizado para el perfil japonés`) de la lista desplegable en la columna **Imagen para desplegar**.

      Nota: Asegúrese de que todos los servidores de destino utilicen el mismo perfil personalizado.
   d. (Opcional) Haga clic en el icono **Clave de licencia** ( ) y especifique la clave de licencia que se va a utilizar para activar el sistema operativo una vez instalado.
   e. Seleccione la ubicación de almacenamiento preferida donde desee desplegar la imagen del sistema operativo desde la columna **Almacenamiento**.

      Nota: Para asegurarse de que los despliegues del sistema operativo sean correctos, desconecte todos los sistemas de almacenamiento del servidor gestionado, a excepción del que haya elegido para el despliegue del sistema operativo.
   f. Compruebe que el estado de despliegue del servidor seleccionado sea **Preparado**.

3. Seleccione todos los servidores de destino y haga clic en el icono **Desplegar imagen** ( ) para iniciar el despliegue del sistema operativo.
4. En la pestaña **Configuración personalizada**, haga clic en la subpestaña **Valores de instalación desatendida y de configuración** y seleccione el archivo de instalación desatendida personalizada (por ejemplo, `Windows_locale_customUnattend.xml`).



5. (Opcional) En la pestaña **Dominio de Active Directory**, especifique la información necesaria para unir un dominio de Active Directory como parte de un despliegue de imagen de Windows (consulte Integración con Windows Active Directory).
6. En la pestaña **Resumen**, revise los valores.
7. Haga clic en **Desplegar** para desplegar el sistema operativo.

   Se muestra el cuadro de diálogo de instalación de Windows en japonés.

Una vez se complete la instalación, la página de inicio de sesión de Windows también se mostrará en japonés.

Capítulo 16. Escenarios integrales para configurar dispositivos nuevos

Utilice estos casos integrales para describir cómo ayudarle a utilizar Lenovo XClarity Administrator para configurar los nuevos dispositivos forma consistente y fácil de repetir.

Despliegue de ESXi en una unidad de disco duro local

Siga estos procedimientos para desplegar VMware ESXi 5.5 en una unidad de disco duro instalada localmente en un Nodo de cálculo Flex System x240. Se ilustra cómo detectar un patrón de servidor de un servidor existente, cómo modificar el patrón de categoría de los valores extendidos de la UEFI para dicho patrón de servidor y cómo instalar VMware ESXi.

VMware ESXi 5.5 requiere que el espacio de E/S asignado a la memoria (MMIO) esté configurado dentro de los 4 GB iniciales del sistema. Dependiendo de la configuración, algunos sistemas tratan de utilizar una memoria superior a 4 GB, lo que puede provocar un error. Para solucionar el problema, puede incrementar el valor de la opción MM Config a 3 GB mediante la Setup Utility de cada servidor en el que se vaya a instalar VMware ESXi 5.5.

Una alternativa consiste en desplegar un patrón de servidor que contenga uno de los patrones de categorías UEFI extendidos y predefinidos relacionados con la virtualización, que establece la opción MM Config y deshabilita la asignación del recurso de 64 bits de la PCI.

Despliegue de un patrón de virtualización predefinido

Un patrón de categoría define valores de firmware específicos que se pueden reutilizar en varios patrones de servidor. Para desplegar un patrón de virtualización predefinido debe crear un patrón de servidor y, a continuación, aplicar un patrón de UEFI extendido predefinido a este patrón de servidor. De este modo el patrón de servidor se podrá aplicar a varios servidores del mismo tipo, como Nodo de cálculo Flex System x240 o Nodo de cálculo Flex System x880 X6.

Acerca de esta tarea

Al crear un patrón de servidor, puede optar por completar la configuración usted mismo o utilizar los atributos de patrón de un servidor existente que ya esté configurado. Al crear un patrón nuevo a partir de un servidor existente, la mayoría de los atributos del patrón ya estarán definidos.

Para obtener más información acerca de los patrones de servidor y los patrones de categorías, consulte Trabajo con patrones de servidor.

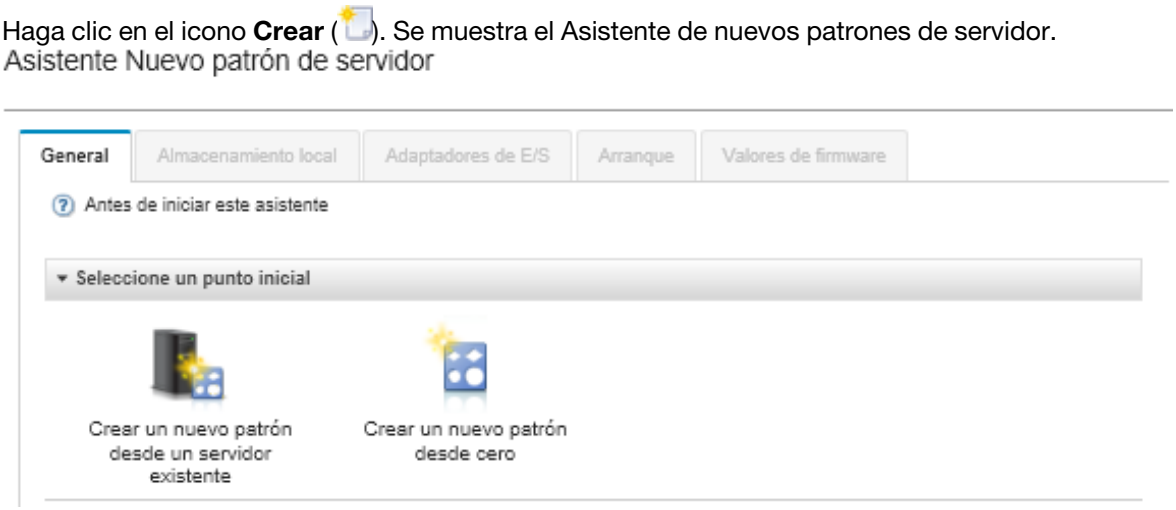
Procedimiento

Para crear un patrón nuevo a partir de un servidor existente, lleve a cabo los pasos siguientes.

Paso 1. En la barra de menús de XClarity Administrator, haga clic en **Aprovisionamiento → Patrones**. Se muestra la página Patrones de configuración: Patrones.

Paso 2. Haga clic en la pestaña **Patrones de servidor**.

Paso 3. Haga clic en el icono **Crear** ( ). Se muestra el Asistente de nuevos patrones de servidor.



Paso 4. Haga clic en **Crear un nuevo patrón desde un servidor existente**. Puede optar por crear un patrón desde cero, aunque normalmente es más eficaz crear un patrón a partir de un servidor existente que tenga la configuración deseada.

Cuando se crea un patrón de servidor desde un servidor existente, XClarity Administrator extrae los valores de un servidor gestionado (incluidos los valores del puerto extendidos, el UEFI y el controlador de gestión de la placa base) y crea patrones de categorías de forma dinámica para dichos valores. Si el servidor es nuevo, XClarity Administrator extrae los valores de fabricación. Si el servidor está en uso, XClarity Administrator extrae los valores personalizados. A continuación, puede modificar los valores específicos del servidor en el que se va a desplegar este patrón.

Paso 5. Seleccione el servidor para utilizarlo como configuración base a la hora de crear el patrón.

Nota: recuerde que el servidor que elija debe ser del mismo modelo que los servidores en los que tiene pensado desplegar el patrón de servidor. Este escenario se basa en seleccionar un Nodo de cálculo Flex System x240.

Paso 6. Introduzca el nombre del patrón nuevo y proporcione una descripción.

Por ejemplo:

- Nombre: **x240_ESXi_deployment**
- Descripción: **Patrón con valores de UEFI extendidos que son adecuados para el despliegue de VMware ESXi**.

Paso 7. Haga clic en **Siguiente** para cargar la información del servidor seleccionado.

Paso 8. En la pestaña **Almacenamiento local**, seleccione **Especificar configuración de almacenamiento** y elija uno de los tipos de almacenamiento. A continuación, haga clic en **Siguiente**.

Para obtener más información acerca de los valores de almacenamiento local, consulte Definición de almacenamiento local.

Paso 9. En la pestaña **Adaptadores de E/S**, introduzca la información relativa a los adaptadores que están en los servidores donde pretende instalar VMware ESXi.

Se mostrarán todos los adaptadores que estuvieran presentes en el servidor utilizado como base.

