



Guía del usuario de Lenovo XClarity Orchestrator



Versión 2.1

Nota

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

Segunda edición (Julio 2024)

© Copyright Lenovo 2020, 2024.

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

Contenido

Contenido	i
----------------------------	----------

Resumen de los cambiosiii
---	-------------

Capítulo 1. Lenovo XClarity Orchestrator Descripción general. . . . 1

Inicio de sesión en XClarity Orchestrator	3
Consejos y técnicas de la interfaz de usuario	7

Capítulo 2. Administración de XClarity Orchestrator 11

Conexión de gestores de recursos	11
Detección y gestión de dispositivos	14
Consideraciones de gestión de dispositivos	16
Configuración de valores globales de detección	20
Gestión de servidores	21
Gestión de dispositivos del cliente ThinkEdge	27
Gestión de los dispositivos de almacenamiento.	30
Gestión del chasis	33
Anular la gestión de dispositivos	37
Uso de VMwareTools	37
Configurar valores de red	38
Configuración de fecha y hora	40
Trabajo con certificados de seguridad	42
Adición de un certificado de confianza para servicios externos	43
Adición de un certificado de confianza para servicios internos	44
Instalación de un certificado de servidor de confianza firmado externamente del XClarity Orchestrator	45
Volver a generar el certificado de servidor firmado internamente de XClarity Orchestrator	47
Importación del certificado de servidor en un navegador web	49
Gestión de la autenticación	50
Configuración de un servidor de autenticación LDAP externo.	50
Gestión de usuarios y sesiones de usuarios	54
Creación de usuarios	54
Creación de grupos de usuario	56
Cambio de detalles de su cuenta de usuario	58
Cambio de los detalles de otro usuario	59
Configuración de los valores de seguridad del usuario	60

Supervisión de sesiones de usuario activas	66
Control de acceso a funciones	66
Asignación de roles a usuarios	68
Control de acceso a recursos	68
Habilitación de acceso basado en recursos	69
Creación de listas de control de acceso	70
Gestión del espacio en el disco duro	72
Reiniciar XClarity Orchestrator	73
Creación de copia de seguridad y restauración de datos de servidor de organización	74
Creación de copia de seguridad y restauración de datos de servidor de organización en un host VMware ESXi	75
Creación de copia de seguridad y restauración de datos de servidor de organización en un host Microsoft Hyper-V	76

Capítulo 3. Supervisión de recursos y actividades 79

Visualización de un resumen del estado de su entorno	79
Visualización del estado y los detalles del gestor de recursos	82
Visualización del estado de los dispositivos	83
Visualización de los detalles del dispositivo	87
Visualización del estado y los detalles de los recursos de infraestructura	89
Supervisión de trabajos.	91
Supervisión de alertas activas	93
Supervisión de sucesos	95
Exclusión de alertas y sucesos	97
Reenvío de datos de sucesos, inventario y métricas.	99
Creación de filtros de reenvío de datos	100
Reenvío de sucesos a SAP Data Intelligence.	104
Reenvío de sucesos a un servicio web REST	105
Reenvío de sucesos a un servicio de correo electrónico mediante SMTP	107
Reenvío de inventario y sucesos a Splunk.	113
Reenvío de sucesos a un syslog	114
Reenvío de datos de métricas a Sitio web de Lenovo TruScale Infrastructure Services	117
Reenvío de informes	119
Creación de configuraciones de destino del despachador	120
Reenvío de informes por correo electrónico	121

Capítulo 4. Gestión de recursos. . . .125

Creación de grupos de recursos	125
Gestión de dispositivos sin conexión	128
Realización de acciones de alimentación en servidores gestionados	129
Apertura de una sesión de control remoto para servidores gestionados	130
Apertura de una sesión de control remoto para servidores ThinkSystem o ThinkAgile	130
Apertura de una sesión de control remoto para servidores ThinkServer	131
Apertura de una sesión de control remoto para servidores System x	132

Capítulo 5. Aprovisionamiento de recursos139

Aprovisionamiento de configuraciones de servidor	139
Consideraciones sobre la configuración de servidores	141
Aprendizaje de un patrón de configuración de servidor a partir de un servidor existente	142
Asignación y despliegue de un patrón de configuración de servidor	145
Mantener el cumplimiento de configuración del servidor.	148
Aprovisionamiento de sistemas operativos	149
Consideraciones del despliegue del sistema operativo	151
Sistemas operativos compatibles	154
Perfiles de las imágenes del sistema operativo	155
Disponibilidad de puertos para sistemas operativos desplegados.	158
Importación de imágenes del sistema operativo	159
Configuración de perfiles del sistema operativo	161
Despliegue de la imagen de un sistema operativo	163
Aprovisionamiento de actualizaciones para los recursos gestionados	166
Consideraciones de actualización	168
Descarga e importación de actualizaciones	169
Creación y asignación de políticas de conformidad de actualización	174
Aplicar y activar actualizaciones a los gestores de recursos	178

Aplicar y activar actualizaciones a los servidores gestionados	180
--	-----

Capítulo 6. Análisis de tendencias y predicción de problemas185

Creación de informes de análisis personalizados	185
Creación de reglas para alertas de análisis personalizadas	185
Creación de informes personalizados (consultas)	188
Análisis de tiempos de arranque de un dispositivo	191
Análisis de problemas de conectividad.	191
Análisis de correcciones de seguridad	192
Análisis de estado de la unidad.	192
Análisis de firmware	193
Análisis de sucesos perdidos	194
Análisis y predicción de la capacidad del gestor de recursos.	194
Análisis y predicción de las tendencias de utilización	195
Análisis de rendimiento y métricas de uso	196
Análisis de sucesos repetidos	197
Análisis de intentos de acceso no autorizado	198
Análisis de estado del dispositivo	198
Análisis del estado de los recursos de infraestructura	200
Análisis de alertas activas	201

Capítulo 7. Trabajo con servicio y soporte203

Envío de datos periódicos a Lenovo	203
Recopilación de datos de servicio para XClarity Orchestrator	204
Recopilar datos del servicio de dispositivos	206
Importación de datos del servicio para dispositivos	208
Creación y asignación de contactos para el servicio y el soporte	209
Apertura automática de informes de servicio mediante la función Llamar a casa	210
Abrir manualmente un informe de servicio en el Centro de Soporte de Lenovo	214
Visualización de estados e informes de servicio	216
Ver información de garantía	219

Resumen de los cambios

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

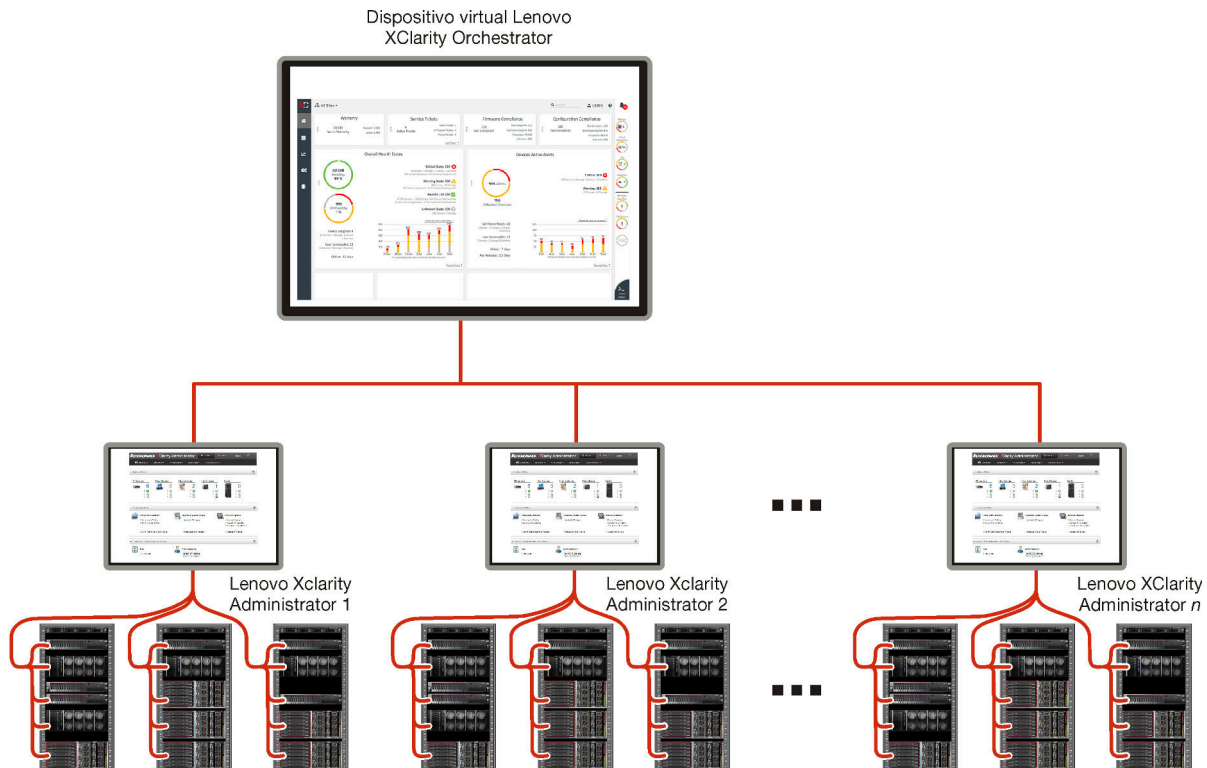
Consulte el archivo de historial de cambios (*.chg) que se proporciona con el paquete de actualización para obtener más información acerca de la solución de los problemas existentes.

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

Función	Descripción
Administración	Puede reiniciar el servidor de Orchestrator desde la interfaz de usuario (consulte Reiniciar XClarity Orchestrator).
Gestión de recursos	Lenovo XClarity Management Hub 2.0 es un nuevo gestor de dispositivos ligero que puede usar para gestionar servidores Lenovo ThinkSystem y ThinkEdge SE (consulte Conexión de gestores de recursos). Puede gestionar un gran número de servidores utilizando la opción de gestión masiva (consulte Gestión de servidores). Puede gestionar servidores utilizando nombres de dominio completo (consulte Gestión de servidores).
Supervisión de recursos y actividades	Los datos del inventario de memoria se muestran ahora en formato de tabla (consulte Visualización de los detalles del dispositivo). Puede ver una lista de todos los trabajos programados (consulte Supervisión de trabajos).
Aprovisionamiento de recursos	Puede programar una actualización de firmware para que se ejecute en una fecha y hora específicas (consulte Aplicar y activar actualizaciones a los servidores gestionados).

Capítulo 1. Lenovo XClarity Orchestrator Descripción general

Lenovo XClarity Orchestrator brinda supervisión centralizada, gestión, aprovisionamiento y análisis para entornos con grandes cantidades de dispositivos. Aprovecha Gestores de recursos existentes (como Lenovo XClarity Administrator y Schneider Electric EcoStruxure IT Expert) en múltiples sitios para ver el estado general, recopilar el inventario del dispositivo y los resúmenes de estado, profundizar en los detalles del dispositivo, ver los registros de sucesos y auditoría y aplicar actualizaciones a los recursos gestionados.



Más información:

- [Descripción general de XClarity Orchestrator](#)
- [Capacidades de gestión](#)

Supervisión y gestión de recursos centralizada

XClarity Orchestrator proporciona una interfaz única para supervisar y gestionar los gestores de recursos y los dispositivos que se gestionan mediante dichos gestores de recursos.

- Vistas de resumen del estado de sus recursos gestionados, incluidos los gestores de recursos, los dispositivos y los recursos de infraestructura (como PDU y UPS)
- Resumen y vistas detalladas del estado de los componentes, el inventario de recursos, el estado de la garantía y las asesorías en varios sitios
- Agregación de alertas y sucesos críticos, creación de alertas personalizadas y reenvío de sucesos a aplicaciones externas
- Control de ciclo de vida para dispositivos gestionados (incluidas las operaciones de alimentación)
- Iniciar en contexto la interfaz de usuario para gestores de recursos y dispositivos gestionados desde las páginas de resumen de dispositivos

Actualizaciones de aprovisionamiento

Puede utilizar XClarity Orchestrator para mantener los niveles de software actuales en los recursos gestionados. Puede utilizar el catálogo de actualizaciones para conocer los niveles de software que están disponibles, utilizar las políticas de conformidad de actualización para identificar los recursos que se deben actualizar basándose en criterios personalizados y, a continuación, desplegar las actualizaciones deseadas en esos recursos. XClarity Orchestrator asegura que el software se aprovisione en los recursos de destino en el orden correcto.

XClarity Orchestrator admite las siguientes operaciones de aprovisionamiento.

- Despliegue de actualizaciones en los gestores de recursos de Lenovo XClarity Administrator.
- Despliegue de actualizaciones de firmware en dispositivos gestionados por XClarity Administrator.

Para obtener más información sobre las actualizaciones de aprovisionamiento, consulte [Aprovisionamiento de actualizaciones para los recursos gestionados](#).

Configuración de aprovisionamiento de servidor

Puede aprovisionar servidores gestionados con rapidez utilizando una configuración coherente. Los valores de configuración (como los valores del controlador de gestión de la placa base y de UEFI) se guardan como un patrón que se puede aplicar en varios servidores.

XClarity Orchestrator no despliega directamente patrones de configuración en servidores gestionados. En su lugar, envía una solicitud al gestor de recursos aplicable para iniciar un trabajo y realizar el despliegue y, a continuación, realiza un seguimiento del progreso de la solicitud.

Para obtener más información sobre cómo aprovisionar configuraciones de servidor, consulte [Aprovisionamiento de configuraciones de servidor](#).

Aprovisionamiento de sistemas operativos

Puede utilizar XClarity Orchestrator para desplegar imágenes de sistemas operativos en varios servidores.

XClarity Orchestrator no despliega directamente el sistema operativo en servidores gestionados. En su lugar, envía una solicitud al gestor de recursos de XClarity Administrator aplicable para iniciar un trabajo y realizar la actualización y, a continuación, realiza un seguimiento del progreso de la solicitud.

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

Para obtener más información sobre cómo aprovisionar configuraciones de servidor, consulte [Aprovisionamiento de sistemas operativos](#).

Aprendizaje automático y análisis predictivo de inteligencia empresarial

XClarity Orchestrator puede conectarse a servicios de terceros (como Splunk) para que el aprendizaje automático y el análisis predictivo de la inteligencia empresarial:

- Recopilen y muestren datos de tendencias (como la utilización de procesador y de memoria, el consumo de alimentación, la temperatura, el acceso no autorizado, los sucesos repetidos y perdidos y el tiempo medio entre procesos como actualizaciones de firmware y rearranques del sistema)
- Utiliza datos métricos para predecir errores (como sucesos repetidos e informes de estado)
- Cree informes personalizados sobre la base de los datos existentes, incluidas las alertas, los sucesos, el inventario de dispositivos y las mediciones de los dispositivos.
- Defina reglas de alertas personalizadas que, cuando están habilitadas, generan alertas cuando existen condiciones específicas en su entorno.

Más información:  [Capacidades predictivas y de análisis](#)

Para obtener más información sobre el análisis predictivo, consulte [Análisis de tendencias y predicción de problemas](#).

Servicio y soporte

XClarity Orchestrator se puede configurar para que automáticamente recopile y envíe archivos de diagnóstico a soporte de Lenovo mediante Llamar a casa cuando ocurran ciertos sucesos de mantenimiento en recursos gestionados. También puede recopilar los archivos de diagnóstico de forma manual, abrir un registro de problemas y enviar archivos de diagnóstico al centro de soporte de Lenovo.

Para obtener más información sobre el servicio y soporte, consulte [Trabajo con servicio y soporte](#).

Documentación

La documentación en línea se actualiza de forma periódica en inglés. Para consultar la información y los procedimientos más recientes, consulte [Documentación en línea de XClarity Orchestrator](#).

La documentación en línea está disponible en los siguientes idiomas.

- Inglés (en)
- Chino simplificado (zh-CN)
- Chino tradicional (zh-TW)
- Francés (fr)
- Alemán (de)
- Italiano (it)
- Japonés (ja)
- Coreano (ko)
- Portugués de Brasil (pt-BR)
- Ruso (ru)
- Español (es)
- Tailandés (th)

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

- Añada `<language_code>` después de `https://pubs.lenovo.com/lxco/`, por ejemplo, para mostrar la documentación en línea en chino simplificado.
`https://pubs.lenovo.com/lxco/zh-CN/`

Inicio de sesión en XClarity Orchestrator

Inicie sesión en la interfaz web de Lenovo XClarity Orchestrator desde un sistema con conectividad de red al dispositivo virtual de XClarity Orchestrator.

Antes de empezar

Asegúrese de utilizar uno de los siguientes navegadores web compatibles. Para obtener más información, consulte [Hardware y software admitidos](#) en la documentación en línea de XClarity Orchestrator..

- Chrome 80.0 o posterior
- Firefox ESR 68.6.0 o posterior
- Microsoft Edge 40.0 o posterior
- Safari 13.0.4 o posterior (se ejecuta en macOS 10.13 o posterior)

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

Al usar una cuenta de usuario LDAP, puede iniciar sesión con el nombre de usuario o nombreusuario@dominio (por ejemplo, user1@company.com).

XClarity Orchestrator cierra automáticamente las sesiones de usuario que han estado inactivas durante un período de tiempo y sesiones de usuario que se han abierto durante un tiempo determinado, independientemente de la actividad. Los siguientes valores predeterminados son establecidos por XClarity Orchestrator.

- Si no hizo clic o escribió en la interfaz de usuario por **30 minutos**, su sesión de usuario se limita a las operaciones de solo lectura. Si intenta modificar los datos, la sesión del usuario se cerrará automáticamente.
- Si no ha visto datos activamente por **1440 los minutos (24 horas)**, su sesión de usuario se cerrará automáticamente.
- Después de **24 horas**, las sesiones de usuario se cierran automáticamente, independientemente de la actividad del usuario.

Procedimiento

Para iniciar sesión en la interfaz web de XClarity Orchestrator, lleve a cabo los pasos siguientes.

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

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

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

Por ejemplo:

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

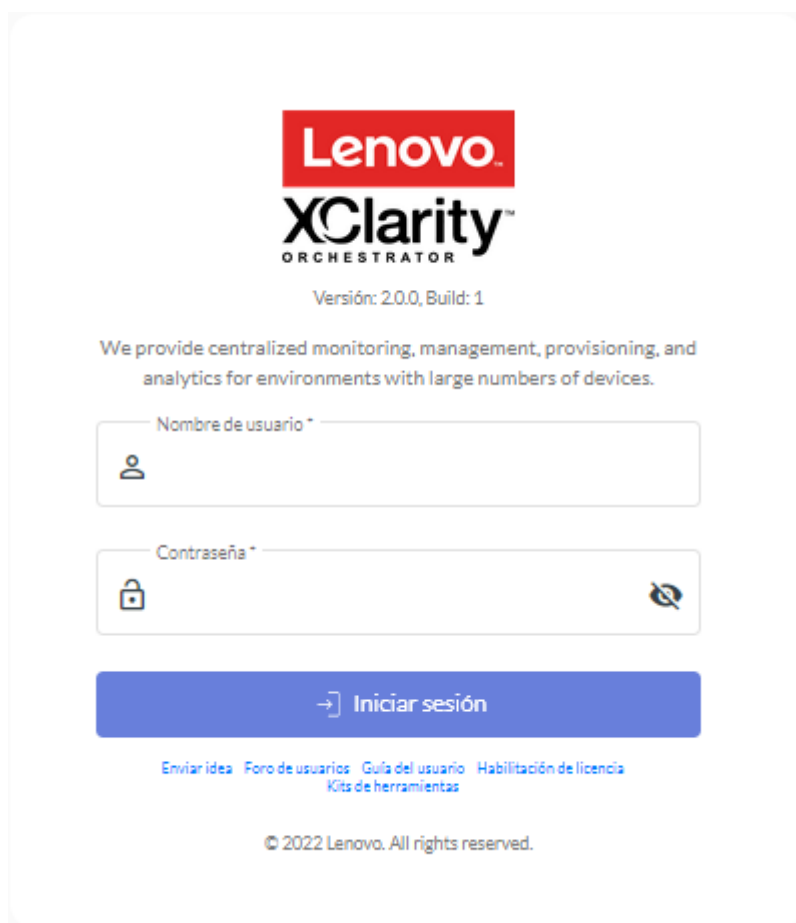
- **Uso de un servidor DHCP en el mismo dominio de difusión que XClarity Orchestrator** Si hay configurado un servidor DHCP en el mismo dominio de difusión que XClarity Orchestrator, utilice la dirección IPv4 que se muestra en la consola del dispositivo virtual de XClarity Orchestrator para acceder a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

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

Por ejemplo:

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

Se muestra la primera página de inicio de sesión.



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

- Envíe ideas para XClarity Orchestrator en [Sitio web de Lenovo XClarity Ideation](#) o haciendo clic en **Enviar idea**.
- Haga preguntas y reciba respuestas en el [Sitio web del foro de la comunidad de Lenovo XClarity](#) haciendo clic en **Foro de usuarios**.
- Para obtener información sobre cómo utilizar XClarity Orchestrator, haga clic en **Guía del usuario**.
- Busque y gestione todas sus licencias de Lenovo desde [Características del portal web on Demand](#) haciendo clic en **Habilitación de licencia**.
- Para obtener información acerca de las API disponibles, haga clic en **Kits de herramientas**.

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

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

3. Introduzca un Id. de usuario y una contraseña válidos y, a continuación, haga clic en **Iniciar sesión**. La primera vez que se usa una cuenta de usuario específica para iniciar sesión en XClarity Orchestrator, se le pedirá que cambie la contraseña. De manera predeterminada, las contraseñas deben contener los caracteres **8 - 256** y deben cumplir los siguientes criterios.


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

- Debe contener al menos un carácter alfabético y no debe tener más de dos caracteres secuenciales, incluidas las secuencias de caracteres alfabéticos, dígitos y las teclas del teclado QWERTY (por ejemplo “abc”, “123” y “asd” no están permitidos)

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

Después de finalizar

Se muestra la el panel XClarity Orchestrator con un resumen del estado del recurso y las actividades en su entorno.

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

- Cambie la contraseña del usuario actual haciendo clic en **Cambiar contraseña**.
- Para cerrar la sesión actual, haga clic en **Cerrar sesión**. Se muestra la página inicio de sesión de XClarity Orchestrator.

Desde la página de inicio de sesión, puede hacer clic en el enlace **Habilitación de licencia** para abrir el [Características del portal web on Demand](#), donde puede encontrar y gestionar todas las licencias de productos de Lenovo.

- Envíe ideas para XClarity Orchestrator en [Sitio web de Lenovo XClarity Ideation](#) o haciendo clic en **Enviar idea**.
- Haga preguntas y reciba respuestas en el [Sitio web del foro de la comunidad de Lenovo XClarity](#) haciendo clic en **Foro de usuarios**.
- Descargue el kit de herramientas de PowerShell (LXCOPSTool) de XClarity Orchestrator haciendo clic en **Kit de herramientas**. El kit de herramientas LXCOPSTool proporciona una biblioteca de cmdlets para automatizar el aprovisionamiento y la gestión de recursos para una sesión de Microsoft PowerShell.
- Encontrará información sobre cómo usar XClarity Orchestrator con el sistema de ayuda integrado al hacer clic en **Ayuda**.

La documentación en línea se actualiza de forma periódica en inglés. Para consultar la información y los procedimientos más recientes, consulte [Documentación en línea de XClarity Orchestrator](#).

- Para ver información sobre la versión de XClarity Orchestrator, haga clic en **Acerca de**.

En el cuadro de diálogo Acerca de encontrará enlaces para ver el **Acuerdo de licencia de usuario final**, las **Licencias de código abierto** y la **Declaración de privacidad de Lenovo**.

- Para cambiar el idioma de la interfaz de usuario, haga clic en **Cambiar idioma**. Se admiten los siguientes idiomas.
 - Inglés (en)
 - Chino simplificado (zh-CN)
 - Chino tradicional (zh-TW)
 - Francés (fr)
 - Alemán (de)
 - Italiano (it)
 - Japonés (ja)
 - Coreano (ko)
 - Portugués de Brasil (pt-BR)
 - Ruso (ru)

- Español (es)
- Tailandés (th)


Consejos y técnicas de la interfaz de usuario

Considere estos consejos y técnicas al utilizar la interfaces de usuario de Lenovo XClarity Orchestrator y Lenovo XClarity Management Hub.

Importación de archivos

Puede importar archivos al arrastrar y soltar los archivos en un cuadro de diálogo Importar.

Al importar un archivo, en la esquina inferior derecha de la interfaz de usuario aparece un elemento emergente ampliable con información acerca del progreso y el estado de cada proceso de importación. Los iconos en el elemento emergente le ayudan a identificar rápidamente el estado del proceso para cada importación. Una vez que la importación se completa correctamente, se inicia un trabajo para validar el archivo. Si se produce un error durante el proceso de importación, en el cuadro de diálogo emergente aparece un mensaje de error que le ayudará a resolver el problema rápidamente.

Cuando el elemento emergente se contrae, puede hacer clic y mantener presionado el icono **Arrastrar**  para mover el elemento emergente a una posición diferente.

Haga clic en **Borrar todo** para borrar la lista de procesos de importación completados. Si todos los procesos de importación están completados, el elemento emergente se oculta.



Introducción de texto en los campos de texto

Los caracteres que se pueden introducir en algunos campos de texto están restringidos. En la lista siguiente se describen los caracteres que están permitidos.

- **Nombres.** Incluye todas las letras y los caracteres numéricos de los idiomas admitidos y los caracteres especiales @ - _ + / [] . , : y espacio.
- **Descripciones.** Incluye todas las letras y los caracteres numéricos de los idiomas admitidos y los caracteres especiales @ - _ % & * + = / () { } [] . , : y espacio.
- **Contraseñas.** Para las cuentas de usuarios locales, las contraseñas pueden tener **8 – 256** caracteres de forma predeterminada, aunque se recomiendan 16 o más caracteres. No hay restricciones de caracteres para las contraseñas. Sin embargo, las contraseñas requieren ciertos tipos de caracteres y restringen algunas secuencias para ser seguras.
 - Debe contener al menos un carácter alfabético y no debe tener más de dos caracteres secuenciales, incluidas las secuencias de caracteres alfabéticos, dígitos y las teclas del teclado QWERTY (por ejemplo “abc”, “123” y “asd” no están permitidos)
 - Debe contener por lo menos un número
 - Deben contener al menos dos de los siguientes caracteres.
 - Caracteres alfabéticos en mayúscula (A - Z)
 - Caracteres alfabéticos en minúscula (a - z)
 - Caracteres especiales ; @ _ ! ' \$ & +Los espacios en blanco no están permitidos.
 - No se debe repetir ni invertir el nombre de usuario.
 - No debe contener más de dos caracteres iguales consecutivamente (por ejemplo, “aaa”, “111” y “...” no están permitidos).

Expanda y contraiga el panel de navegación

El panel de navegación se contrae de manera predeterminada, mostrando solo los iconos que representan elementos específicos del menú. Puede hacer clic en un icono para expandir temporalmente el panel de navegación y el menú para dicho icono. Al desplazar el cursor fuera del panel de navegación, el panel se contrae de manera tal que solo se muestren los iconos.

Para mantener el panel de navegación expandido permanentemente, haga clic en el icono de **Expandir** (). A continuación, puede contraer el panel de navegación haciendo clic en el icono de **Contraer** (.

Alcance de la interfaz de usuario

De forma predeterminada, XClarity Orchestrator muestra datos para *todos los recursos*. Puede restringir el alcance de los datos que se muestran en la sesión actual del usuario a solo los recursos que se encuentran en gestores y grupos de recursos específicos mediante el uso del menú desplegable **Alcance actual** que se encuentra en la parte superior de la página. En el menú desplegable, puede ver la lista de gestores de recursos y grupos en el alcance actual en **Mi lista de alcances**. Haga clic en **Cambiar alcance** para mostrar un cuadro de diálogo en el cual crea un alcance personalizado con varios gestores y grupos de recursos, o seleccione **Todos los recursos** para cambiar el alcance para ver todos los recursos.

El alcance seleccionado solo es persistente en la sesión de usuario actual. Puede abrir varias sesiones de usuario, cada una de ellas con vistas diferentes del panel, los recursos, los sucesos y los datos de alerta.

Nota: Los gestores de recursos de VMware vRealize Operations Manager no se incluyen en la lista de gestores de recursos, ya que no gestionan dispositivos en XClarity Orchestrator.

Visualización de más o menos datos por página

Cambie el número de filas que se listan en una tabla por página utilizando la lista desplegable **Filas por página** en la parte inferior de cada tabla. Puede mostrar 10, 15, 25 o 50 filas.

Búsqueda de datos en listas grandes

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

- Ordene las filas de la tabla haciendo clic en el encabezado de la columna.
- Restrinja el alcance de los datos en la sesión actual del usuario a solo los recursos que se encuentran en un gestor o grupo de recursos específico mediante el uso del menú desplegable **Alcance actual** que se encuentra en la parte superior de la página (consulte “Alcance de la interfaz” de usuario arriba).
- Cree dinámicamente un subconjunto de listas basado en los datos que se encuentran en columnas específicas usando los campos de entrada **Filtros**. Puede filtrar por columnas mostradas y ocultas. También puede guardar las consultas de filtro que desee utilizar habitualmente.
- Refine aún más el subconjunto al ingresar texto (como el nombre o la dirección IP) en el campo **Buscar** para buscar datos que se encuentran en cualquier columna disponible.

Consejo: Separe múltiples búsquedas mediante comas. Por ejemplo, "180.190" muestra todas las filas que contienen 180 o 190 en cualquiera de las columnas disponibles.

- Seleccione la casilla de verificación del encabezado de la tabla para seleccionar o borrar todos los elementos que se enumeran en la tabla.

Visualización de los datos de una tabla

Actualice las tablas de datos; para ello, haga clic en el icono **Actualizar** (.

Expanda o contraiga cada fila para mostrar u ocultar los subdetalles de las tablas con filas expansibles (como en los trabajos y las tarjetas de gestión del repositorio). También puede hacer clic en el icono **Contraer todo** (☰) para ocultar los subdetalles de todas las filas.

Si el tamaño de la columna impide que parte de 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 la celda.

Exportación de datos de tabla

Haga clic en el icono **Exportar datos** (📄) para exportar los datos de la tabla actual al sistema local. Puede exportar todas las páginas, la página actual o las filas seleccionadas, elegir el formato de archivo (XLSX, CSV o JSON) y si desea incluir todas las columnas o solo las columnas visibles. Para el formato CSV, también puede elegir cómo separar los datos (con punto y coma, tabulación o carácter de barra vertical).