Si todos los Nodos de cálculo Flex System x240 de su instalación tienen los mismos adaptadores, no es necesario que modifique ningún valor en esta pestaña.

Para obtener más información acerca de los valores de los adaptadores de E/S, consulte Definición de adaptadores de E/S.

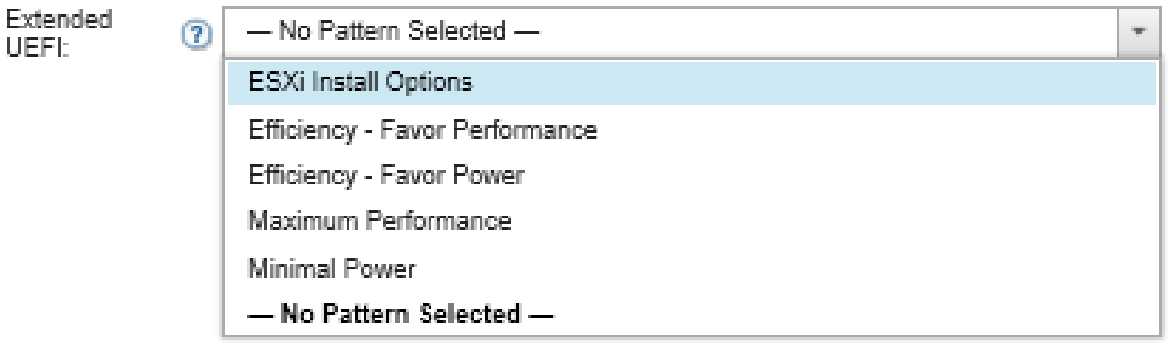
Paso 10. Haga clic en **Siguiente** para continuar.

Paso 11. En la pestaña **Boot**, configure los valores para el entorno de arranque solo heredado y para los entornos de arranque de SAN. A menos que utilice uno de estos entornos, acepte el valor predeterminado de **Arrancar solo UEFI** y, a continuación, haga clic en **Siguiente**.

Para obtener más información acerca de los valores de arranque, consulte Definición de opciones de arranque.

Paso 12. En la pestaña **Valores de firmware**, especifique los valores de firmware de controlador de gestión y UEFI que se van a utilizar para los servidores de destino cuando se despliegue este patrón (por ejemplo, seleccione **Virtualización x240**).

En esta pestaña puede elegir uno de los patrones UEFI extendidos predefinidos:



Para obtener más información acerca de los valores de firmware, consulte Definición de valores de firmware.

Paso 13. Haga clic en **Guardar y desplegar** para guardar el patrón en XClarity Administrator y desplegarlo en los servidores en los que tenga pensado instalar VMware ESXi.

Después de finalizar

Cuando haya desplegado el patrón de servidor en todos los servidores, puede instalar el sistema operativo en esos servidores.

Despliegue de VMware ESXi en un Nodo de cálculo Flex System x240

Utilice este procedimiento como un flujo de ejemplo para ilustrar el proceso de despliegue del sistema operativo ESXi en un Nodo de cálculo Flex System x240.

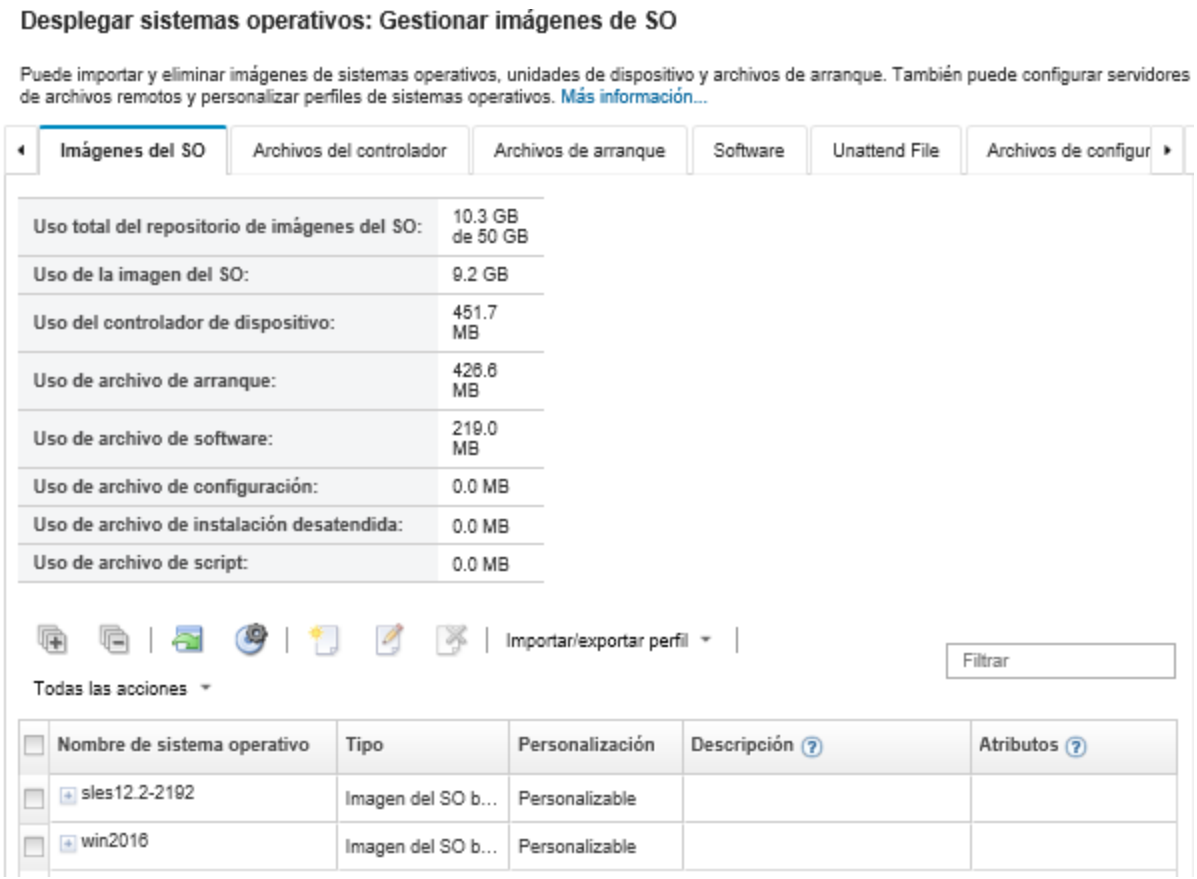
Antes de empezar

Antes de iniciar este procedimiento, asegúrese de que Lenovo XClarity Administrator está gestionando el chasis en el que está instalado Nodo de cálculo Flex System x240.

Procedimiento

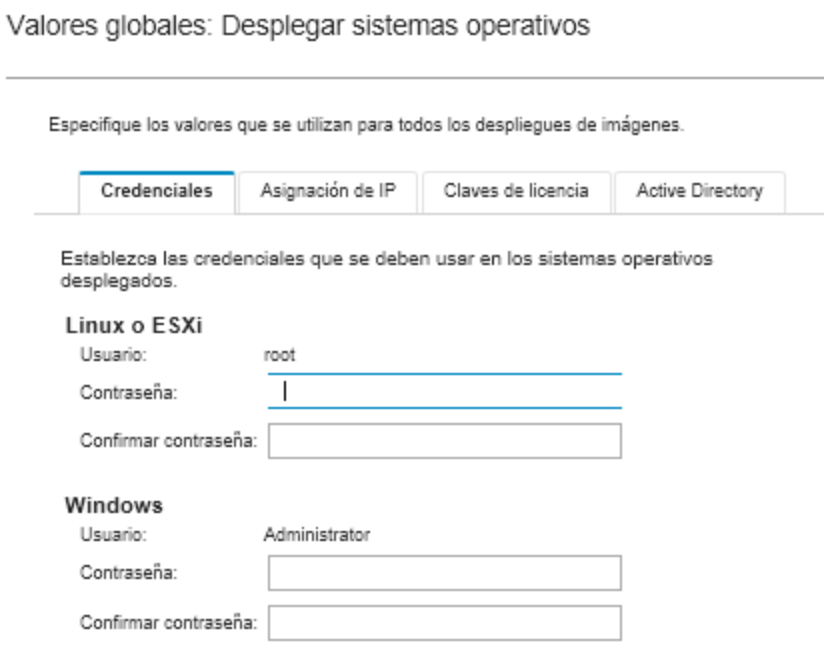
Lleve a cabo los pasos siguientes para desplegar el sistema operativo ESXi en un Nodo de cálculo Flex System x240.