Consejo: Para el formato JSON, las marcas de tiempo de los datos exportados reflejan la zona horaria establecida para XClarity Orchestrator y no para el sistema local. Para los formatos CSV y XLSX, las marcas de tiempo se convierten en la zona horaria del usuario, que se muestra en la interfaz web.

Al exportar datos, en la esquina inferior derecha de la interfaz de usuario aparece un elemento emergente ampliable con información acerca del progreso y el estado. Los iconos en el elemento emergente le ayudan a identificar rápidamente el estado del proceso para cada exportación. Si se produce un error durante el proceso de exportación, en el cuadro de diálogo emergente aparece un mensaje de error que le ayudará a resolver el problema rápidamente.

Cuando el elemento emergente se contrae, puede hacer clic y mantener presionado el icono **Arrastrar** (☰) para mover el elemento emergente a una posición diferente.

Haga clic en **Borrar todo** para borrar la lista de procesos de exportación completados. Si todos los procesos de exportación están completados, el elemento emergente se oculta.

Configure las columnas de la tabla

Configure las tablas para que muestren información más importante para usted.

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

Cambiar el idioma de la interfaz de usuario

Puede cambiar el idioma de la interfaz de usuario cuando inicie sesión por primera vez.


Una vez que haya iniciado sesión, puede cambiar el idioma haciendo clic en el menú de **Cuenta del usuario** (👤) y luego en **Cambiar idioma**.

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

Cómo obtener ayuda

Hay varias formas de obtener ayuda con la interfaz de usuario.

- Desplace el cursor sobre un icono de **Ayuda** (❓) en algunas páginas para mostrar un elemento emergente con detalles adicionales sobre un campo específico.
- Haga clic en el enlace **Obtener más información** en algunas páginas para abrir el sistema de ayuda y obtener más información en contexto.

- Obtenga ayuda sobre cómo realizar acciones específicas desde la interfaz de usuario haciendo clic en el menú de **Cuenta del usuario** () y luego en **Ayuda**. La documentación en línea se actualiza de forma periódica en inglés. Para consultar la información y los procedimientos más recientes, consulte [Documentación en línea de XClarity Orchestrator](#).

Capítulo 2. Administración de XClarity Orchestrator

Hay varias actividades de gestión disponibles, como la configuración del sistema, como la fecha y hora y el acceso de red, la conexión de los administradores de recursos, la gestión de los servidores de autenticación y el acceso de usuarios y la gestión de certificados de seguridad.

Conexión de gestores de recursos

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

Antes de empezar

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

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

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

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

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

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

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

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

Acerca de esta tarea

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

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

Importante: El XClarity Management Hub 2.0 del proceso de registro es diferente del de otro gestor de recursos. Para obtener instrucciones detalladas, consulte [Conexión de XClarity Management Hub 2.0 a XClarity Orchestrator](#) en la documentación en línea de XClarity Orchestrator..

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

Importante: El XClarity Management Hub del proceso de registro es diferente del de otro gestor de recursos. Para obtener instrucciones detalladas, consulte [Conexión de XClarity Management Hub a XClarity Orchestrator](#) en la documentación en línea de XClarity Orchestrator..

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

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

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

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

Procedimiento

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

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

<input type="checkbox"/>	Gestor de re	Estado	Tipo	Versión	Build	Conectado	Datos de aná	Grupos
<input type="checkbox"/>	XClarity...	🟢 No...	XClarity...	2.0.0	279	No Disponi	No Disponi	No Disponi
<input type="checkbox"/>	host-10-...	🟢 No...	XClarity...	3.6.0	108	16/2/23 10	🔴 1	No Disponi

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

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

- **XClarity Management Hub 2.0 o XClarity Management Hub**
 1. Introduzca la clave de registro generada por la instancia del concentrador de gestión y, a continuación, haga clic en **Conectar**. Para obtener el token de solicitud de registro, inicie sesión en el portal del concentrador de gestión, haga clic en **Registro** y, a continuación, haga clic en **Crear clave de registro**.
 2. Copie la clave de registro de XClarity Orchestrator generada.
 3. En el portal del concentrador de gestión, haga clic en **Registro**, después en **Instalar clave de registro**, pegue el token de registro de XClarity Orchestrator y, a continuación, haga clic en **Conectar**.
- **XClarity Administrator**
 - Especifique el nombre de dominio o la dirección IP (IPv4 o IPv6) totalmente cualificados. No se admite el uso del nombre de host sin el nombre de dominio.
 - Opcionalmente, cambie el puerto del gestor de recursos. El valor predeterminado es 443.
 - Especifique la cuenta de usuario y contraseña que utilizará para iniciar sesión en Gestor de recursos.
 - Opcionalmente, habilite **Recopilación de datos de análisis de unidad**. Cuando está habilitado, los datos de análisis de la unidad para los dispositivos ThinkSystem y ThinkAgile se recopilan a diario y se usan para fines de análisis predictivo. La Recopilación de datos de análisis de unidad solo se admite en XClarity Administrator v3.3.0 y versiones posteriores de los gestores de recursos.

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

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

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

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

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

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

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

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

Después de finalizar

Puede realizar las siguientes acciones desde la tarjeta Gestores de recursos.

- Ver el estado de conexión del gestor de recursos desde la columna **Estado**.
- Modifique las credenciales y propiedades para un gestor de recursos seleccionado haciendo clic en el icono de **Editar** (✎). Se crea un trabajo para llevar a cabo esta operación. Puede supervisar el progreso del trabajo desde la tarjeta **Supervisión** (📄) → **Trabajos**. Si el trabajo no finalizó correctamente, haga clic en el enlace del trabajo para mostrar los detalles correspondientes (consulte .)
- Habilite o deshabilite la Recopilación de datos de análisis de unidad para un gestor de recursos XClarity Administrator seleccionado haciendo clic en el icono de **Editar** (✎).

Nota: El icono de alternación de **Recopilación de datos de análisis de unidad** se desactiva cuando XClarity Administrator tiene problemas de conectividad o de credenciales (consulte [Pérdida de conectividad repentina de un gestor de recursos](#) en la documentación en línea de XClarity Orchestrator).

- Desconecte y quite un gestor de recursos seleccionado haciendo clic en el icono de **Eliminar** (🗑️).

Nota: Si XClarity Orchestrator no puede conectarse con el gestor de recursos (por ejemplo, si las credenciales han caducado o si hay problemas de red), seleccione **Forzar desconexión**.

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

Cuando se quita el gestor de recursos, todos los dispositivos que gestiona dicho gestor de recursos también se quitan. Esto incluye el inventario de dispositivos, los registros, los datos de métrica y los informes analíticos.

- Resolución de problemas al conectarse a un gestor de recursos (consulte [No se puede conectar un gestor de recursos](#) en la documentación en línea de XClarity Orchestrator).

Detección y gestión de dispositivos

Puede detectar y gestionar dispositivos utilizando Lenovo XClarity Orchestrator y asignar la gestión de esos dispositivos a un gestor de recursos específico.

Antes de empezar

Para realizar esta tarea, debe ser miembro de un grupo de usuarios al que se le haya asignado el rol de **Supervisor** o Administrador de **seguridad** predefinido.

Acerca de esta tarea

XClarity Orchestrator supervisa y gestiona dispositivos a través de gestores de recursos. Cuando se conecta a un gestor de recursos, XClarity Orchestrator gestiona todos los dispositivos que gestiona dicho gestor de recursos.

También puede gestionar dispositivos utilizando XClarity Orchestrator. XClarity Orchestrator muestra una lista de los dispositivos que ya se han detectado (pero no gestionado) mediante los gestores de recursos. Cuando gestiona dispositivos detectados desde XClarity Orchestrator, los dispositivos se gestionan mediante el gestor de recursos que los ha detectado. Cuando detecta y gestiona dispositivos manualmente utilizando direcciones IP, nombres de host o subredes, debe elegir qué gestor de recursos desea utilizar para gestionar los dispositivos. XClarity Management Hub se puede utilizar para gestionar dispositivos del cliente ThinkEdge. XClarity Management Hub 2.0 se puede utilizar para gestionar dispositivos ThinkServer. Lenovo XClarity Administrator se puede utilizar para gestionar servidores, almacenamiento, conmutadores y chasis.

Notas:

- Si intenta gestionar un dispositivo a través de XClarity Management Hub 2.0 y ese dispositivo ya se gestiona a través de otro XClarity Management Hub 2.0, XClarity Orchestrator elimina la cuenta de usuario de gestión y las suscripciones del dispositivo sin el reconocimiento de gestión anterior y luego gestiona el dispositivo de nuevo a través del nuevo concentrador de gestión. Tras este proceso, el dispositivo se sigue gestionando, pero sin conexión, desde el antiguo concentrador de gestión, pero el dispositivo ya no le envía datos. Tenga en cuenta que debe anular manualmente la gestión de los dispositivos del primer concentrador de gestión a través del portal conectado.
- Si intenta gestionar un dispositivo a través de XClarity Management Hub 2.0 y ese dispositivo ya se gestiona a través de otro XClarity Administrator, XClarity Orchestrator elimina la cuenta de usuario de gestión, las suscripciones y la información de LDAP y SSO que registra XCC mediante XClarity Administrator desde el dispositivo sin el reconocimiento de XClarity Administrator y, a continuación, gestiona el dispositivo de nuevo a través del nuevo XClarity Management Hub 2.0. Tras este proceso, el dispositivo se sigue gestionando, pero sin conexión, desde el concentrador XClarity Administrator, pero el dispositivo ya no le envía datos. Tenga en cuenta que debe anular manualmente la gestión de los dispositivos del XClarity Administrator a través del portal conectado.

Los gestores de recursos pueden detectar automáticamente los dispositivos siguientes utilizando un protocolo de detección de servicios.

- Servidores y dispositivos ThinkSystem y ThinkAgile
- Servidores ThinkEdge SE
- Chasis de Flex System y dispositivos ThinkSystem y Flex System en un chasis de Flex System
- Servidores de bastidor y torre de ThinkServer
- Servidores y dispositivos System x, Converged HX y NeXtScale
- Dispositivos de almacenamiento

Los gestores de recursos *no* pueden detectar automáticamente los dispositivos siguientes utilizando un protocolo de detección de servicios. Para que se puedan detectar y gestionar de forma segura, debe instalar el agente de UDC en estos dispositivos.

- Cliente ThinkCentre
- Clientes ThinkEdge

Actualmente, no es posible gestionar conmutadores desde XClarity Orchestrator. Tampoco puede anular la gestión de conmutadores Flex System desde XClarity Orchestrator.

Consideraciones de gestión de dispositivos

Antes de intentar detectar y gestionar dispositivos utilizando XClarity Orchestrator, revise las siguientes consideraciones.

- [Consideraciones generales](#)
- [Consideraciones sobre el servidor](#)
- [Consideraciones de almacenamiento](#)
- [Consideraciones sobre el conmutador](#)
- [Consideraciones sobre el chasis](#)
- [Varias consideraciones sobre la herramienta de gestión](#)

Consideraciones generales

Asegúrese de que XClarity Orchestrator admite los dispositivos que desea gestionar.

Asegúrese de que el firmware mínimo necesario esté instalado en cada sistema que desee gestionar.

Algunos puertos deben estar disponibles para comunicarse con los dispositivos. Asegúrese de que todos los puertos requeridos estén disponibles antes de intentar gestionar servidores.

XClarity Orchestrator puede detectar automáticamente dispositivos en su entorno, sondeando los dispositivos gestionables que se encuentran en la misma subred IP, como XClarity Orchestrator utilizando un protocolo de detección de servicios. Para detectar los dispositivos que están en otras subredes, puede especificar manualmente direcciones IP, nombres de host, rango de direcciones IP o subredes.

Una vez que XClarity Orchestrator gestiona los dispositivos, XClarity Orchestrator sondea periódicamente todos los dispositivos de almacenamiento gestionados para recopilar información, como el inventario, los datos de producto fundamentales y el estado.

Si XClarity Orchestrator pierde la comunicación con un dispositivo (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 dispositivo entre en línea y que XClarity Orchestrator sondee el dispositivo para el inventario o recopile manualmente el inventario en el dispositivo desde la interfaz web del gestor de recursos seleccionando el dispositivo y haciendo clic en **Todas las acciones** → **Inventario** → **Actualizar inventario**.

Los dispositivos solo se pueden gestionar a la vez por un gestor de recursos (XClarity Orchestrator, XClarity Management Hub 2.0, XClarity Management Hub o XClarity Administrator). Si un dispositivo está gestionado por un gestor de recursos y desea gestionarlo con otro, primero debe dejar de gestionar el dispositivo en el gestor de recursos inicial.

Si cambia la dirección IP de un dispositivo después de que el dispositivo está gestionado por XClarity Orchestrator reconoce la nueva dirección IP y continúa gestionando el servidor. Sin embargo, XClarity Orchestrator no reconoce el cambio de dirección IP para algunos servidores. Si XClarity Orchestrator 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**.

Si quita, sustituye o configura cualquier adaptador en un dispositivo, reinicie el dispositivo al menos una vez para actualizar la información de inventario.

Para detectar un dispositivo que está en una subred *distinta* del gestor de recursos, asegúrese de que se cumpla una de las siguientes condiciones:

- Asegúrese de que el reenvío multidifusión SLP esté habilitado en los conmutadores del bastidor y 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 dispositivo 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). Por ejemplo:

```
lxco.company.com service = 0 0 443 server1.company.com
```

A continuación, habilite la detección de DNS en la consola de gestión de la placa base desde la interfaz web de gestión haciendo clic en **Configuración de BMC → Red**, haciendo clic en la pestaña **DNS**.

Consideraciones sobre la encapsulación

Puede elegir habilitar la encapsulación en el chasis y servidores durante el proceso de gestión de dispositivos. Cuando los valores globales de encapsulación están habilitados y el dispositivo admite la encapsulación, el gestor de recursos 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 del gestor de recursos.

Nota: La gestión de dispositivos con la encapsulación habilitada puede tardar bastante tiempo cuando la interfaz de red de gestión está configurada para utilizar el protocolo de configuración dinámica de host (DHCP).

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 durante el proceso de gestión del dispositivo.

Atención: Si el modo de encapsulación es **encapsulationLite** en dispositivos gestionados, las siguientes situaciones pueden provocar problemas de comunicación y autenticación entre el gestor de recursos y los dispositivos gestionados, lo que hace que no se pueda acceder a los dispositivos gestionados. Dado que los dispositivos están configurados para ignorar las solicitudes TCP de otras fuentes, no es posible acceder a estos dispositivos mediante una interfaz de red. En la mayoría de los casos, estos dispositivos no responden a solicitudes de ping, SSH o TELNET.

- Cambios de red en el hipervisor en el que se ejecuta el gestor de recursos
- Cambios de las redes de área local virtual (VLAN) o de las etiquetas VLAN
- Cambios permanentes en las direcciones IP del dispositivo cuando la encapsulación está habilitada
- Forzar la anulación de la gestión de un dispositivo cuando la encapsulación está habilitada
- Pérdida de la máquina virtual del gestor de recursos
- Pérdida de la comunicación TCP entre la máquina virtual y los dispositivos gestionados
- Otros problemas de red que impiden que el gestor de recursos se comunique directamente con los dispositivos gestionados cuando el modo de encapsulación está habilitado

Si se produce un problema permanente, realice una de las acciones siguientes para recuperar el acceso a los dispositivos gestionados previamente. Para obtener más información, consulte [Gestión de encapsulación](#), [Recuperación de la gestión con un CMM tras un error de servidor de gestión](#) y [Recuperación de la gestión con un CMM tras un error de servidor de gestión](#) en la documentación en línea de XClarity Administrator.