Paso 1. Asegúrese de que la imagen que va a desplegarse ya esté cargada en el Repositorio de imágenes del SO pulsando **Todas las acciones → Gestionar imágenes de SO** para mostrar una lista de todas las imágenes disponibles.



Paso 2. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Aprovisionamiento → Desplegar imágenes de SO**. Aparece la página Desplegar imágenes de SO.

Paso 3. Establezca los valores globales que van a utilizarse como configuración predeterminada para todos los despliegues de imágenes haciendo clic en **Todas las acciones → Valores globales** a fin de mostrar el cuadro de diálogo Valores globales.



a. En la pestaña **Credenciales**, introduzca la contraseña que utilizará la cuenta de administrador para iniciar sesión en el sistema operativo.

b. En la pestaña **Asignación de IP**, especifique cómo se asignará al servidor la dirección IP del sistema operativo.

   Si elige **Utilizar protocolo de configuración de host dinámico** para asignar direcciones IP, la información de la dirección IP no se muestra en el cuadro de diálogo Editar valores de red (consulte el Paso 8 9 en la página 638). Si elige **Asignar dirección IP estática (IPv4)**, puede especificar una dirección IP, una subred y una puerta de enlace para cada despliegue.

c. En la pestaña **Claves de licencia**, introduzca una clave de licencia de activación masiva, si lo desea.

d. Haga clic en **Aceptar** para cerrar el cuadro de diálogo.

Paso 4. Asegúrese de que el servidor esté listo para el despliegue del sistema operativo seleccionando el servidor en el que desee desplegar el sistema operativo. Inicialmente, es estado de despliegue podría mostrarse como No preparado. El estado de despliegue debe estar Preparado antes de que pueda desplegar un sistema operativo en un servidor.

Consejo: puede elegir varios servidores de varios chasis de Flex System si piensa desplegar el mismo sistema operativo en todos los servidores. Puede elegir hasta 28 servidores.

Paso 5. Haga clic en la columna **Imagen para desplegar** y seleccione VMware ESXi 5.5 (**esxi5.5_2.33|esxi5.5_2.33-x86_64-install-Virtualization**).

Paso 6. En esa misma columna, haga clic en el icono **Clave de licencia** ( ) para introducir la clave de licencia para este despliegue.

Consejo: también puede optar por utilizar una clave de activación masiva que haya introducido en el cuadro de diálogo Valores globales.

Paso 7. Asegúrese de que la opción **Disco local** esté seleccionada en la columna Almacenamiento.

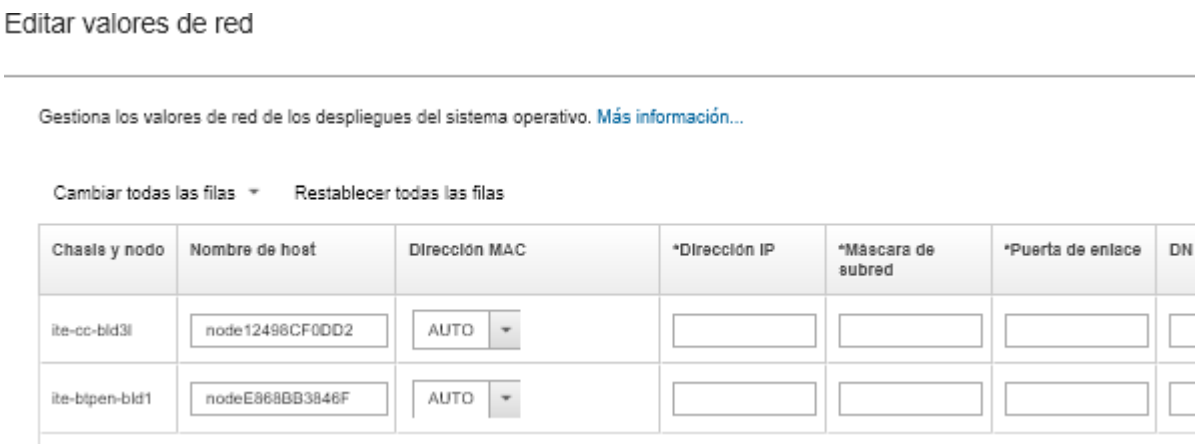
Paso 8. Haga clic en **Editar** en la columna **Valores de red** de la fila del servidor para configurar los valores de red que desee utilizar para este despliegue. Se muestra la página Editar valores de red.

Rellene los campos siguientes:

- Nombre de host
- Dirección MAC del puerto en el host donde va a instalarse el sistema operativo
- Servidores de sistemas de nombres de dominio (DNS), si procede
- Velocidad de la unidad de transmisión máxima (MTU)

Notas: Si elige **Asignar dirección IP estática (IPv4)** en el cuadro de diálogo Valores globales (consulte el Paso 3 4 en la página 636), también debe indicar la información siguiente:

- Dirección IPv4
- Máscara de subred
- Puerta de enlace



Paso 9. Haga clic en **Aceptar** para cerrar el cuadro de diálogo.

En la página Desplegar imágenes de SO, asegúrese de que el servidor muestre Preparado en el área Estado de despliegue.

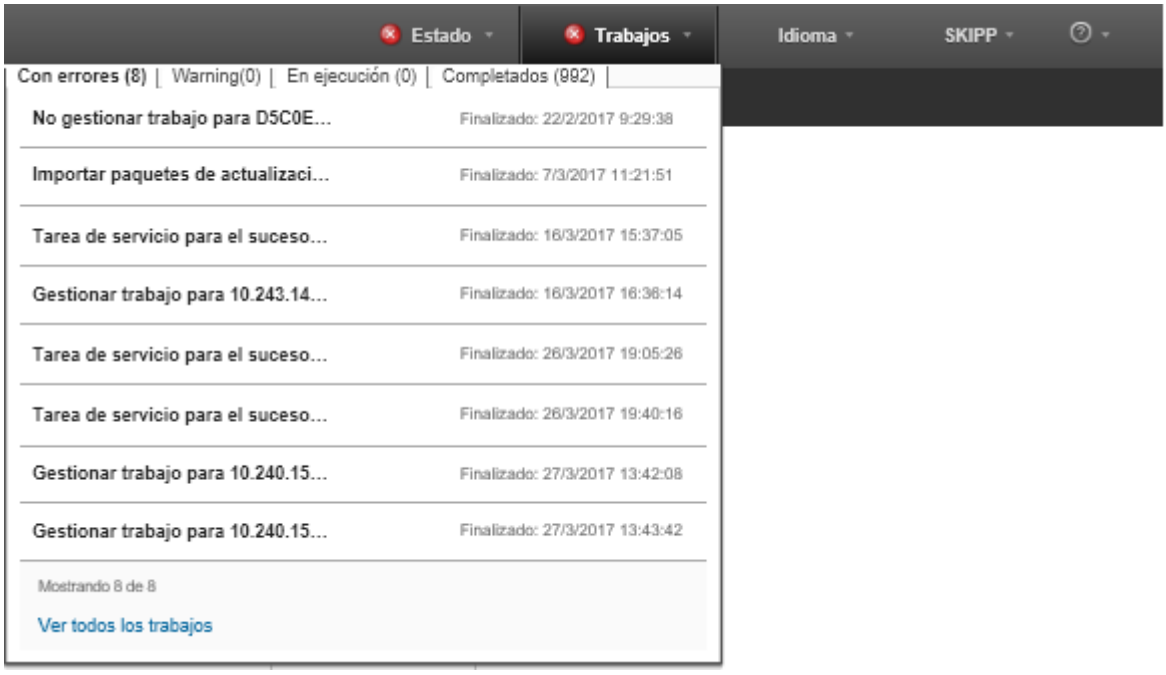
Paso 10. Despliegue el sistema operativo haciendo clic en **Todas las acciones → Desplegar imágenes**.

Paso 11. En la página de confirmación, haga clic en **Desplegar** para desplegar la imagen.

Si el servidor tiene instalado actualmente un sistema operativo, se le advierte del hecho de que al desplegar la imagen se sobrescribirá el sistema operativo actual.

Consejo: puede configurar una sesión de control remoto para ver cómo va progresando la instalación. Haga clic en **Todas las acciones → Control remoto** para iniciar una sesión de control remoto con el servidor.

Cuando despliega el sistema operativo, Lenovo XClarity Administrator inicia un trabajo para hacer un seguimiento del despliegue. Para ver el estado del trabajo de despliegue, haga clic en **Trabajos** en la barra de menús de Lenovo XClarity Administrator. A continuación, haga clic en la pestaña **En ejecución**.

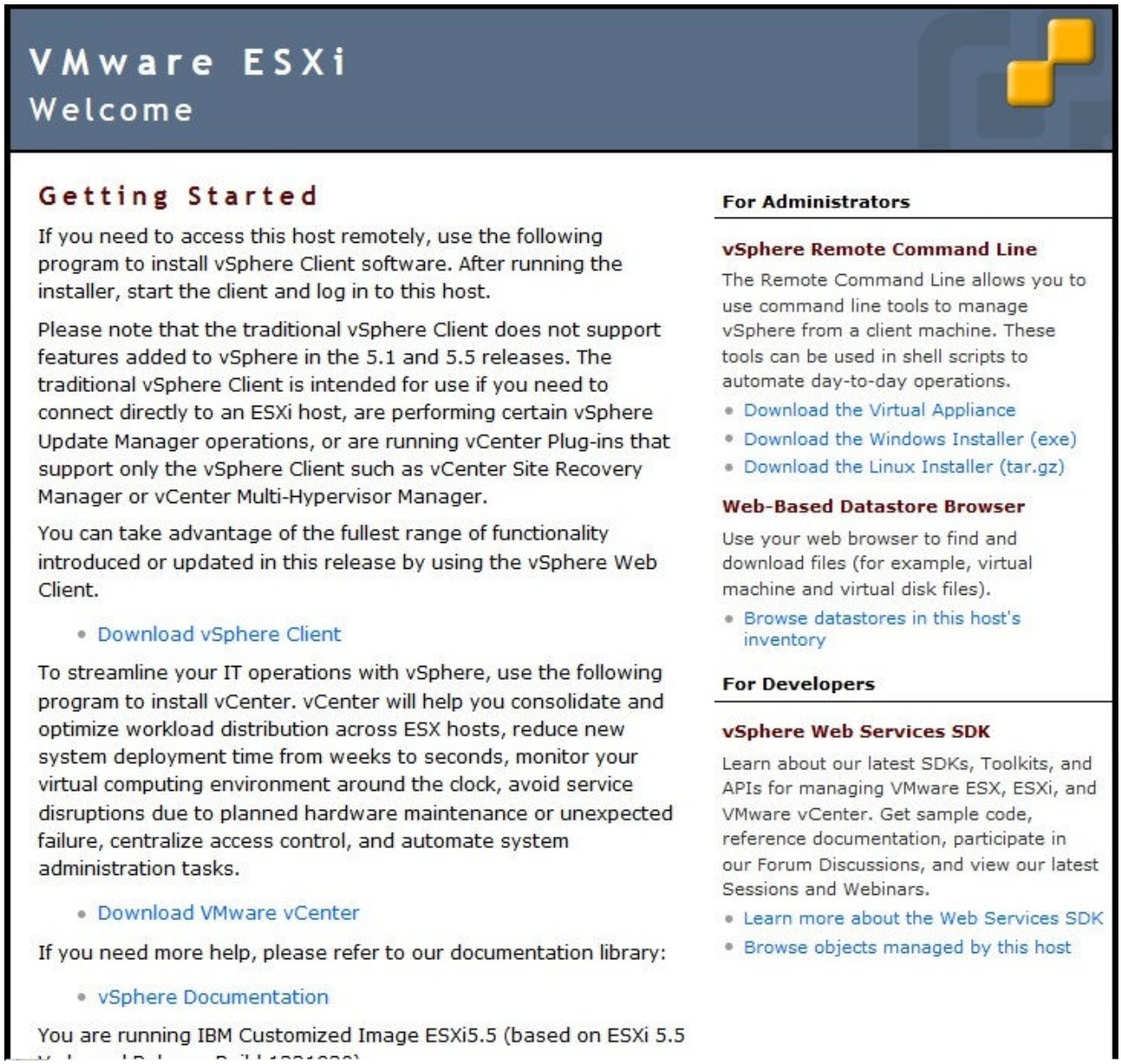


Pase el cursor sobre el trabajo en ejecución para ver los detalles, como el porcentaje del trabajo que está completo.

Resultados

Una vez completado el despliegue del sistema operativo, inicie sesión en la dirección IP que ha especificado en la página Editar valores de red para continuar con el proceso de configuración.

Nota: La licencia proporcionada con la imagen es una prueba gratuita de 60 días. El usuario es el responsable de cumplir todos los requisitos de licencia de VMware.



Despliegue de ESXi en un almacenamiento SAN

Siga estos procedimientos para desplegar VMware ESXi 5.5 en volúmenes SAN anexos a servidores.

Al desplegar un sistema operativo en un SAN, este se despliega en el primer destino de arranque de SAN que se haya configurado mediante un patrón de servidor. Además, no es posible habilitar una unidad de disco duro local en el servidor que se va a arrancar desde SAN. Se debe deshabilitar o quitar si hay una unidad de disco duro.

Despliegue de un patrón de servidor para respaldar el arranque de SAN

Al crear y desplegar un patrón de servidor para respaldar el arranque de un sistema desde SAN, debe asegurarse de identificar el destino de arranque de SAN y los adaptadores que forman parte del servidor.

Procedimiento

Para crear y desplegar un patrón de servidor que respalde el despliegue del sistema operativo en un almacenamiento SAN, lleve a cabo los pasos siguientes.

Paso 1. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Aprovisionamiento → Patrones**. Se muestra la página Patrones de configuración: Patrones.

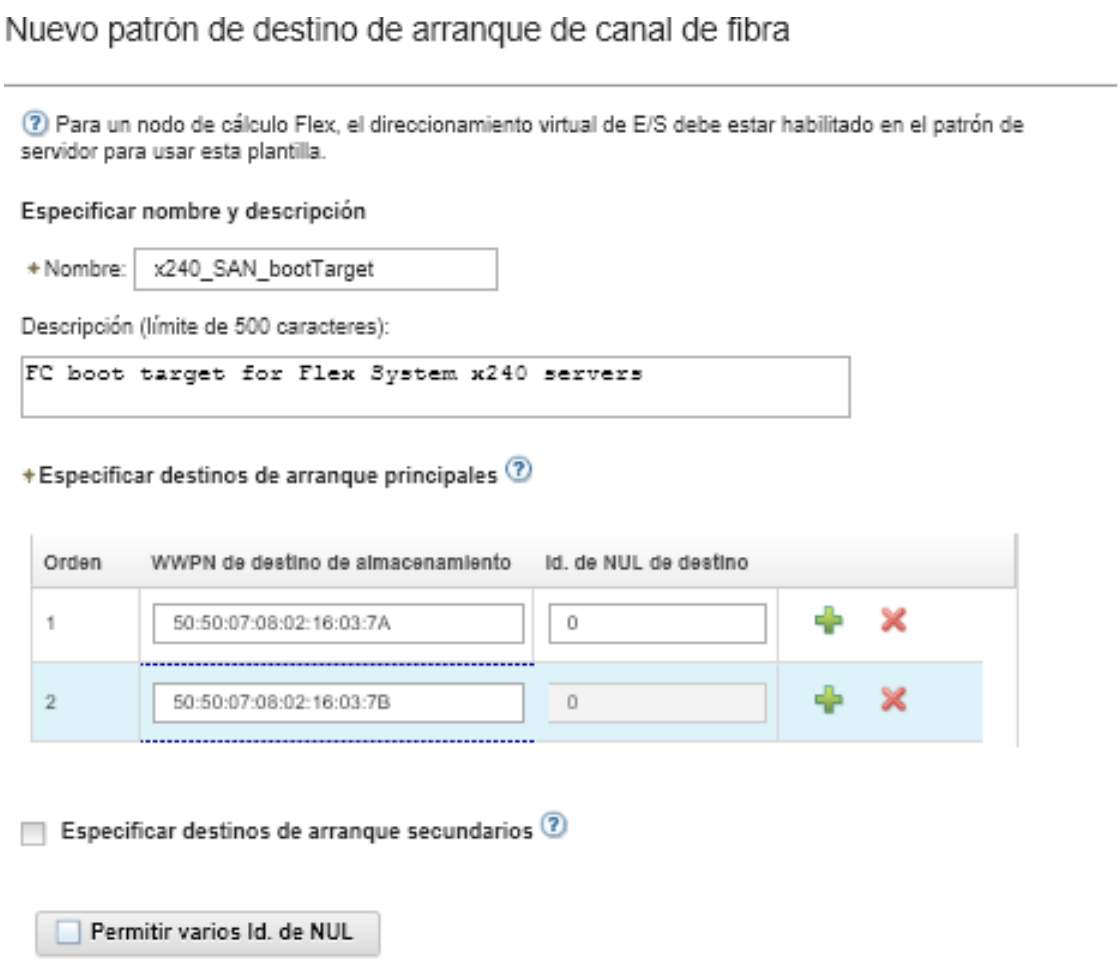
Paso 2. Para identificar los identificadores de WWPN y LUN de los volúmenes de almacenamiento donde debe desplegarse el sistema operativo, cree un patrón de categoría.

a. Haga clic en la pestaña **Patrones de categorías**.

b. Haga clic en **Patrones de destino de arranque de Fibre Channel** y, a continuación, haga clic en el icono **Crear** ( ).

c. Introduzca el WWPN del destino de almacenamiento.