- Para recuperar el acceso a un IMM gestionado donde está activado el modo de encapsulación, los valores predeterminados se deben cargar desde la consola local mediante la interfaz gráfica de usuario UEFI.
- Utilice el puente USB a Ethernet para obtener acceso en banda al controlador de gestión y ejecute el siguiente comando:
encaps lite -off
- Para recuperar el acceso a un CMM gestionado donde está activado el modo de encapsulación, los valores predeterminados se deben cargar mediante el botón de restablecimiento posterior o ejecutando el siguiente comando si aún se puede acceder a ella:

```
accesscontrol -off -T mm[p]
```

Consideraciones sobre el servidor

Asegúrese de que el CIM sobre HTTPS esté habilitado en el dispositivo. Inicie sesión en la interfaz web de gestión del servidor utilizando la cuenta de usuario `RECOVERY_ID`. Haga clic en **Configuración de BMC → Seguridad** y, a continuación, haga clic en la pestaña **CIM sobre HTTPS** y asegúrese de que la opción **Habilitar CIM sobre HTTPS** esté seleccionada.

Cuando se realizan las acciones de gestión en un servidor, asegúrese de que el servidor esté apagado o encendido en la configuración de BIOS/UEFI o en un sistema operativo en ejecución (consulte [Realización de acciones de alimentación en servidores gestionados.](#)) 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, pulse **F1** para iniciar la Setup Utility. Acceda a **Valores de sistema → Dispositivos y puertos de E/S → Habilitar/deshabilitar el soporte de ROM de opción de adaptador** y, a continuación, ubique la sección **Habilitar/deshabilitar la opción de ROM de UEFI** para verificar que los valores estén habilitados. 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.

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 Orchestrator (consulte [Instalación de un certificado de servidor de confianza firmado externamente del XClarity Orchestrator](#)).

Dispositivos del cliente ThinkEdge

Los dispositivos del cliente ThinkEdge no tienen controladores de gestión de la placa base y, por lo tanto, no se pueden detectar mediante protocolos de detección de servicio. Debe instalar un agente de UDC en los dispositivos del cliente ThinkEdge para que el gestor de recursos de Lenovo XClarity Management Hub asignado pueda detectar y gestionar de forma segura los dispositivos. Para obtener más información, consulte el apartado [Gestión de dispositivos del cliente ThinkEdge](#).

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 efisshell al menos una vez, de modo que XClarity Orchestrator 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 en la interfaz web de ThinkSystem System Manager, haga clic en **Valores → Configuración de IPMI**. Es posible que tenga que reiniciar el servidor para activar el cambio.

Servidores ThinkServer

Se debe configurar el nombre de host del servidor mediante un nombre de host o dirección IP válida para detectar automáticamente esos servidores.

La red de configuración debe permitir el tráfico SLP entre XClarity Orchestrator y el servidor.

Se requiere SLP de difusión única.

Para detectar 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 Orchestrator, asegúrese de que la red se configure para permitir UDP entrante mediante el puerto 162 para que XClarity Orchestrator pueda recibir sucesos para esos dispositivos.

Servidores System x3950 X6

Estos servidores se deben gestionar como dos alojamientos 4U, cada uno con su propio controlador de gestión de la placa base.

Para obtener más información sobre cómo gestionar servidores, consulte [Gestión de servidores](#) y [Gestión de dispositivos del cliente ThinkEdge](#).

Consideraciones de almacenamiento

Asegúrese de que se cumplan los siguientes requisitos antes de detectar y gestionar dispositivos de almacenamiento de bastidor (que no sea ThinkSystem serie DE).

- La red de configuración debe permitir el tráfico SLP entre el gestor de recursos y el dispositivo de almacenamiento de bastidor.
- Se requiere SLP de difusión única.
- Se requiere SLP de multidifusión si desea que XClarity Orchestrator detecte automáticamente los dispositivos Lenovo Storage. Además, se debe habilitar SLP en el dispositivo de almacenamiento de bastidor.

Para obtener más información sobre cómo gestionar dispositivos de almacenamiento, consulte [Gestión de los dispositivos de almacenamiento](#).

Consideraciones sobre el conmutador

Actualmente, no se admite la gestión de conmutadores de bastidor con XClarity Orchestrator.

Consideraciones sobre el chasis

Cuando gestiona un chasis, también se gestionan todos los dispositivos del chasis. No puede detectar ni gestionar componentes del chasis de forma independiente del chasis.

Asegúrese de que el 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 **Configuración de BMC → Cuentas de usuarios**, después en **Valores de inicio de sesión global** y, a continuación, 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](#).

Considere la posibilidad de implementar direcciones IPv4 o IPv6 para todos los CMM y conmutadores Flex System que están gestionados mediante XClarity Orchestrator. 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).

Para detectar un chasis que está en una subred *distinta* del gestor de recursos, asegúrese de que se cumpla una de las siguientes condiciones:

- Asegúrese de que el reenvío multidifusión SLP esté habilitado en los conmutadores del bastidor y 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 dispositivo 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). Por ejemplo:

```
lxco.company.com service = 0 0 443 cmm1.company.com
```

A continuación, habilite la detección de DNS en la consola de gestión de la placa base desde la interfaz web de gestión haciendo clic en **Configuración de BMC → Red**, haciendo clic en la pestaña **DNS**.

Para obtener más información sobre cómo gestionar los chasis, consulte [Gestión del chasis](#).

Varias consideraciones sobre la herramienta de gestión

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 Orchestrator.

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 de controlador de gestión de la placa base. 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 de RECOVERY_ID.
2. Si la política de seguridad está configurada como **Segura**, cambie el método de autenticación del usuario.
 - a. Haga clic en **Configuración de BMC → Cuentas de usuarios**.
 - b. Haga clic en la pestaña **Cuentas**.
 - c. Haga clic en **Valores de inicio de sesión global**.
 - 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.

Configuración de valores globales de detección

Elija los valores que desee que se utilicen al detectar dispositivos.

Procedimiento

- Paso 1. En la barra de menús de XClarity Orchestrator, haga clic en **Recursos** (⚙️) → **Nuevos dispositivos** para ver la tarjeta Detectar y gestionar nuevos dispositivos.
- Paso 2. Haga clic en ⚙️ **Configuración** para ver el cuadro de diálogo Valores de detección.
- Paso 3. Seleccione los valores de detección que desee.
 - **Detección de SLP** Indica si se deben detectar automáticamente dispositivos mediante el protocolo de ubicación de servicio (SLP).

Cuando está habilitado, XClarity Orchestrator intenta detectar nuevos dispositivos cada 15 minutos y en cada inicio de sesión de usuario.

Nota: El valor de detección de SLP que elija en XClarity Orchestrator sustituye cualquier valor de detección de SLP elegido para las instancias de Lenovo XClarity Administrator que se gestionan mediante XClarity Orchestrator. Si el valor de detección de SLP se cambia en Lenovo XClarity Administrator, se sincronizará con XClarity Orchestrator.

- **Encapsulación en todos los dispositivos gestionados futuros** Indica si la encapsulación está habilitada durante la gestión de dispositivos.

La encapsulación está deshabilitada 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 la encapsulación está habilitada y el dispositivo admite la encapsulación, XClarity Orchestrator se comunica con el dispositivo (mediante el gestor de recursos) 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 del gestor de recursos elegido para gestionar el dispositivo.

Atención: Si se habilita la encapsulación y el gestor de recursos elegido para gestionar el dispositivo no está disponible antes de que se anule la gestión de un dispositivo, se deben realizar algunos pasos para deshabilitar la encapsulación y establecer comunicación con ese dispositivo.

- **Solicitud de registro habilitada** Indica si los gestores de recursos (Lenovo XClarity Administrator y Lenovo XClarity Management Hub) aceptan las solicitudes de detección de un controlador de gestión de la placa base cuando el controlador de gestión utiliza DNS para buscar instancias de gestor de recursos. Cuando está habilitada, el controlador de gestión puede registrarse con el gestor de recursos como un dispositivo detectado.
- **Limpeza de dispositivos offline.** Indica si se debe anular automáticamente la gestión de los dispositivos que están fuera de línea durante al menos la cantidad de tiempo especificada en **Tiempo de espera de dispositivos fuera de línea.** Cuando está habilitada, XClarity Orchestrator comprueba si hay dispositivos fuera de línea cada hora y cada vez que un usuario inicia sesión en el portal.
- **Tiempo de espera de dispositivos fuera de línea** Cantidad de tiempo, en horas, que los dispositivos deben estar fuera de línea antes de que se anule su gestión automáticamente. Este valor puede estar comprendido entre **1 y 24** horas. El valor predeterminado es **24** horas.

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

Gestión de servidores

Puede utilizar Lenovo XClarity Orchestrator para gestionar varios tipos de servidores.

Antes de empezar

Para realizar esta tarea, debe ser miembro de un grupo de usuarios al que se le haya asignado el rol de **Supervisor** o Administrador de **seguridad** predefinido.

Revise las consideraciones de gestión antes de gestionar un dispositivo (consulte [Consideraciones de gestión de dispositivos](#)).

Revise los valores globales de detección antes de gestionar un dispositivo (consulte [Configuración de valores globales de detección](#)).

Para detectar y gestionar dispositivos Edge que no responden al protocolo de detección de servicios, consulte [Gestión de dispositivos del cliente ThinkEdge](#).

La opción de gestión masiva solo está disponible para los servidores. No admite otros tipos de dispositivos.

Acerca de esta tarea

XClarity Orchestrator supervisa y gestiona dispositivos a través de gestores de recursos. Cuando se conecta a un gestor de recursos, XClarity Orchestrator gestiona todos los dispositivos que gestiona dicho gestor de recursos.

También puede gestionar dispositivos utilizando XClarity Orchestrator. XClarity Orchestrator muestra una lista de los dispositivos que ya se han detectado (pero no gestionado) mediante los gestores de recursos. Cuando gestiona dispositivos detectados desde XClarity Orchestrator, los dispositivos se gestionan mediante el gestor de recursos que los ha detectado. Cuando detecta y gestiona dispositivos manualmente utilizando direcciones IP, nombres de host o subredes, debe elegir qué gestor de recursos desea utilizar para gestionar los dispositivos. XClarity Management Hub se puede utilizar para gestionar dispositivos del cliente ThinkEdge. XClarity Management Hub 2.0 se puede utilizar para gestionar dispositivos ThinkServer. Lenovo XClarity Administrator se puede utilizar para gestionar servidores, almacenamiento, conmutadores y chasis.

Notas:

- Si intenta gestionar un dispositivo a través de XClarity Management Hub 2.0 y ese dispositivo ya se gestiona a través de otro XClarity Management Hub 2.0, XClarity Orchestrator elimina la cuenta de usuario de gestión y las suscripciones del dispositivo sin el reconocimiento de gestión anterior y luego gestiona el dispositivo de nuevo a través del nuevo concentrador de gestión. Tras este proceso, el dispositivo se sigue gestionando, pero sin conexión, desde el antiguo concentrador de gestión, pero el dispositivo ya no le envía datos. Tenga en cuenta que debe anular manualmente la gestión de los dispositivos del primer concentrador de gestión a través del portal conectado.
- Si intenta gestionar un dispositivo a través de XClarity Management Hub 2.0 y ese dispositivo ya se gestiona a través de otro XClarity Administrator, XClarity Orchestrator elimina la cuenta de usuario de gestión, las suscripciones y la información de LDAP y SSO que registra XCC mediante XClarity Administrator desde el dispositivo sin el reconocimiento de XClarity Administrator y, a continuación, gestiona el dispositivo de nuevo a través del nuevo XClarity Management Hub 2.0. Tras este proceso, el dispositivo se sigue gestionando, pero sin conexión, desde el concentrador XClarity Administrator, pero el dispositivo ya no le envía datos. Tenga en cuenta que debe anular manualmente la gestión de los dispositivos del XClarity Administrator a través del portal conectado.

Los gestores de recursos pueden detectar automáticamente los dispositivos siguientes utilizando un protocolo de detección de servicios.

- Servidores y dispositivos ThinkSystem y ThinkAgile
- Servidores ThinkEdge SE
- Chasis de Flex System y dispositivos ThinkSystem y Flex System en un chasis de Flex System
- Servidores de bastidor y torre de ThinkServer
- Servidores y dispositivos System x, Converged HX y NeXtScale
- Dispositivos de almacenamiento

Procedimiento

Para gestionar sus servidores, realice uno de los procedimientos siguientes.

- [Detección manual de servidores](#)
- [Gestionar servidores detectados](#)
- [Gestión de un *gran número* de servidores](#)

Detección manual de servidores

Para detectar manualmente la gestión de servidores específicos que no están en la misma subred que el servidor de Orchestrator, siga estos pasos.

1. En la barra de menús de XClarity Orchestrator, haga clic en **Recursos** (🔍) → **Nuevos dispositivos** para ver la tarjeta Detectar y gestionar nuevos dispositivos.
2. Haga clic en **Entrada manual** para mostrar el cuadro de diálogo Detectar nuevos dispositivos.
3. Seleccione **Dispositivos que responden al Protocolo de detección de servicios** y, a continuación, haga clic en **Siguiente**.
4. Seleccione **Manual** y, a continuación, haga clic en **Siguiente**.
5. Elija cómo desea detectar los dispositivos y, a continuación, especifique los valores apropiados.
 - **Direcciones IP/nombres de host.** Introduzca la dirección IP IPV4 o IPV6 o el nombre de dominio completo para cada dispositivo que desee gestionar (por ejemplo, 192.0.2.0 o d1.acme.com).
 - **Rangos IP.** Introduzca las direcciones IP de inicio y finalización del conjunto de dispositivos que desea gestionar.
 - **Subredes.** Introduzca la dirección IP y la máscara de la subred. XClarity Orchestrator analiza la subred en busca de dispositivos gestionables.
6. Seleccione el gestor de recursos que desee utilizar para gestionar los dispositivos.
7. Haga clic en **Detectar dispositivos**. Cuando el proceso de detección finaliza, los dispositivos detectados se enumeran en la tabla Nuevos dispositivos.

Gestionar servidores detectados

Para gestionar dispositivos que ya se han detectado, siga estos pasos.

1. En la barra de menús de XClarity Orchestrator, haga clic en **Recursos** (🔍) → **Nuevos dispositivos** para ver la tarjeta Detectar y gestionar nuevos dispositivos.



- Haga clic en **Todas las acciones** → **Actualizar** para detectar todos los dispositivos gestionables en el dominio de XClarity Orchestrator. La detección puede durar varios minutos.
- Seleccione uno o más servidores que desee gestionar.
- Haga clic en el icono de **Gestionar dispositivos seleccionados** (+) para mostrar el cuadro de diálogo Gestionar dispositivos detectados.
- Revise la lista de dispositivos seleccionados para gestionar y haga clic en **Siguiente**.
- Especifique el nombre de usuario y la contraseña para su autenticación en el servidor.