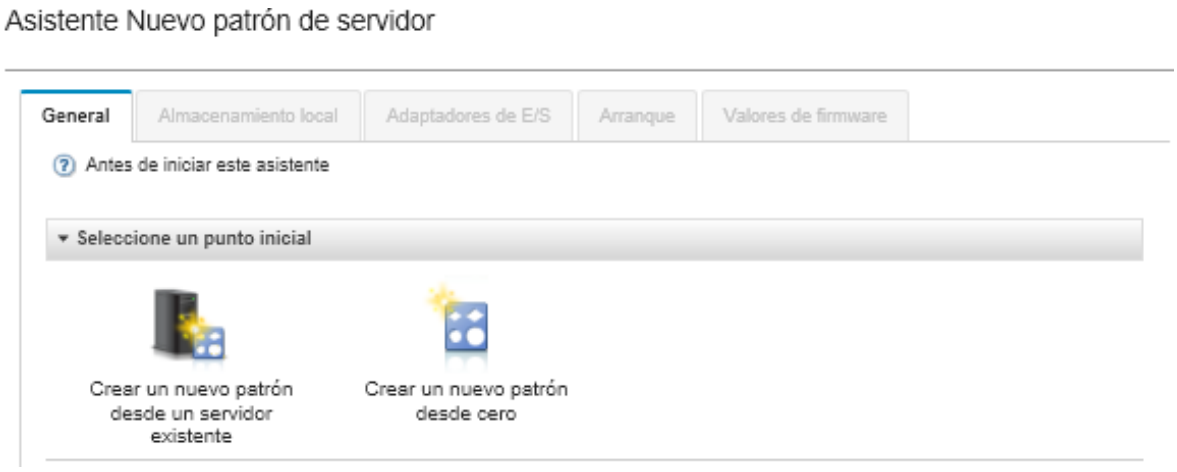
Nota: Haga clic en **Permitir varios identificadores de LUN** para asignar varios identificadores de LUN de destino a los mismos volúmenes de almacenamiento.



d. Haga clic en **Crear** para crear el patrón. El destino se muestra en la lista de Patrones de destino de arranque de Fibre Channel.

Paso 3. Haga clic en la pestaña **Patrones de servidor** para crear un patrón.

Paso 4. Haga clic en el icono **Crear** ( ). Se muestra el Asistente de nuevos patrones de servidor.



Paso 5. Haga clic en **Crear un nuevo patrón desde cero**.

Paso 6. En la pestaña **General**:

- Seleccione **Nodo de cálculo Flex** para el factor de forma.

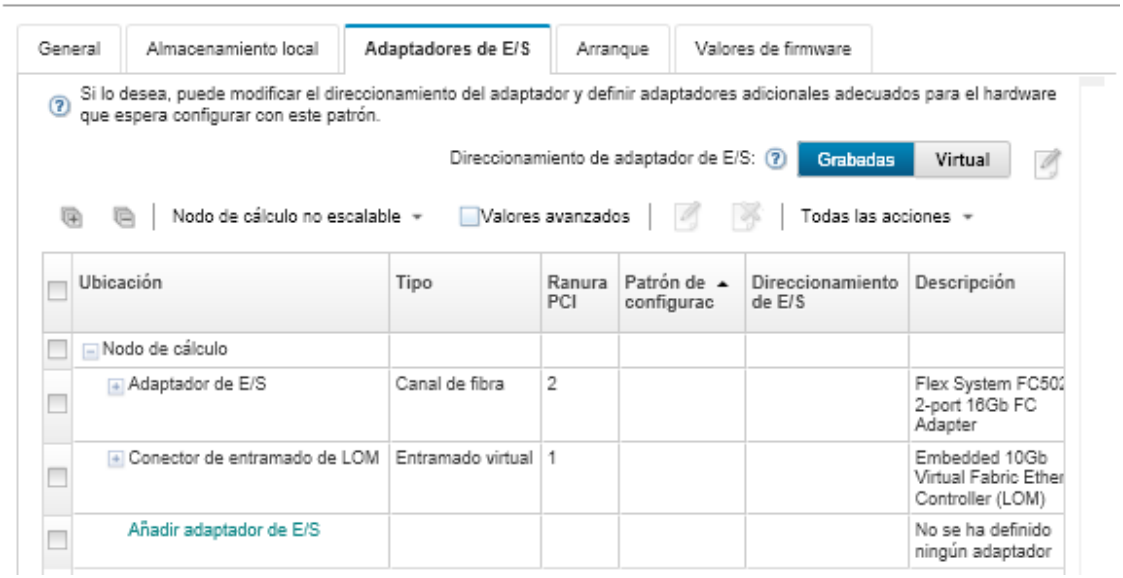
- Especifique el nombre del patrón (**x240_san_boot**) y una descripción.
- Haga clic en **Siguiente**.

Paso 7. En la pestaña **Almacenamiento local**, considere deshabilitar el adaptador de almacenamiento local si está utilizando un sistema sin discos para mejorar los tiempos de arranque del sistema que están relacionados con la búsqueda de las unidades locales. A continuación, haga clic en **Siguiente**.

Paso 8. En la pestaña **Adaptadores de E/S**, añada las tarjetas Ethernet y de Fibre Channel. Asegúrese de que se encuentran en las ranuras PCI adecuadas.

a. Para cada tarjeta, haga clic en **Añadir adaptador de E/S**, elija la ranura de la PCI donde se encuentra la tarjeta y, a continuación, seleccione la tarjeta.

Nota: Asegúrese de especificar una tarjeta Ethernet y una de Fibre Channel.



b. Asegúrese de que el direccionamiento del adaptador de E/S esté establecido en **Virtual**. A continuación, haga clic en el icono **Editar** para especificar la configuración que se va a utilizar para el direccionamiento virtual de Ethernet (MAC) y el direccionamiento virtual de Fibre Channel (WWN).

Nota: en la página Editar direccionamiento virtual puede optar por utilizar la dirección MAC grabada para la tarjeta de Ethernet deshabilitando el direccionamiento virtual. Sin embargo, para seleccionar y utilizar un patrón de destino de arranque de Fibre Channel, debe utilizar el direccionamiento virtual para el adaptador de Fibre Channel.

c. Haga clic en **Siguiente**.

Paso 9. En la pestaña **Boot**, añada el patrón de destino de arranque de SAN que creó anteriormente.

a. En la pestaña **Arranque de SAN**, elija el patrón de destino de arranque que ha definido.

b. Haga clic en **Siguiente**.

Paso 10. En la pestaña **Valores de firmware**, defina los patrones de categorías adicionales que desee incluir en este patrón de servidor. Puede definir los siguientes patrones de categorías.

- **Información del sistema** (consulte Definición de los valores de la información del sistema)
- **Interfaz de gestión** (consulte Definición de los valores de la interfaz de gestión)

- **Dispositivos y puertos de E/S** (consulte Definición de los valores de los dispositivos y puertos de E/S)
- **BMC extendido**. Puede elegir entre los valores del controlador de gestión de la placa base que ha creado anteriormente (consulte Definición de configuración de controlador de gestión extendido).
- **UEFI extendido**. Puede elegir entre los valores predefinidos o los valores de UEFI creados previamente (consulte Definición de los valores extendidos de UEFI).

Paso 11. Haga clic en **Guardar y desplegar** para guardar el patrón en Lenovo XClarity Administrator y desplegarlo en los servidores en los que tenga pensado instalar VMware ESXi.

Después de finalizar

Considere la necesidad de llevar a cabo los pasos siguientes después de desplegar el patrón de servidor en todos los servidores.

1. Tome las direcciones WWPN virtualizadas que se han creado y añádalas a la zona de almacenamiento para que el servidor pueda acceder a las LUN de almacenamiento definidas.

   Consejo: una vez desplegado el perfil de servidor, podrá encontrar las direcciones WWPN virtualizadas consultando dicho perfil.

   a. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Aprovisionamiento → Perfiles de servidor**.

   b. Haga clic en el perfil de servidor desplegado (por ejemplo, **x240_SAN_boot**). En la pestaña **Asignación de dirección virtual** se muestra la lista de direcciones.

2. Despliegue el sistema operativo en el servidor.

Despliegue de VMware ESXi en un almacenamiento SAN

Utilice este procedimiento como un flujo de ejemplo para ilustrar el proceso de despliegue del sistema operativo ESXi en un almacenamiento SAN conectado a un servidor.

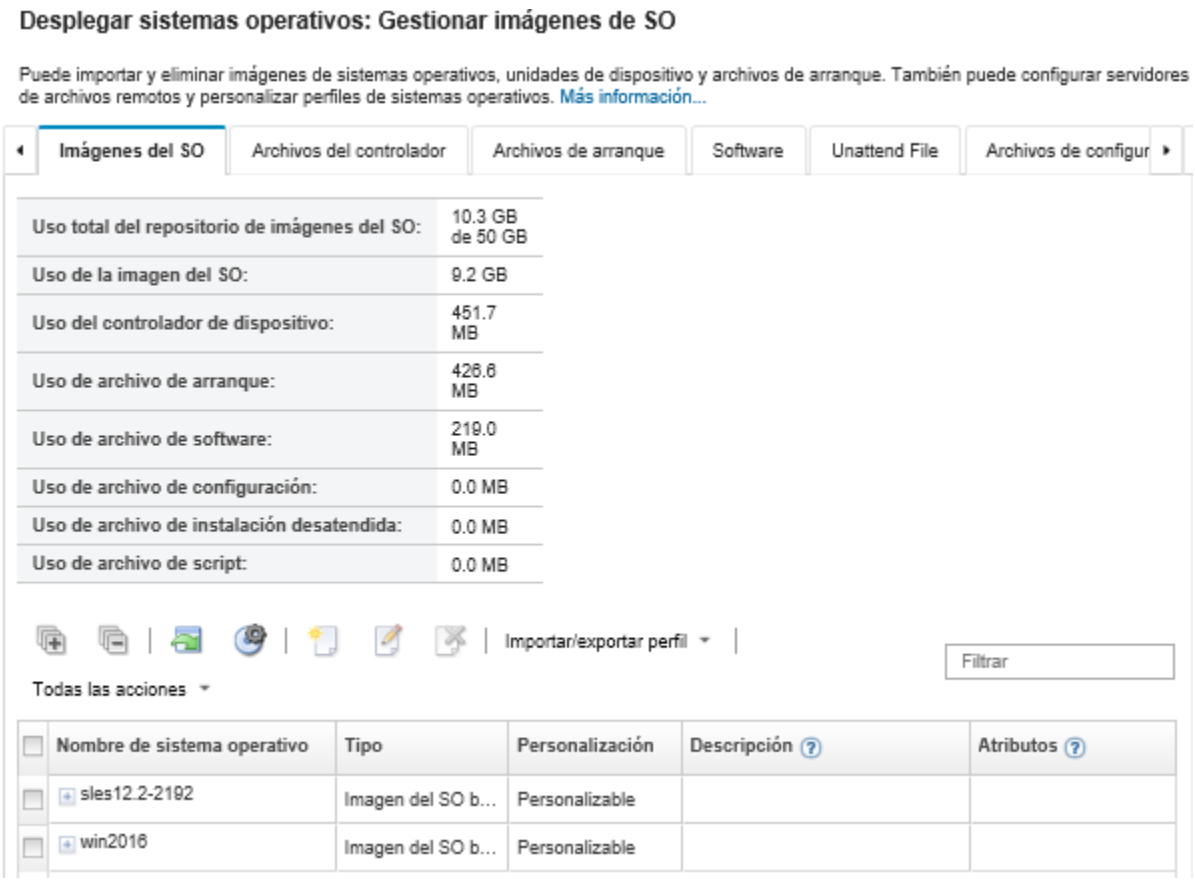
Antes de empezar

Antes de iniciar este procedimiento, asegúrese de que Lenovo XClarity Administrator está gestionando el chasis en el que está instalado Nodo de cálculo Flex System x220.

Procedimiento

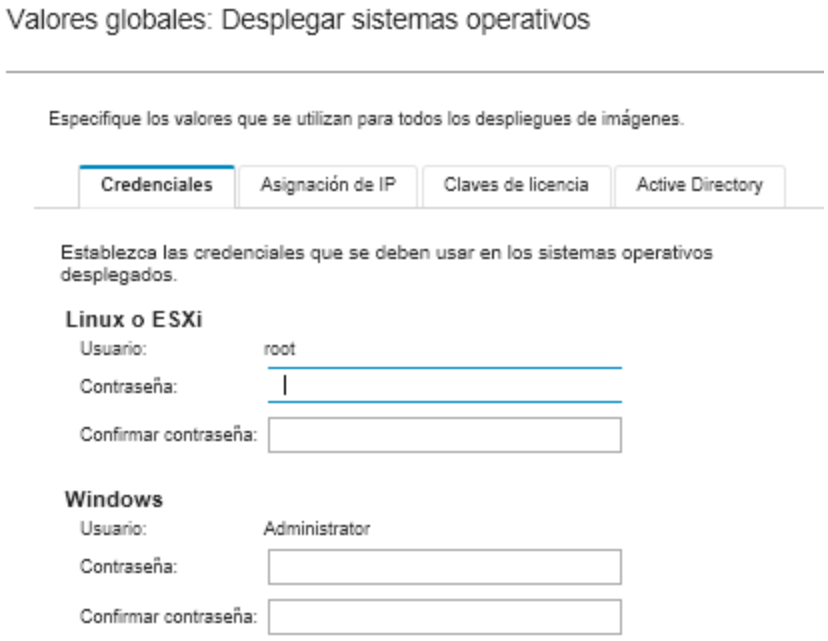
Lleve a cabo los pasos siguientes para desplegar el sistema operativo ESXi en un Nodo de cálculo Flex System x222.

Paso 1. Asegúrese de que la imagen que se va a desplegar ya está cargada en el Repositorio de imágenes del SO pulsando **Todas las acciones → Gestionar imágenes de SO**.



Paso 2. En la barra de menús de Lenovo XClarity Administrator, haga clic en **Aprovisionamiento → Desplegar imágenes de SO**.

Paso 3. Establezca los valores globales que van utilizarse como configuración predeterminada para todos los despliegues de imágenes haciendo clic en **Todas las acciones → Valores globales** a fin de mostrar el cuadro de diálogo Valores globales: Desplegar sistemas operativos.



a. En la pestaña **Credenciales**, introduzca la contraseña que utilizará la cuenta de administrador para iniciar sesión en el sistema operativo.

b. En la pestaña **Asignación** de IP, especifique cómo se asignará al servidor la dirección IP del sistema operativo.

   Si elige **Utilizar protocolo de configuración de host dinámico** para asignar direcciones IP, la información de la dirección IP no se muestra en el cuadro de diálogo Editar valores de red (consulte el Paso 8 9 en la página 647). Si elige **Asignar dirección IP estática (IPv4)**, puede especificar una dirección IP, una subred y una puerta de enlace para cada despliegue.

c. En la pestaña **Claves de licencia**, introduzca una clave de licencia de activación masiva, si lo desea.

d. Haga clic en **Aceptar** para cerrar el cuadro de diálogo.

Paso 4. Asegúrese de que el servidor esté listo para el despliegue del sistema operativo seleccionando el servidor en el que desee desplegar el sistema operativo. Inicialmente, es estado de despliegue podría mostrarse como No preparado. El estado de despliegue debe estar Preparado antes de que pueda desplegar un sistema operativo en un servidor.