Consejo: se recomienda usar una cuenta de supervisor o administrador para gestionar el dispositivo. Si se utiliza una cuenta con autoridad de nivel inferior, puede que la gestión falle o que se haga correctamente, pero algunas características pueden fallar.

- Opcional:** seleccione **Crear una cuenta de recuperación y deshabilitar todos los usuarios locales** y, a continuación, especifique la contraseña de recuperación. Si se deshabilita, se utilizan las cuentas de usuarios locales para la autenticación.

Si se habilita, el gestor de recursos asignado crea una cuenta de usuario de autenticación gestionada y una cuenta de recuperación (RECOVERY_ID) en el servidor, mientras que el resto de las cuentas de usuarios locales se deshabilitan. El XClarity Orchestrator y el gestor de recursos usan la cuenta de usuario de autenticación gestionada para la autenticación. Si hay un problema con el XClarity Orchestrator o con el gestor de recursos y deja de funcionar por alguna razón, *tampoco* podrá iniciar sesión en el controlador de gestión de la placa base utilizando las cuentas de usuarios normales. Sin embargo, puede iniciar sesión utilizando la cuenta de RECOVERY_ID.

Importante: Asegúrese de guardar la contraseña de recuperación para utilizarla en el futuro.

Nota: Los servidores ThinkServer y System x M4 no admiten cuentas de recuperación.

- Opcional:** habilite **Establecer nueva contraseña si han caducado las credenciales** y, a continuación, especifique la nueva contraseña del servidor. Si la contraseña del servidor actual ha caducado, la

detección fallará hasta que se cambie la contraseña. Si especifica una nueva contraseña, las credenciales se cambian y el proceso de gestión puede continuar. La contraseña solo se cambia si la contraseña actual ha caducado.

9. Seleccione **Gestionar**. Se crea un trabajo para completar el proceso de gestión en segundo plano. Puede supervisar el estado del proceso de gestión desde el cuadro de diálogo o desde el registro de trabajos haciendo clic en **Supervisión** (🔍) → **Trabajos** (consulte [Supervisión de trabajos](#)).

Si no se realizó correctamente la gestión debido a una de las siguientes condiciones de error, repita este proceso mediante la opción Forzar gestión.

- El gestor de recursos ha fallado y no se puede recuperar.

Nota: Si la instancia del gestor de recursos de sustitución utiliza la misma dirección IP que el gestor de recursos que ha fallado, puede volver a gestionar el dispositivo utilizando la cuenta y la contraseña de RECOVERY_ID (si procede) y la opción **Forzar gestión**.

- El gestor de recursos se desactivó antes de que se anulara la gestión de los dispositivos.
- No se anuló correctamente la gestión de los dispositivos.
- XClarity Orchestrator muestra un dispositivo gestionado como fuera de línea después de cambiar la dirección IP del dispositivo.

Gestión de un gran número de servidores

Para gestionar un gran número de servidores, siga estos pasos.

1. En la barra de menús de XClarity Orchestrator, haga clic en **Recursos** (⚙️) → **Nuevos dispositivos** para ver la tarjeta Detectar y gestionar nuevos dispositivos.
2. Haga clic en el botón **Gestión masiva** para mostrar el cuadro de diálogo Gestión masiva.
3. Seleccione el gestor de recursos que desee utilizar para gestionar los dispositivos.
4. Introduzca la dirección IP o el nombre de dominio completo de cada servidor que desee gestionar, separados por una coma (por ejemplo 192.0.2.0, d1.acme.com).

Importante:

- Todos estos servidores especificados deben utilizar las mismas credenciales.
- Los FQDN solo pueden contener caracteres alfanuméricos, puntos y guiones.

5. Haga clic en **Siguiente**.
6. Especifique el nombre de usuario y la contraseña para su autenticación en el servidor.

Consejo: se recomienda usar una cuenta de supervisor o administrador para gestionar el dispositivo. Si se utiliza una cuenta con autoridad de nivel inferior, puede que la gestión falle o que se haga correctamente, pero algunas características pueden fallar.

7. **Opcional:** seleccione **Crear una cuenta de recuperación y deshabilitar todos los usuarios locales** y, a continuación, especifique la contraseña de recuperación. Si se deshabilita, se utilizan las cuentas de usuarios locales para la autenticación.

Si se habilita, el gestor de recursos asignado crea una cuenta de usuario de autenticación gestionada y una cuenta de recuperación (RECOVERY_ID) en el servidor, mientras que el resto de las cuentas de usuarios locales se deshabilitan. El XClarity Orchestrator y el gestor de recursos usan la cuenta de usuario de autenticación gestionada para la autenticación. Si hay un problema con el XClarity Orchestrator o con el gestor de recursos y deja de funcionar por alguna razón, *tampoco* podrá iniciar sesión en el controlador de gestión de la placa base utilizando las cuentas de usuarios normales. Sin embargo, puede iniciar sesión utilizando la cuenta de RECOVERY_ID.

Importante: Asegúrese de guardar la contraseña de recuperación para utilizarla en el futuro.

Nota: Los servidores ThinkServer y System x M4 no admiten cuentas de recuperación.

8. **Opcional:** habilite **Establecer nueva contraseña si han caducado las credenciales** y, a continuación, especifique la nueva contraseña del servidor. Si la contraseña del servidor actual ha caducado, la detección fallará hasta que se cambie la contraseña. Si especifica una nueva contraseña, las credenciales se cambian y el proceso de gestión puede continuar. La contraseña solo se cambia si la contraseña actual ha caducado.
9. Seleccione **Gestionar**. Se crea un trabajo para completar el proceso de gestión en segundo plano. Puede supervisar el estado del proceso de gestión desde el cuadro de diálogo o desde el registro de trabajos haciendo clic en **Supervisión** (📄) → **Trabajos** (consulte [Supervisión de trabajos](#)).

Si no se realizó correctamente la gestión debido a una de las siguientes condiciones de error, repita este proceso mediante la opción Forzar gestión.

- El gestor de recursos ha fallado y no se puede recuperar.

Nota: Si la instancia del gestor de recursos de sustitución utiliza la misma dirección IP que el gestor de recursos que ha fallado, puede volver a gestionar el dispositivo utilizando la cuenta y la contraseña de RECOVERY_ID (si procede) y la opción **Forzar gestión**.

- El gestor de recursos se desactivó antes de que se anulara la gestión de los dispositivos.
- No se anuló correctamente la gestión de los dispositivos.
- XClarity Orchestrator muestra un dispositivo gestionado como fuera de línea después de cambiar la dirección IP del dispositivo.

Después de finalizar

Puede realizar las acciones siguientes en el dispositivo gestionado.

- Supervisar el estado y los detalles del dispositivo (consulte [Visualización del estado de los dispositivos](#) y [Visualización de los detalles del dispositivo](#)).
- No gestionar y quitar un dispositivo seleccionado. Para ello, haga clic en **Recursos** (🔍) y, a continuación, haga clic en el tipo de dispositivo en el panel de navegación izquierdo para mostrar una tarjeta con una vista de tabla de todos los dispositivos gestionados de ese tipo, seleccione los dispositivos para no gestionar y, después, haga clic en el icono de **No gestionar** (🗑️).

Notas:

- Puede anular la gestión de un máximo de **50** dispositivos a la vez.
- Asegúrese de que no haya trabajos activos en ejecución en el dispositivo.
- Si XClarity Orchestrator no puede conectarse con el gestor de recursos (por ejemplo, si las credenciales han caducado o si hay problemas de red), seleccione **Forzar anulación de gestión incluso si no se puede acceder al dispositivo**.
- De forma predeterminada, la gestión de los dispositivos gestionados mediante XClarity Administrator y que están fuera de línea durante 24 horas o más se anula automáticamente (consulte [Configuración de valores globales de detección](#)).
- En la mayoría de los dispositivos, se conserva determinada información acerca del dispositivo una vez que se ha anulado su gestión. Cuando no se gestionan dispositivos:
 - La cuenta de usuario de gestión y las suscripciones de sucesos y métricas se eliminan del dispositivo.
 - En el caso de dispositivos gestionados mediante XClarity Administrator, si la función Llamar a casa está habilitada en XClarity Administrator, se deshabilita en el dispositivo.
 - Para los dispositivos gestionados mediante XClarity Administrator, si la encapsulación está habilitada en el dispositivo, las reglas de firewall del dispositivo se cambian a los valores que tenía el dispositivo antes de que se gestionara.

- La información sensible, el inventario y los sucesos y las alertas que ha generado el dispositivo se descartan en el concentrador de gestión.
- Los sucesos y alertas que el concentrador de gestión ha generado para el dispositivo se mantienen en el concentrador de gestión.

Gestión de dispositivos del cliente ThinkEdge

Los dispositivos del cliente ThinkEdge no tienen controladores de gestión de la placa base y, por lo tanto, no se pueden detectar mediante protocolos de detección de servicio. Debe instalar un agente de Universal Device Client (UDC) en los dispositivos del cliente ThinkEdge para que el gestor de recursos de Lenovo XClarity Management Hub asignado pueda detectar y gestionar de forma segura los dispositivos. Solo los gestores de recursos de Lenovo XClarity Management Hub pueden detectar y gestionar estos dispositivos.

Antes de empezar

Revise las consideraciones de gestión antes de gestionar un dispositivo (consulte [Consideraciones de gestión de dispositivos](#)).

Asegúrese de que al menos un gestor de recursos de Lenovo XClarity Management Hub esté conectado a XClarity Orchestrator (consulte [Conexión de gestores de recursos](#)).

Para realizar esta tarea, debe ser miembro de un grupo de usuarios al que se le haya asignado el rol de **Supervisor** o Administrador de **seguridad** predefinido.

Asegúrese de que las Credenciales de UDS Portal estén configuradas con el ID y el secreto de cliente. Las credenciales se utilizan para firmar la política que se utiliza en el paquete de aprovisionamiento del cliente. El UDS Portal es el origen de confianza para firmar esta política para que el agente de UDC funcione correctamente. Para configurar las credenciales, haga clic en **Recursos** (⚙️) → **Nuevos dispositivos** en la barra de menús, después en **Credenciales de UDS Portal** y, a continuación, introduzca el ID y el secreto de cliente. Debe solicitar el ID y secreto de cliente de Lenovo enviando un correo electrónico a uedmcredreq@lenovo.com, utilizando “Credenciales de UDS Portal” en la descripción del correo electrónico e incluya el nombre de su empresa, la información de contacto (correo electrónico o número de teléfono) y el número de cliente de Lenovo de 10 dígitos.

Asegúrese de que un agente UDC *no esté* instalado actualmente en el dispositivo del cliente ThinkEdge. Si hay instalado un agente de UDC, debe desinstalarlo ejecutando los comandos siguientes. Debe tener privilegios de nivel superior para instalar el agente de UDC.

- **Linux**
`sudo apt purge udc-release`
- **Windows**
`PUSHD %windir%\System32\drivers\Lenovo\udc\Data\InfBackup\.\UDCInfInstaller.exe -uninstall`

`POPD`

Asegúrese de que el servidor DNS esté configurado para incluir los dominios siguientes, donde *(hub-domain)* es el nombre de dominio completo del gestor de recursos de XClarity Management Hub que desea utilizar para gestionar los dispositivos del cliente ThinkEdge.

- `api.(hub-domain)`
- `api-mtls.(hub-domain)`
- `auth.(hub-domain)`
- `mqtt.(hub-domain)`
- `mqtt-mtls.(hub-domain)`
- `s3.(hub-domain)`
- `s3console.(hub-domain)`

Acerca de esta tarea

XClarity Orchestrator supervisa y gestiona dispositivos a través de gestores de recursos. Cuando se conecta a un gestor de recursos, XClarity Orchestrator gestiona todos los dispositivos que gestiona dicho gestor de recursos.

También puede gestionar dispositivos utilizando XClarity Orchestrator. XClarity Orchestrator muestra una lista de los dispositivos que ya se han detectado (pero no gestionado) mediante los gestores de recursos. Cuando gestiona dispositivos detectados desde XClarity Orchestrator, los dispositivos se gestionan mediante el gestor de recursos que los ha detectado. Cuando detecta y gestiona dispositivos manualmente utilizando direcciones IP, nombres de host o subredes, debe elegir qué gestor de recursos desea utilizar para gestionar los dispositivos. XClarity Management Hub se puede utilizar para gestionar dispositivos del cliente ThinkEdge. XClarity Management Hub 2.0 se puede utilizar para gestionar dispositivos ThinkServer. Lenovo XClarity Administrator se puede utilizar para gestionar servidores, almacenamiento, conmutadores y chasis.

Encontrará una lista completa de los dispositivos de cliente ThinkEdge compatibles en el [Sitio web de soporte de Lenovo XClarity](#), haciendo clic en la pestaña **Compatibilidad** y, a continuación, haciendo clic en el enlace para los tipos de dispositivo correspondientes.

Nota: Los servidores ThinkEdge (como SE350, SE360 y SE450) tienen controladores de gestión de placa base y se pueden detectar mediante un protocolo de detección de servicios. Para gestionar estos dispositivos, consulte [Gestión de servidores](#).

Procedimiento

Para detectar y gestionar dispositivos del cliente ThinkEdge, siga estos pasos.

1. Instale el agente de UDC en cada dispositivo del cliente ThinkEdge.
 - a. En la barra de menús de XClarity Orchestrator, haga clic en **Recursos** (🔍) → **Nuevos dispositivos** para ver la tarjeta Detectar y gestionar nuevos dispositivos.
 - b. Haga clic en **Entrada manual** para mostrar el cuadro de diálogo Detectar nuevos dispositivos.
 - c. Seleccione **Dispositivos que no responden al Protocolo de detección de servicios** y, a continuación, haga clic en **Siguiente**.
 - d. Seleccione la dirección IP del gestor de recursos de XClarity Management Hub que desee utilizar para gestionar los dispositivos del cliente ThinkEdge. Solo pueden seleccionarse los gestores de recursos de XClarity Management Hub cuyo estado sea correcto.
 - e. Seleccione el tipo de sistema operativo que está instalado en el servidor.
 - **Linux ARM**
 - **Linux x86**
 - **Windows**
 - f. Seleccione el número de días antes de que el instalador del agente de UDC quede inutilizado tras su descarga. El valor predeterminado es **30** días.
 - g. Seleccione las veces que tiene pensado instalar el agente de UDC en un servidor. Normalmente, este es el número de dispositivos en los que necesita instalar el agente de UDC. Puede especificar hasta un máximo **1 000 000** usos; el valor predeterminado es **10** usos.
 - h. Haga clic en **Descargar el Agente de UDC** para descargar el instalador del agente de UDC en su sistema local. Se crea un trabajo para completar el proceso de descarga en segundo plano. Puede supervisar el estado del proceso de descarga desde el cuadro de diálogo o desde el registro de trabajos haciendo clic en **Supervisión** (📄) → **Trabajos** (consulte [Supervisión de trabajos](#)).
 - i. Haga clic en **Cerrar** para cerrar el cuadro de diálogo.

- j. Copie el instalador del agente de UDC en cada dispositivo del cliente ThinkEdge adecuado, desempaque/descomprima el paquete y, a continuación, instale el agente de UDC en esos dispositivos mediante el siguiente comando. Para instalar el agente, debe tener privilegios de **administrador**.

- **Linux** `install.sh`
- **Windows** `setup.cmd`

Una vez que el agente de UDC se haya instalado correctamente en cada dispositivo del cliente de ThinkEdge, el gestor de recursos de XClarity Management Hub seleccionado puede detectar automáticamente los dispositivos.