Consejo: puede elegir varios servidores de entre varios chasis de Flex System si piensa desplegar el mismo sistema operativo en todos los servidores. Puede elegir hasta 28 servidores.

Paso 5. Haga clic en la columna **Imagen para desplegar** y seleccione VMware ESXi 5.5 (**esxi5.5_2.33| esxi5.5_2.33-x86_64-install-Virtualization**).

Paso 6. En esa misma columna, haga clic en el icono **Clave de licencia** () para introducir la clave de licencia para este despliegue.

Consejo: también puede elegir utilizar una clave de activación masiva que haya introducido en el cuadro de diálogo Valores globales: Desplegar sistemas operativos.

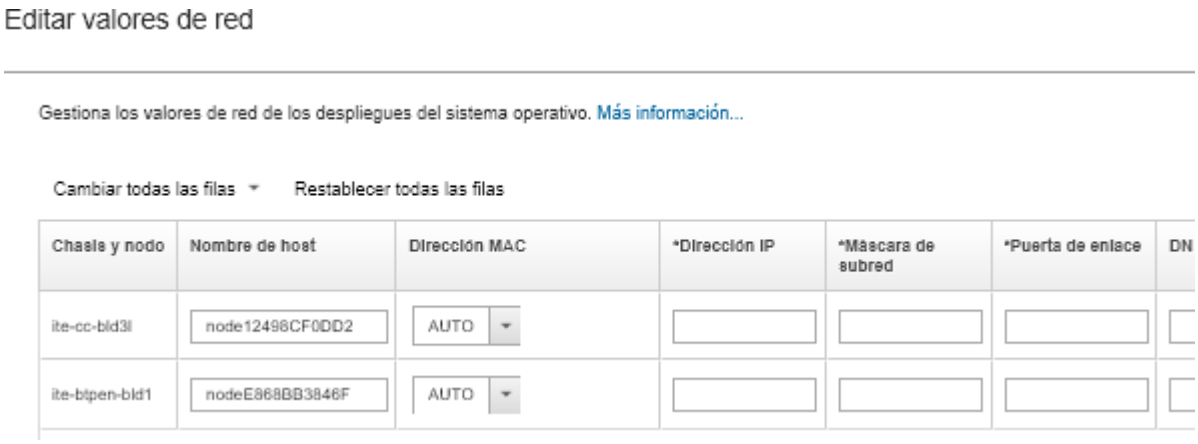
Paso 7. En la columna **Almacenamiento**, seleccione el almacenamiento SAN en el que desee desplegar el sistema operativo.

El almacenamiento aparece como:
`LUN: <LUN VALUE>  WWPN: <WWPN_VALUE>`

Paso 8. Haga clic en **Editar** en la columna **Valores de red** de la fila del servidor para configurar los valores de red que desee utilizar para este despliegue. Se muestra la página Editar valores de red.

Rellene los campos siguientes:
- Nombre de host
- Dirección MAC del puerto en el host donde se instalará el sistema operativo
- Servidores de sistemas de nombres de dominio (DNS), si procede
- Velocidad de la unidad de transmisión máxima (MTU)

Notas: Si ha elegido **Asignar dirección IP estática (IPv4)** en el cuadro de diálogo Valores globales: Desplegar sistemas operativos (Paso 3 4 en la página 645), especifique también la información siguiente:
- Dirección IPv4
- Máscara de subred
- Puerta de enlace



Paso 9. Haga clic en **Aceptar** para cerrar el cuadro de diálogo.

En la página Desplegar imágenes de SO, el servidor debe mostrar ahora el estado de despliegue Preparado.

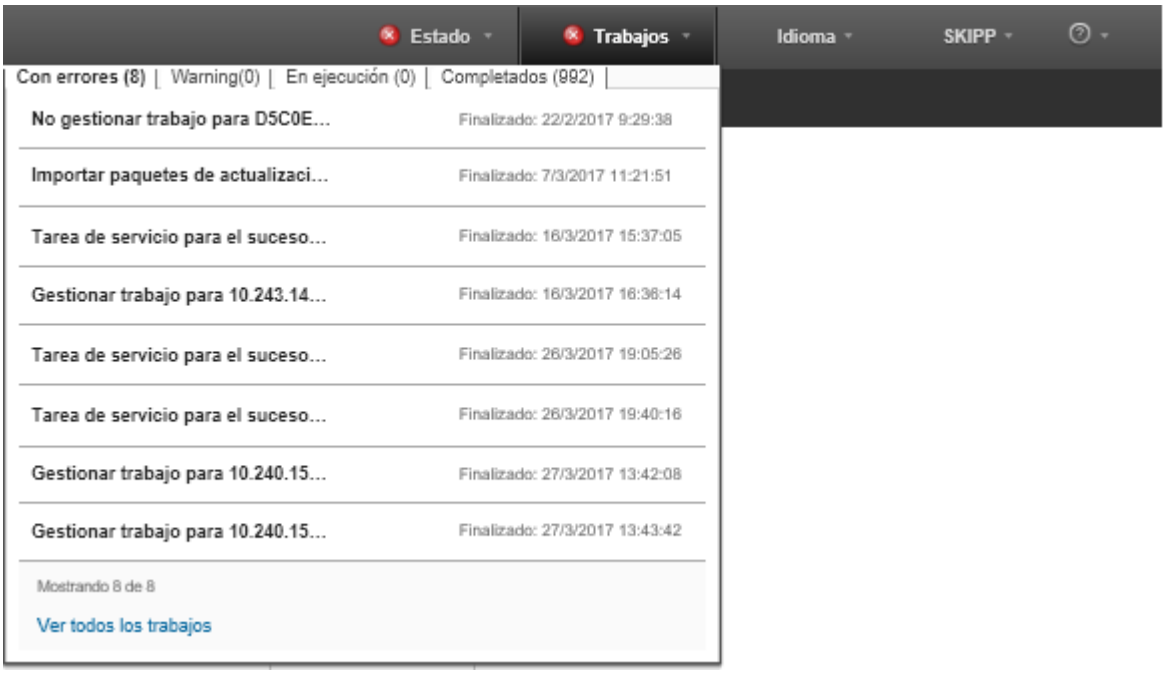
Paso 10. Despliegue el sistema operativo haciendo clic en **Todas las acciones → Desplegar imágenes**.

Paso 11. En la página de confirmación, haga clic en **Desplegar** para desplegar la imagen.

Si el servidor tiene instalado actualmente un sistema operativo, se le advierte del hecho de que al desplegar la imagen se sobrescribirá el sistema operativo actual.

Consejo: puede configurar una sesión de control remoto para ver cómo va progresando la instalación. Haga clic en **Todas las acciones → Control remoto** para iniciar una sesión de control remoto con el servidor.

Cuando despliega el sistema operativo, Lenovo XClarity Administrator inicia un trabajo para hacer un seguimiento del despliegue. Para ver el estado del trabajo de despliegue, haga clic en **Trabajos** en la barra de menús de Lenovo XClarity Administrator. A continuación, haga clic en la pestaña **En ejecución**.