2. Gestione los dispositivos del cliente ThinkEdge.

- a. En la barra de menús de XClarity Orchestrator, haga clic en **Recursos** (🔍) → **Nuevos dispositivos** para ver la tarjeta Detectar y gestionar nuevos dispositivos.

Nota: Es posible que las direcciones IP tarden en aparecer en la tabla.

Descubrir y gestionar nuevos dispositivos

Haga clic en **Configuración** para definir los valores de detección globales.
 Haga clic en **Credenciales de UDS Portal** para establecer las credenciales de UDS Portal necesarias para descargar paquetes de aprovisionamiento de UDC para dispositivos que no responden a un protocolo de detección de servicios.
 Si la siguiente lista no contiene el dispositivo que espera, utilice la opción **Entrada manual** para detectar el dispositivo.
 Para obtener más información acerca de la causa por la que es posible que el dispositivo no se detecte automáticamente, consulte el siguiente tema de ayuda: [No se puede detectar un dispositivo](#).

🔍 Entrada manual ⚙️ Configuración 🔑 Credenciales de UDS Portal

Nuevos dispositivos

🔄 + 👉 Todas las acciones ▾ Filtros ▾ 🔍 Buscar ✕

<input type="checkbox"/>	Dispositivo detectado	Direcciones IP	Número de serie	Tipo-Modelo	Tipo	Detectado por
<input type="checkbox"/>	G8052-1	10.241.5.1, 10.	Y010CM345...	7309/HC1 (...)	Switch	10.241.5.134
<input type="checkbox"/>	G8052-2	10.241.5.254, 1	Y010CM35C...	7309/HC1 (...)	Switch	10.241.5.134
<input type="checkbox"/>	Shanghai-SD...	10.241.5.42, 1C	1234567890	7D75/CTO1...	Server	10.241.5.134

0 Seleccionado / 3 Total Filas por página: 10 ▾

- b. Haga clic en **Todas las acciones** → **Actualizar** para detectar todos los dispositivos gestionables en el dominio de XClarity Orchestrator. La detección puede durar varios minutos.
- c. Seleccione los dispositivos del cliente ThinkEdge que desee gestionar.
- d. Haga clic en el icono de **Gestionar** (⊕) para mostrar el cuadro de diálogo Gestionar dispositivos.
- e. Revise la lista de dispositivos seleccionados para gestionar.
- f. Seleccione **Gestionar**. Se crea un trabajo para completar el proceso de gestión en segundo plano. Puede supervisar el estado del proceso de gestión desde el cuadro de diálogo o desde el registro de trabajos haciendo clic en **Supervisión** (📄) → **Trabajos** (consulte [Supervisión de trabajos](#)).

Si no se realizó correctamente la gestión debido a una de las siguientes condiciones de error, repita este proceso mediante la opción Forzar gestión.

- El gestor de recursos ha fallado y no se puede recuperar.

Nota: Si la instancia del gestor de recursos de sustitución utiliza la misma dirección IP que el gestor de recursos que ha fallado, puede volver a gestionar el dispositivo utilizando la cuenta y la contraseña de RECOVERY_ID (si procede) y la opción **Forzar gestión**.

- El gestor de recursos se desactivó antes de que se anulara la gestión de los dispositivos.
- No se anuló correctamente la gestión de los dispositivos.
- XClarity Orchestrator muestra un dispositivo gestionado como fuera de línea después de cambiar la dirección IP del dispositivo.

Después de finalizar

Puede realizar las acciones siguientes en el dispositivo gestionado.

- Supervisar el estado y los detalles del dispositivo (consulte [Visualización del estado de los dispositivos y Visualización de los detalles del dispositivo](#)).
- No gestionar y quitar un dispositivo seleccionado. Para ello, haga clic en **Recursos** (🔍) y, a continuación, haga clic en el tipo de dispositivo en el panel de navegación izquierdo para mostrar una tarjeta con una vista de tabla de todos los dispositivos gestionados de ese tipo, seleccione los dispositivos para no gestionar y, después, haga clic en el icono de **No gestionar** (🗑️).

Notas:

- Puede anular la gestión de un máximo de **50** dispositivos a la vez.
- Asegúrese de que no haya trabajos activos en ejecución en el dispositivo.
- Si XClarity Orchestrator no puede conectarse con el gestor de recursos (por ejemplo, si las credenciales han caducado o si hay problemas de red), seleccione **Forzar anulación de gestión incluso si no se puede acceder al dispositivo**.
- De forma predeterminada, la gestión de los dispositivos gestionados mediante XClarity Administrator y que están fuera de línea durante 24 horas o más se anula automáticamente (consulte [Configuración de valores globales de detección](#)).
- En la mayoría de los dispositivos, se conserva determinada información acerca del dispositivo una vez que se ha anulado su gestión. Cuando no se gestionan dispositivos:
 - La cuenta de usuario de gestión y las suscripciones de sucesos y métricas se eliminan del dispositivo.
 - En el caso de dispositivos gestionados mediante XClarity Administrator, si la función Llamar a casa está habilitada en XClarity Administrator, se deshabilita en el dispositivo.
 - Para los dispositivos gestionados mediante XClarity Administrator, si la encapsulación está habilitada en el dispositivo, las reglas de firewall del dispositivo se cambian a los valores que tenía el dispositivo antes de que se gestionara.
 - La información sensible, el inventario y los sucesos y las alertas que ha generado el dispositivo se descartan en el concentrador de gestión.
 - Los sucesos y alertas que el concentrador de gestión ha generado para el dispositivo se mantienen en el concentrador de gestión.

Gestión de los dispositivos de almacenamiento

Lenovo XClarity Orchestrator puede gestionar varios tipos de dispositivos de almacenamiento, dispositivos y bibliotecas de cintas de Lenovo.

Antes de empezar

Para realizar esta tarea, debe ser miembro de un grupo de usuarios al que se le haya asignado el rol de **Supervisor** o Administrador de **seguridad** predefinido.

Revise las consideraciones de gestión antes de gestionar un dispositivo (consulte [Consideraciones de gestión de dispositivos](#)).

Para detectar y gestionar dispositivos Edge que no responden al protocolo de detección de servicios, consulte [Gestión de dispositivos del cliente ThinkEdge](#).

La opción de gestión masiva solo está disponible para los servidores. No admite otros tipos de dispositivos.

Acerca de esta tarea

XClarity Orchestrator supervisa y gestiona dispositivos a través de gestores de recursos. Cuando se conecta a un gestor de recursos, XClarity Orchestrator gestiona todos los dispositivos que gestiona dicho gestor de recursos.

También puede gestionar dispositivos utilizando XClarity Orchestrator. XClarity Orchestrator muestra una lista de los dispositivos que ya se han detectado (pero no gestionado) mediante los gestores de recursos. Cuando gestiona dispositivos detectados desde XClarity Orchestrator, los dispositivos se gestionan mediante el gestor de recursos que los ha detectado. Cuando detecta y gestiona dispositivos manualmente utilizando direcciones IP, nombres de host o subredes, debe elegir qué gestor de recursos desea utilizar para gestionar los dispositivos. XClarity Management Hub se puede utilizar para gestionar dispositivos del cliente ThinkEdge. XClarity Management Hub 2.0 se puede utilizar para gestionar dispositivos ThinkServer. Lenovo XClarity Administrator se puede utilizar para gestionar servidores, almacenamiento, conmutadores y chasis.

Procedimiento

Para gestionar sus dispositivos de almacenamiento, realice uno de los procedimientos siguientes.

- [Detección manual de dispositivos de almacenamiento](#)
- [Gestionar dispositivos de almacenamiento detectados](#)

Detección manual de dispositivos de almacenamiento

Para detectar manualmente y gestionar dispositivos de almacenamiento específicos que no están en la misma subred que el servidor de Orchestrator, siga estos pasos.

1. En la barra de menú de XClarity Orchestrator, haga clic en **Recursos** (⚙️) → **Nuevos dispositivos** para ver la tarjeta Detectar y gestionar nuevos dispositivos.
2. Haga clic en **Entrada manual** para mostrar el cuadro de diálogo Detectar nuevos dispositivos.
3. Seleccione **Dispositivos que responden al Protocolo de detección de servicios** y, a continuación, haga clic en **Siguiente**.
4. Seleccione **Manual** y, a continuación, haga clic en **Siguiente**.
5. Elija cómo desea detectar los dispositivos y, a continuación, especifique los valores apropiados.
 - **Direcciones IP/nombres de host.** Introduzca la dirección IP IPV4 o IPV6 o el nombre de dominio completo para cada dispositivo que desee gestionar (por ejemplo, 192.0.2.0 o d1.acme.com).
 - **Rangos IP.** Introduzca las direcciones IP de inicio y finalización del conjunto de dispositivos que desea gestionar.
 - **Subredes.** Introduzca la dirección IP y la máscara de la subred. XClarity Orchestrator analiza la subred en busca de dispositivos gestionables.
6. Seleccione el gestor de recursos que desee utilizar para gestionar los dispositivos.

- Haga clic en **Detectar dispositivos**. Cuando el proceso de detección finaliza, los dispositivos detectados se enumeran en la tabla Nuevos dispositivos.

Gestionar dispositivos de almacenamiento detectados

Para gestionar dispositivos que ya se han detectado, siga estos pasos.

- En la barra de menús de XClarity Orchestrator, haga clic en **Recursos** (🔍) → **Nuevos dispositivos** para ver la tarjeta Detectar y gestionar nuevos dispositivos.

Descubrir y gestionar nuevos dispositivos

Haga clic en **Configuración** para definir los valores de detección globales.
Haga clic en **Credenciales de UDS Portal** para establecer las credenciales de UDS Portal necesarias para descargar paquetes de aprovisionamiento de UDC para dispositivos que no responden a un protocolo de detección de servicios.
Si la siguiente lista no contiene el dispositivo que espera, utilice la opción **Entrada manual** para detectar el dispositivo.
Para obtener más información acerca de la causa por la que es posible que el dispositivo no se detecte automáticamente, consulte el siguiente tema de ayuda: [No se puede detectar un dispositivo](#).

⊕ Entrada manual ⚙ Configuración 🔑 Credenciales de UDS Portal

Nuevos dispositivos

🔄 ⊕ 📄 Todas las acciones ▾ Filtros ▾ 🔍 Buscar ✕

<input type="checkbox"/>	Dispositivo detectado	Direcciones IP	Número de serie	Tipo-Modelo	Tipo	Detectado por
<input type="checkbox"/>	G8052-1	10.241.5.1, 10.241.5.2	Y010CM345...	7309/HC1 (...)	Switch	10.241.5.134
<input type="checkbox"/>	G8052-2	10.241.5.254, 10.241.5.1	Y010CM35C...	7309/HC1 (...)	Switch	10.241.5.134
<input type="checkbox"/>	Shanghai-SD...	10.241.5.42, 10.241.5.1	1234567890	7D75/CTO1...	Server	10.241.5.134

0 Seleccionado / 3 Total Filas por página: 10 ▾

- Haga clic en **Todas las acciones** → **Actualizar** para detectar todos los dispositivos gestionables en el dominio de XClarity Orchestrator. La detección puede durar varios minutos.
- Seleccione el sistema o los dispositivos de almacenamiento que desee gestionar.
- Haga clic en el icono de **Gestionar dispositivos seleccionados** (⊕) para mostrar el cuadro de diálogo Gestionar dispositivos detectados.
- Revise la lista de dispositivos seleccionados para gestionar y haga clic en **Siguiente**.
- Especifique el nombre de usuario y la contraseña para su autenticación en el servidor.

Consejo: se recomienda usar una cuenta de supervisor o administrador para gestionar el dispositivo. Si se utiliza una cuenta con autoridad de nivel inferior, puede que la gestión falle o que se haga correctamente, pero algunas características pueden fallar.

- Seleccione **Gestionar**. Se crea un trabajo para completar el proceso de gestión en segundo plano. Puede supervisar el estado del proceso de gestión desde el cuadro de diálogo o desde el registro de trabajos haciendo clic en **Supervisión** (📧) → **Trabajos** (consulte [Supervisión de trabajos](#)).

Si no se realizó correctamente la gestión debido a una de las siguientes condiciones de error, repita este proceso mediante la opción Forzar gestión.

- El gestor de recursos ha fallado y no se puede recuperar.

Nota: Si la instancia del gestor de recursos de sustitución utiliza la misma dirección IP que el gestor de recursos que ha fallado, puede volver a gestionar el dispositivo utilizando la cuenta y la contraseña de RECOVERY_ID (si procede) y la opción **Forzar gestión**.

- El gestor de recursos se desactivó antes de que se anulara la gestión de los dispositivos.
- No se anuló correctamente la gestión de los dispositivos.
- XClarity Orchestrator muestra un dispositivo gestionado como fuera de línea después de cambiar la dirección IP del dispositivo.

Después de finalizar

Puede realizar las acciones siguientes en el dispositivo gestionado.

- Supervisar el estado y los detalles del dispositivo (consulte [Visualización del estado de los dispositivos](#) y [Visualización de los detalles del dispositivo](#)).
- No gestionar y quitar un dispositivo seleccionado. Para ello, haga clic en **Recursos** (🔍) y, a continuación, haga clic en el tipo de dispositivo en el panel de navegación izquierdo para mostrar una tarjeta con una vista de tabla de todos los dispositivos gestionados de ese tipo, seleccione los dispositivos para no gestionar y, después, haga clic en el icono de **No gestionar** (🗑️).

Notas:

- Puede anular la gestión de un máximo de **50** dispositivos a la vez.
- Asegúrese de que no haya trabajos activos en ejecución en el dispositivo.
- Si XClarity Orchestrator no puede conectarse con el gestor de recursos (por ejemplo, si las credenciales han caducado o si hay problemas de red), seleccione **Forzar anulación de gestión incluso si no se puede acceder al dispositivo**.
- De forma predeterminada, la gestión de los dispositivos gestionados mediante XClarity Administrator y que están fuera de línea durante 24 horas o más se anula automáticamente (consulte [Configuración de valores globales de detección](#)).
- En la mayoría de los dispositivos, se conserva determinada información acerca del dispositivo una vez que se ha anulado su gestión. Cuando no se gestionan dispositivos:
 - La cuenta de usuario de gestión y las suscripciones de sucesos y métricas se eliminan del dispositivo.
 - En el caso de dispositivos gestionados mediante XClarity Administrator, si la función Llamar a casa está habilitada en XClarity Administrator, se deshabilita en el dispositivo.
 - Para los dispositivos gestionados mediante XClarity Administrator, si la encapsulación está habilitada en el dispositivo, las reglas de firewall del dispositivo se cambian a los valores que tenía el dispositivo antes de que se gestionara.
 - La información sensible, el inventario y los sucesos y las alertas que ha generado el dispositivo se descartan en el concentrador de gestión.
 - Los sucesos y alertas que el concentrador de gestión ha generado para el dispositivo se mantienen en el concentrador de gestión.

Gestión del chasis

Lenovo XClarity Orchestrator puede gestionar varios tipos de chasis y componentes de chasis.

Antes de empezar

Para realizar esta tarea, debe ser miembro de un grupo de usuarios al que se le haya asignado el rol de **Supervisor** o Administrador de **seguridad** predefinido.

Revise las consideraciones de gestión antes de gestionar un dispositivo (consulte [Consideraciones de gestión de dispositivos](#)).

Para detectar y gestionar dispositivos Edge que no responden al protocolo de detección de servicios, consulte [Gestión de dispositivos del cliente ThinkEdge](#).

La opción de gestión masiva solo está disponible para los servidores. No admite otros tipos de dispositivos.

Acerca de esta tarea

XClarity Orchestrator supervisa y gestiona dispositivos a través de gestores de recursos. Cuando se conecta a un gestor de recursos, XClarity Orchestrator gestiona todos los dispositivos que gestiona dicho gestor de recursos.

También puede gestionar dispositivos utilizando XClarity Orchestrator. XClarity Orchestrator muestra una lista de los dispositivos que ya se han detectado (pero no gestionado) mediante los gestores de recursos. Cuando gestiona dispositivos detectados desde XClarity Orchestrator, los dispositivos se gestionan mediante el gestor de recursos que los ha detectado. Cuando detecta y gestiona dispositivos manualmente utilizando direcciones IP, nombres de host o subredes, debe elegir qué gestor de recursos desea utilizar para gestionar los dispositivos. XClarity Management Hub se puede utilizar para gestionar dispositivos del cliente ThinkEdge. XClarity Management Hub 2.0 se puede utilizar para gestionar dispositivos ThinkServer. Lenovo XClarity Administrator se puede utilizar para gestionar servidores, almacenamiento, conmutadores y chasis.

Procedimiento

Para gestionar sus chasis, realice uno de los procedimientos siguientes.

- [Detección manual del chasis](#)
- [Gestionar chasis detectado](#)

Detección manual del chasis

Para detectar manualmente y gestionar chasis específicos que no están en la misma subred que el servidor de Orchestrator, siga estos pasos.

1. En la barra de menús de XClarity Orchestrator, haga clic en **Recursos** (⚙️) → **Nuevos dispositivos** para ver la tarjeta Detectar y gestionar nuevos dispositivos.
2. Haga clic en **Entrada manual** para mostrar el cuadro de diálogo Detectar nuevos dispositivos.
3. Seleccione **Dispositivos que responden al Protocolo de detección de servicios** y, a continuación, haga clic en **Siguiente**.
4. Seleccione **Manual** y, a continuación, haga clic en **Siguiente**.
5. Elija cómo desea detectar los dispositivos y, a continuación, especifique los valores apropiados.
 - **Direcciones IP/nombres de host.** Introduzca la dirección IP IPV4 o IPV6 o el nombre de dominio completo para cada dispositivo que desee gestionar (por ejemplo, 192.0.2.0 o d1.acme.com).
 - **Rangos IP.** Introduzca las direcciones IP de inicio y finalización del conjunto de dispositivos que desea gestionar.
 - **Subredes.** Introduzca la dirección IP y la máscara de la subred. XClarity Orchestrator analiza la subred en busca de dispositivos gestionables.
6. Seleccione el gestor de recursos que desee utilizar para gestionar los dispositivos.
7. Haga clic en **Detectar dispositivos**. Cuando el proceso de detección finaliza, los dispositivos detectados se enumeran en la tabla Nuevos dispositivos.

Gestionar chasis detectado

Para gestionar dispositivos que ya se han detectado, siga estos pasos.

1. En la barra de menús de XClarity Orchestrator, haga clic en **Recursos** (🔍) → **Nuevos dispositivos** para ver la tarjeta Detectar y gestionar nuevos dispositivos.

Descubrir y gestionar nuevos dispositivos

Haga clic en **Configuración** para definir los valores de detección globales.
Haga clic en **Credenciales de UDS Portal** para establecer las credenciales de UDS Portal necesarias para descargar paquetes de aprovisionamiento de UDC para dispositivos que no responden a un protocolo de detección de servicios.
Si la siguiente lista no contiene el dispositivo que espera, utilice la opción **Entrada manual** para detectar el dispositivo.
Para obtener más información acerca de la causa por la que es posible que el dispositivo no se detecte automáticamente, consulte el siguiente tema de ayuda: [No se puede detectar un dispositivo.](#)

🔍 Entrada manual ⚙️ Configuración 🔄 Credenciales de UDS Portal

Nuevos dispositivos

🔄 📄 Todas las acciones ▼ Filtros ▼ 🔍 Buscar ✕

<input type="checkbox"/>	Dispositivo detectado	Direcciones IP	Número de serie	Tipo-Modelo	Tipo	Detectado por
<input type="checkbox"/>	G8052-1	10.241.5.1, 10.	Y010CM345...	7309/HC1 (...)	Switch	10.241.5.134
<input type="checkbox"/>	G8052-2	10.241.5.254, 1	Y010CM35C...	7309/HC1 (...)	Switch	10.241.5.134
<input type="checkbox"/>	Shanghai-SD...	10.241.5.42, 10	1234567890	7D75/CTO1...	Server	10.241.5.134

0 Seleccionado / 3 Total Filas por página: 10 ▼

2. Haga clic en **Todas las acciones** → **Actualizar** para detectar todos los dispositivos gestionables en el dominio de XClarity Orchestrator. La detección puede durar varios minutos.
3. Seleccione el chasis o los chasis que desee gestionar.
4. Haga clic en el icono de **Gestionar dispositivos seleccionados** (⊕) para mostrar el cuadro de diálogo Gestionar dispositivos detectados.
5. Revise la lista de dispositivos seleccionados para gestionar y haga clic en **Siguiente**.
6. Especifique el nombre de usuario y la contraseña para su autenticación en el servidor.

Consejo: se recomienda usar una cuenta de supervisor o administrador para gestionar el dispositivo. Si se utiliza una cuenta con autoridad de nivel inferior, puede que la gestión falle o que se haga correctamente, pero algunas características pueden fallar.

7. **Opcional:** seleccione **Crear una cuenta de recuperación y deshabilitar todos los usuarios locales** y, a continuación, especifique la contraseña de recuperación. Si se deshabilita, se utilizan las cuentas de usuarios locales para la autenticación.

Si se habilita, el gestor de recursos asignado crea una cuenta de usuario de autenticación gestionada y una cuenta de recuperación (RECOVERY_ID) en el servidor, mientras que el resto de las cuentas de usuarios locales se deshabilitan. El XClarity Orchestrator y el gestor de recursos usan la cuenta de usuario de autenticación gestionada para la autenticación. Si hay un problema con el XClarity Orchestrator o con el gestor de recursos y deja de funcionar por alguna razón, *tampoco* podrá iniciar sesión en el controlador de gestión de la placa base utilizando las cuentas de usuarios normales. Sin embargo, puede iniciar sesión utilizando la cuenta de RECOVERY_ID.

Importante: Asegúrese de guardar la contraseña de recuperación para utilizarla en el futuro.

Nota: Los servidores ThinkServer y System x M4 no admiten cuentas de recuperación.

8. **Opcional:** habilite **Establecer nueva contraseña si han caducado las credenciales** y, a continuación, especifique la nueva contraseña del servidor. Si la contraseña del servidor actual ha caducado, la detección fallará hasta que se cambie la contraseña. Si especifica una nueva contraseña, las credenciales se cambian y el proceso de gestión puede continuar. La contraseña solo se cambia si la contraseña actual ha caducado.
9. Seleccione **Gestionar**. Se crea un trabajo para completar el proceso de gestión en segundo plano. Puede supervisar el estado del proceso de gestión desde el cuadro de diálogo o desde el registro de trabajos haciendo clic en **Supervisión** (📄) → **Trabajos** (consulte [Supervisión de trabajos](#)).

Si no se realizó correctamente la gestión debido a una de las siguientes condiciones de error, repita este proceso mediante la opción Forzar gestión.

- El gestor de recursos ha fallado y no se puede recuperar.

Nota: Si la instancia del gestor de recursos de sustitución utiliza la misma dirección IP que el gestor de recursos que ha fallado, puede volver a gestionar el dispositivo utilizando la cuenta y la contraseña de RECOVERY_ID (si procede) y la opción **Forzar gestión**.

- El gestor de recursos se desactivó antes de que se anulara la gestión de los dispositivos.
- No se anuló correctamente la gestión de los dispositivos.
- XClarity Orchestrator muestra un dispositivo gestionado como fuera de línea después de cambiar la dirección IP del dispositivo.

Después de finalizar

Puede realizar las acciones siguientes en el dispositivo gestionado.

- Supervisar el estado y los detalles del dispositivo (consulte [Visualización del estado de los dispositivos](#) y [Visualización de los detalles del dispositivo](#)).
- No gestionar y quitar un dispositivo seleccionado. Para ello, haga clic en **Recursos** (📁) y, a continuación, haga clic en el tipo de dispositivo en el panel de navegación izquierdo para mostrar una tarjeta con una vista de tabla de todos los dispositivos gestionados de ese tipo, seleccione los dispositivos para no gestionar y, después, haga clic en el icono de **No gestionar** (🗑️).

Notas:

- Puede anular la gestión de un máximo de **50** dispositivos a la vez.
- Asegúrese de que no haya trabajos activos en ejecución en el dispositivo.
- Si XClarity Orchestrator no puede conectarse con el gestor de recursos (por ejemplo, si las credenciales han caducado o si hay problemas de red), seleccione **Forzar anulación de gestión incluso si no se puede acceder al dispositivo**.
- De forma predeterminada, la gestión de los dispositivos gestionados mediante XClarity Administrator y que están fuera de línea durante 24 horas o más se anula automáticamente (consulte [Configuración de valores globales de detección](#)).
- En la mayoría de los dispositivos, se conserva determinada información acerca del dispositivo una vez que se ha anulado su gestión. Cuando no se gestionan dispositivos:
 - La cuenta de usuario de gestión y las suscripciones de sucesos y métricas se eliminan del dispositivo.
 - En el caso de dispositivos gestionados mediante XClarity Administrator, si la función Llamar a casa está habilitada en XClarity Administrator, se deshabilita en el dispositivo.

- Para los dispositivos gestionados mediante XClarity Administrator, si la encapsulación está habilitada en el dispositivo, las reglas de firewall del dispositivo se cambian a los valores que tenía el dispositivo antes de que se gestionara.
- La información sensible, el inventario y los sucesos y las alertas que ha generado el dispositivo se descartan en el concentrador de gestión.
- Los sucesos y alertas que el concentrador de gestión ha generado para el dispositivo se mantienen en el concentrador de gestión.

Anular la gestión de dispositivos

Puede utilizar Lenovo XClarity Orchestrator para quitar dispositivos de la gestión mediante su gestor de recursos correspondiente. Este proceso se denomina *anular la gestión* (no gestionar).

Antes de empezar

Para realizar esta tarea, debe ser miembro de un grupo de usuarios al que se le haya asignado el rol de **Supervisor** o Administrador de **seguridad** predefinido.

Asegúrese de que no haya trabajos activos en ejecución en el dispositivo.



Acerca de esta tarea

De forma predeterminada, XClarity Orchestrator anula automáticamente la gestión de los dispositivos que están fuera de línea durante 24 horas o más (consulte [Configuración de valores globales de detección](#)).

En la mayoría de los dispositivos, el XClarity Orchestrator y el gestor de recursos conservan determinada información acerca del dispositivo una vez que se ha anulado su gestión. Esta información se vuelve a aplicar cuando se gestiona de nuevo el mismo dispositivo.

Procedimiento

Para anular la gestión de dispositivos, siga estos pasos.

- Paso 1. Desde la barra de menú de XClarity Orchestrator, haga clic en **Recursos**  y luego haga clic en el tipo de dispositivo para mostrar una tarjeta con una vista de tabla de todos los dispositivos gestionados de ese tipo.
- Paso 2. Seleccione uno o más dispositivos para anular la gestión.
- Paso 3. Haga clic en el icono de **No gestionar**  para mostrar el cuadro de diálogo No gestionar.
- Paso 4. Seleccione **Forzar anulación de gestión incluso si no se puede acceder al dispositivo**.
- 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.

Uso de VMwareTools

El paquete de herramientas de VMware se instala en la máquina virtual y en el sistema operativo invitado cuando instala Lenovo XClarity Orchestrator 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](#).

Configurar valores de red

Puede configurar una interfaz de red única (mediante los valores IPv4 e IPv6) y los valores de enrutamiento de Internet y los valores de proxy.

Antes de empezar

Más información:  [Cómo configurar redes y configurar servidores NTP](#)

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


Revise las siguientes consideraciones al elegir la interfaz.

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

Atención:

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

Procedimiento

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

- **Configurar valores de IP** Puede elegir utilizar los valores de red IPv4 e IPv6 desde las tarjetas de Configuración de IPv4 y Configuración de IPv6. Habilite y modifique los valores de configuración de IP aplicables y luego haga clic en **Aplicar**.
 - **Valores de IPv4.** Puede configurar el método de asignación de IP, la dirección IPv4, la máscara de red y la puerta de enlace predeterminada. Para el método de asignación de IP, puede elegir usar una dirección IP asignada de forma estática, o bien obtener una dirección IP desde un servidor DHCP. Al utilizar una dirección IP estática, debe proporcionar una dirección IP, una máscara de red y una puerta de enlace predeterminada. La puerta de enlace predeterminada debe ser una dirección IP válida que debe estar en la misma subred que la interfaz de red.

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

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

The image shows two configuration panels. The top panel is titled 'Configuration de IPv4' and has an 'Enabled' toggle switch. It contains four input fields: 'Método' (set to 'Obtain IP from DHCP'), 'Máscara de red IPv4' (255.255.224.0), 'Dirección IPv4' (10.243.14.36), and 'Puerta de enlace predeterminad...' (10.243.0.1). Below these are 'Aplicar' and 'Restablecer' buttons. The bottom panel is titled 'Configuration de IPv6' and also has an 'Enabled' toggle switch. It contains four input fields: 'Método' (set to 'Use stateless address...'), 'Longitud del prefijo de IPv6' (64), 'Dirección IPv6' (fd55:faaf:e1ab:2021:20c:2'), and 'Puerta de enlace predeterm...' (fe80::5:73ff:fea0:2c). Below these are 'Aplicar' and 'Restablecer' buttons.

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

Actualmente, solo se admiten direcciones IPv4.

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

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

Notas:

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

Configuración de DNS

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

Tipo de dirección DNS de preferencia IPv4 IPv6

Enabled

Primera dirección DNS: 10.240.0.10

Método: Use domain name o...

Segunda dirección DNS: 10.240.0.11

Nombre de dominio:

Nombre de host: lxco

Aplicar Restablecer

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

Notas:

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

Configuración de proxy

Disabled

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

Puerto del servidor proxy Contraseña

Aplicar Restablecer

Configuración de fecha y hora

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

Antes de empezar

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

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

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

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

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

Procedimiento

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

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

Fecha y hora

La fecha y hora se sincronizarán automáticamente con el servidor NTP

Fecha 3/10/22

Tiempo 18:57:21

Zona horaria UTC -00:00, Coordinated Universal Time Universal

Después de que se apliquen los cambios, esta página se actualizará automáticamente para obtener la configuración más reciente.

Zona horaria*

UTC -00:00, Coordinated Universal Time Universal

Servidores NTP*

Servidores NTP 1 FQDN o dirección IP

⊕ Añadir nuevo servidor NTP

Aplicar

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

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

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

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

Trabajo con certificados de seguridad

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

Antes de empezar

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

Acerca de esta tarea

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

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

XClarity Orchestrator proporciona varios servicios que aceptan conexiones SSL/TLS entrantes. Cuando un cliente, como un navegador web, se conecta a uno de estos servicios, XClarity Orchestrator 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 Orchestrator no está incluido en la lista del cliente, el cliente se desconecta de XClarity Orchestrator para evitar intercambiar cualquier información confidencial de seguridad con una fuente que no sea de confianza.