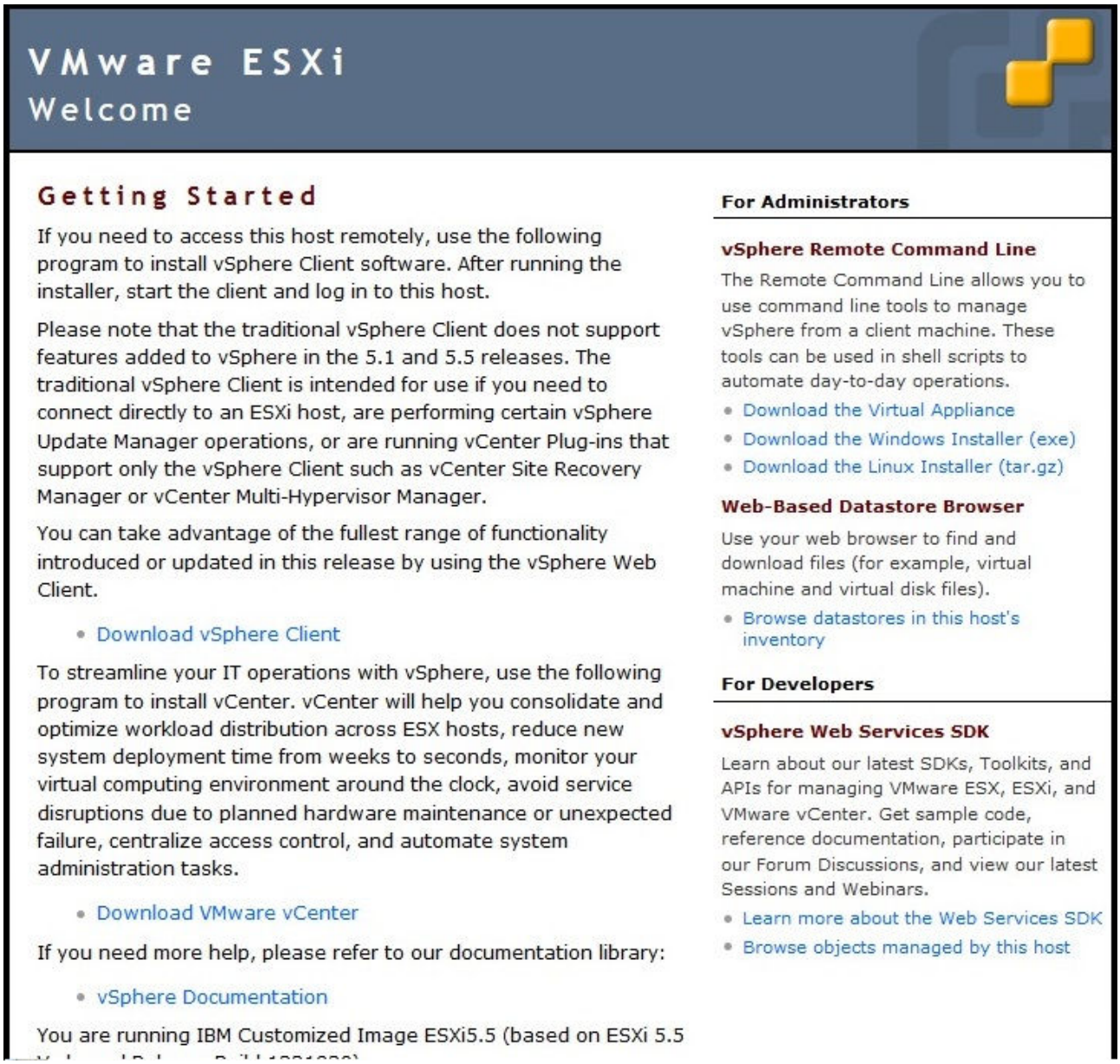


Pase el cursor sobre el trabajo en ejecución para ver los detalles, como el porcentaje del trabajo que está completo.

Resultados

Una vez completado el despliegue del sistema operativo, inicie sesión en la dirección IP que ha especificado en la página Editar valores de red para continuar con el proceso de configuración.

Nota: La licencia proporcionada con la imagen es una prueba gratuita de 60 días. El usuario es el responsable de cumplir todos los requisitos de licencia de VMware.


VMware ESXi
Welcome
Getting Started
If you need to access this host remotely, use the following program to install vSphere Client software. After running the installer, start the client and log in to this host.
Please note that the traditional vSphere Client does not support features added to vSphere in the 5.1 and 5.5 releases. The traditional vSphere Client is intended for use if you need to connect directly to an ESXi host, are performing certain vSphere Update Manager operations, or are running vCenter Plug-ins that support only the vSphere Client such as vCenter Site Recovery Manager or vCenter Multi-Hypervisor Manager.
You can take advantage of the fullest range of functionality introduced or updated in this release by using the vSphere Web Client.
Download vSphere Client
To streamline your IT operations with vSphere, use the following program to install vCenter. vCenter will help you consolidate and optimize workload distribution across ESX hosts, reduce new system deployment time from weeks to seconds, monitor your virtual computing environment around the clock, avoid service disruptions due to planned hardware maintenance or unexpected failure, centralize access control, and automate system administration tasks.
Download VMware vCenter
If you need more help, please refer to our documentation library:
vSphere Documentation
You are running IBM Customized Image ESXi5.5 (based on ESXi 5.5
For Administrators
vSphere Remote Command Line
The Remote Command Line allows you to use command line tools to manage vSphere from a client machine. These tools can be used in shell scripts to automate day-to-day operations.
Download the Virtual Appliance
Download the Windows Installer (exe)
Download the Linux Installer (tar.gz)
Web-Based Datastore Browser
Use your web browser to find and download files (for example, virtual machine and virtual disk files).
Browse datastores in this host's inventory
For Developers
vSphere Web Services SDK
Learn about our latest SDKs, Toolkits, and APIs for managing VMware ESX, ESXi, and VMware vCenter. Get sample code, reference documentation, participate in our Forum Discussions, and view our latest Sessions and Webinars.
Learn more about the Web Services SDK
Browse objects managed by this host

Avisos

Puede que Lenovo no comercialice en todos los países los productos, servicios o características a los que se hace referencia en este documento. Póngase en contacto con su representante local de Lenovo para obtener información acerca de los productos y servicios disponibles actualmente en su zona.

Las referencias a productos, programas o servicios de Lenovo no pretenden afirmar ni implicar que solo puedan utilizarse esos productos, programas o servicios de Lenovo. En su lugar, puede utilizarse cualquier producto, programa o servicio funcionalmente equivalente que no infrinja ninguno de los derechos de propiedad intelectual de Lenovo. Sin embargo, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier otro producto, programa o servicio.

Lenovo puede tener patentes o solicitudes de patentes pendientes que aborden temas descritos en este documento. La posesión de documento no constituye una oferta y no le otorga ninguna licencia sobre ninguna patente o solicitud de patente. Puede enviar sus consultas, por escrito, a:

Lenovo (United States), Inc.
1009 Think Place
Morrisville, NC 27560
U.S.A.
Attention: Lenovo VP of Intellectual Property

LENOVO PROPORCIONA ESTA PUBLICACIÓN “TAL CUAL” SIN GARANTÍA DE NINGUNA CLASE, NI EXPLÍCITA NI IMPLÍCITA, INCLUIDAS, PERO SIN LIMITARSE A, LAS GARANTÍAS IMPLÍCITAS DE NO VULNERACIÓN DE DERECHOS, COMERCIABILIDAD O IDONEIDAD PARA UNA FINALIDAD DETERMINADA. Algunas legislaciones no contemplan la exclusión de garantías, ni implícitas ni explícitas, por lo que puede haber usuarios a los que no afecte dicha norma.

Esta información podría incluir inexactitudes técnicas o errores tipográficos. La información aquí contenida está sometida a modificaciones periódicas, las cuales se incorporarán en nuevas ediciones de la publicación. Lenovo se reserva el derecho a realizar, si lo considera oportuno, cualquier modificación o mejora en los productos o programas que se describen en esta publicación.

Los productos descritos en este documento no están previstos para su utilización en implantes ni otras aplicaciones de reanimación en las que el funcionamiento incorrecto podría provocar lesiones o la muerte a personas. La información contenida en este documento no cambia ni afecta a las especificaciones o garantías del producto de Lenovo. Ninguna parte de este documento deberá regir como licencia explícita o implícita o indemnización bajo los derechos de propiedad intelectual de Lenovo o de terceros. Toda la información contenida en este documento se ha obtenido en entornos específicos y se presenta a título ilustrativo. Los resultados obtenidos en otros entornos operativos pueden variar.

Lenovo puede utilizar o distribuir la información que le suministre el cliente de la forma que crea oportuna, sin incurrir con ello en ninguna obligación con el cliente.

Las referencias realizadas en esta publicación a sitios web que no son de Lenovo se proporcionan únicamente en aras de la comodidad del usuario y de ningún modo pretenden constituir un respaldo de los mismos. La información de esos sitios web no forma parte de la información para este producto de Lenovo, por lo que la utilización de dichos sitios web es responsabilidad del usuario.

Los datos de rendimiento incluidos en este documento se han obtenido en un entorno controlado. Así pues, los resultados obtenidos en otros entornos operativos pueden variar de forma significativa. Es posible que algunas mediciones se hayan realizado en sistemas en desarrollo, por lo que no existen garantías de que estas sean las mismas en los sistemas de disponibilidad general. Además, es posible que la estimación de

algunas mediciones se haya realizado mediante extrapolación. Los resultados reales pueden variar. Los usuarios de la presente publicación deben verificar los datos pertinentes en su entorno de trabajo específico.

Marcas registradas

Lenovo