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

Los servicios de XClarity Orchestrator 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 Orchestrator. 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

[Volver a generar el certificado de servidor firmado internamente de XClarity Orchestrator](#)). También durante la configuración inicial, se genera una clave separada y se crea un certificado de servidor y es firmado por la autoridad de certificación interna. Este certificado utilizado como el certificado de servidor de XClarity Orchestrator predeterminado. Se regenera automáticamente cada vez que XClarity Orchestrator 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 genera a demanda (consulte [Volver a generar el certificado de servidor firmado internamente de XClarity Orchestrator](#)).

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 Orchestrator (consulte [Instalación de un certificado de servidor de confianza firmado externamente del XClarity Orchestrator](#)

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

Los clientes de XClarity Orchestrator 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 Orchestrator actúa como un cliente. Ejemplos de recursos locales son Gestores de recursos, software local al reenviar sucesos, etc.
- **Certificados de servicios externos.** Este almacén de confianza gestiona certificados que se usan para establecer una conexión segura con dispositivos externos cuando XClarity Orchestrator actúa como un cliente. Ejemplos de servicios externos son los servicios de Lenovo Support 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. 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 Orchestrator 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.

Adición de un certificado de confianza para servicios externos

Estos certificados se utilizan para establecer relaciones de confianza con servicios externos. Por ejemplo, los certificados de este almacén se utilizan al recuperar la información de garantía de Lenovo, crear informes, reenviar sucesos a una aplicación externa (como Splunk) y usar servidores LDAP externos.

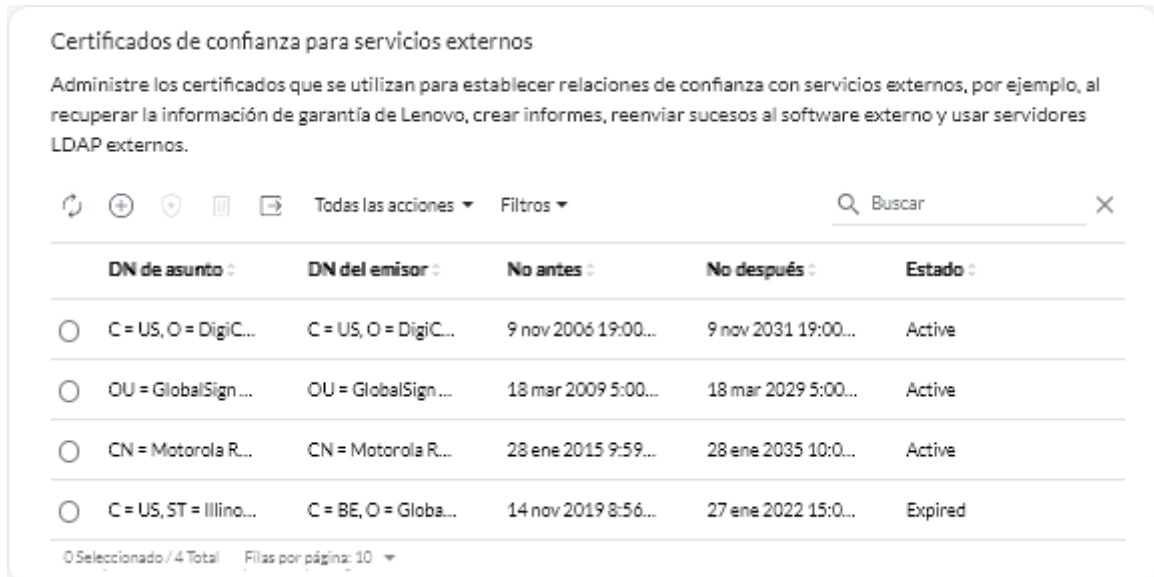
Antes de empezar

No se confía en los certificados en esta almacén de confianza al establecer conexiones con otros servicios a menos que también los agregue al almacén de confianza de Certificados de confianza principal. Quitar certificados de este almacén de confianza evita una operación satisfactoria de estos servicios.

Procedimiento

Para agregar un certificado de confianza, lleve a cabo los pasos siguientes.

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



Paso 2. Haga clic en el icono de **Agregar** (+) para agregar un certificado. Se muestra el cuadro de diálogo Agregar certificado.

Paso 3. Copie y pegue los datos de certificado en formato PEM.

Paso 4. Haga clic en **Añadir**.

Después de finalizar

Puede realizar las acciones siguientes desde la tarjeta de Certificados de confianza para la tarjeta de servicios externos.

- Ver los detalles de un certificado de confianza seleccionado haciendo clic en el icono de **Ver** (🔍).
- Guarde un certificado de confianza seleccionado en el sistema local haciendo clic en el icono **Ver** (🔍) y luego haciendo clic en **Guardar como pem**.
- Elimine un certificado de confianza seleccionado haciendo clic en el icono de **Eliminar** (🗑️).

Adición de un certificado de confianza para servicios internos

Estos certificados se utilizan para establecer relaciones de confianza con los recursos locales cuando Lenovo XClarity Orchestrator actúa como cliente de dichos recursos, como los administradores de recursos, el reenvío de sucesos al software local y el servidor LDAP incorporado. Además, el certificado de CA interno y el certificado de CA del certificado de servidor firmado externamente personalizado (si hay uno instalado) están presentes en esta almacén de confianza para admitir la comunicación interna de XClarity Orchestrator.


Procedimiento



Para agregar un certificado de confianza, lleve a cabo los pasos siguientes.



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

Certificados de confianza

Administre los certificados que se utilizan para establecer relaciones de confianza con los recursos locales cuando XClarity Orchestrator actúa como cliente de esos recursos, como los administradores de recursos (XClarity Administrator), el reenvío de sucesos al software local y el al servidor LDAP.





 Todas las acciones ▾ Filtros ▾

 Buscar 

	DN de asunto :	DN del emisor :	No antes :	No después :	Estado :
<input type="radio"/>	C = US, ST = Nort...	C = US, ST = Nort...	31 dic 1969 19:0...	31 dic 2069 18:5...	Active
<input type="radio"/>	C = US, ST = NC, L...	C = US, ST = NC, L...	3 oct 2022 10:14:...	3 oct 2023 10:14:...	Active

0 Seleccionado / 2 Total Filas por página: 10 ▾

Paso 2. Haga clic en el icono de **Agregar** (+) para agregar un certificado. Se muestra el cuadro de diálogo Agregar certificado.

Paso 3. Copie y pegue los datos de certificado en formato PEM.

Paso 4. Haga clic en **Añadir**.

Después de finalizar

Puede realizar las siguientes acciones desde la tarjeta de Certificado de confianza.

- Ver los detalles de un certificado de confianza seleccionado haciendo clic en el icono de **Ver** (🔍).
- Guarde un certificado de confianza seleccionado en el sistema local haciendo clic en el icono **Ver** (🔍) y luego haciendo clic en **Guardar como pem**.
- Elimine un certificado de confianza seleccionado haciendo clic en el icono de **Eliminar** (🗑️).

Instalación de un certificado de servidor de confianza firmado externamente del XClarity Orchestrator

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

Acerca de esta tarea

Como práctica recomendada, utilice siempre los certificados firmados v3.

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

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

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

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

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

Procedimiento

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

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

1. En la barra de menús de XClarity Orchestrator, haga clic en **Administración** (⚙️) → **Seguridad** y, a continuación, haga clic en **Certificado de servidor** en el panel de navegación izquierdo para mostrar la tarjeta de Generar solicitud de firma de certificado.

Generar solicitud de firma de certificado (CSR)

Cree y guarde una Solicitud de firma de certificado mediante los valores proporcionados.

País/región*	Organización*
UNITED STATES	Lenovo
Estado/provincia*	Unidad organizativa*
NC	DCG
Ciudad*	Nombre común*
Raleigh	Generated by Lenovo Management Ecosystem

Nombres alternativos del asunto ?

Para añadir un nuevo Nombre alternativo de asunto, haga clic en +

Generar archivo CSR Importar certificado

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

- Nombre común del propietario del certificado. Este debe ser el nombre de host del servidor que está utilizando el certificado. La longitud de este valor no puede sobrepasar de 63 caracteres.
- (Opcional) Nombres alternativos de asunto que se añaden a la extensión X.509 “subjectAltName” cuando se genera el CSR. De forma predeterminada, XClarity Orchestrator define automáticamente los nombres alternativos de asunto para CSR según la dirección IP y el nombre de host que se detectó mediante las interfaces de red del sistema operativo invitado de XClarity Orchestrator. Puede personalizar, eliminar o agregar a estos valores de nombre alternativos de asunto. Sin embargo, los nombres alternativos del asunto deben tener el nombre de dominio totalmente cualificado (FQDN) o la dirección IP del servidor, así como el nombre del asunto debe configurarse en el FQDN.

El nombre que especifique debe ser válido para el tipo seleccionado.

- **DNS** (utilice el FQDN, por ejemplo, hostname.labs.company.com)
- **Dirección IP** (por ejemplo, 192.0.2.0)
- **Correo electrónico** (por ejemplo, example@company.com)

Nota: Todos los nombres alternativos de asunto que se enumeran en la tabla se validan, guardan y añaden a CSR solo después de que genere CSR en el paso siguiente.

- Paso 2. Proporcione una entidad emisora de certificación de confianza (CA) para CSR. La CA firma el CSR y arroja un certificado de servidor.
- Paso 3. Importe el certificado de servidor firmado externamente y el certificado de la CA a XClarity Orchestrator y sustituya el certificado de servidor actual.
1. En la tarjeta generar solicitud de firma de certificado (CSR) , haga clic en **Importar certificado** para mostrar el cuadro de diálogo Importar certificado.
 2. Copie y pegue el certificado de servidor y el certificado de la CA en formato PEM. Debe proporcionar toda la cadena de certificados, comenzando con el certificado de servidor y terminando en el certificado de CA raíz.
 3. Haga clic en **Importar** para almacenar el certificado de servidor en el almacén de confianza de XClarity Orchestrator.
- Paso 4. Acepte el nuevo certificado pulsando Ctrl+F5 para actualizar el navegador y luego vuelva a establecer la conexión con la interfaz web. Esto debe ser realizado por todas las sesiones de usuario establecidas.

Volver a generar el certificado de servidor firmado internamente de XClarity Orchestrator

Puede generar un nuevo certificado de servidor para sustituir el certificado firmado internamente actual de Lenovo XClarity Orchestrator o para reinstalar un certificado generador por XClarity Orchestrator si XClarity Orchestrator utiliza actualmente un certificado de servidor firmado externamente personalizado. El nuevo certificado de servidor firmado internamente se usa XClarity Orchestrator para el acceso HTTPS.

Acerca de esta tarea

El certificado de servidor que está actualmente en uso ya sea interna o externamente firmado, permanece en uso hasta que se regenere y está firmado el nuevo certificado de servidor.

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

Procedimiento

Para generar un certificado de servidor firmado internamente por XClarity Orchestrator, lleve a cabo los siguientes pasos.

Paso 1. En la barra de menú de XClarity Orchestrator, haga clic en **Administración** (⚙️) → **Seguridad** y luego haga clic en **Certificado de servidor** en el panel de navegación izquierdo para mostrar la tarjeta de Volver a generar certificado de servidor.

Volver a generar certificado de servidor

Genere una clave y un certificado nuevos mediante los datos de certificado proporcionados.

Pais/región*	Organización*
UNITED STATES	Lenovo
Estado/provincia*	Unidad organizativa*
NC	DCG
Ciudad*	Nombre común*
Raleigh	Generated by Lenovo Management Ecosystem
No válido antes de la fecha	No válido después de la fecha*
3/Oct/2022 13:21	30/Sep/2032 13:21

[Volver a generar certificado](#) [Guardar certificado](#) [Restablecer certificado](#)

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

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

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

Paso 3. Haga clic en **Volver a generar certificado** para volver a generar el certificado firmado internamente y luego haga clic en **Volver a generar certificado** para confirmar.

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

Después de finalizar

Puede realizar las siguientes acciones desde la tarjeta de Volver a generar certificado de servidor.

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

Importación del certificado de servidor en un navegador web

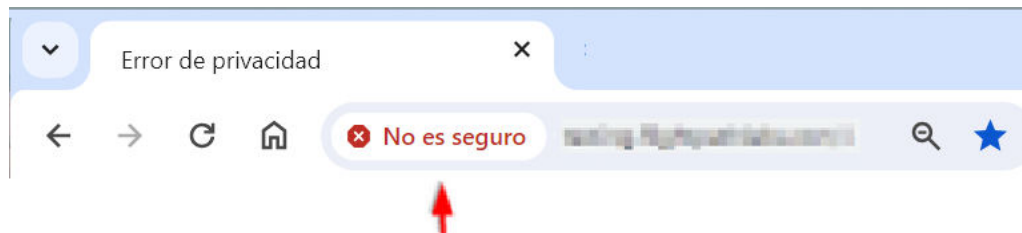
Puede guardar una copia del certificado de servidor, en formato PEM, a su sistema local. Luego puede importar el certificado a la lista de certificados de confianza del navegador web o a otras aplicaciones (como Lenovo XClarity Mobile o Lenovo XClarity Integrator) para evitar los mensajes de advertencia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

Procedimiento

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

• Chrome

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

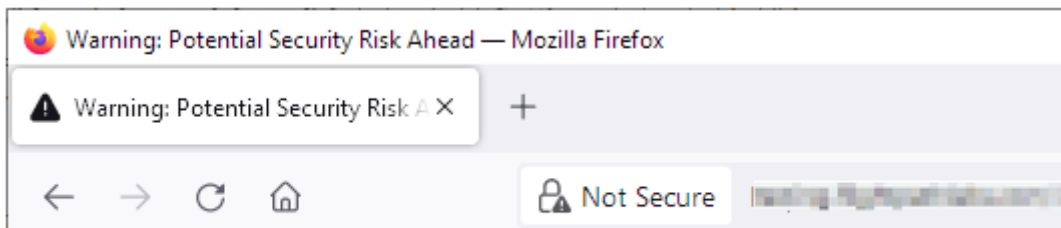


- b. Haga clic en **Certificado (no válido)** para mostrar el cuadro de diálogo Certificado.
 - c. Haga clic en la pestaña **Detalles**.
 - d. Haga clic en **Copiar en el archivo** para mostrar el Asistente para exportación de certificados.
 - e. Seleccione **Estándar de sintaxis de mensajes criptográficos** y, a continuación, haga clic en **Siguiente**.
 - f. Especifique el nombre y la ubicación del archivo del certificado y, a continuación, **Finalizar** para exportar el certificado.
 - g. Haga clic en **Aceptar** para cerrar el cuadro de diálogo de Certificado.
2. Importe el certificado de servidor XClarity Orchestrator en la lista de certificados de confianza de la autoridad raíz del navegador.
 - a. Desde el navegador Chrome, haga clic en los tres puntos de la esquina superior derecha de la ventana y, a continuación, haga clic en **Valores**.
 - b. Desplácese a la sección **Privacidad y seguridad** y, a continuación, haga clic en **Gestionar certificados** para mostrar el cuadro de diálogo Certificados.
 - c. Haga clic en **Importar**, seleccione el archivo de certificado que exportó anteriormente y, a continuación, haga clic en **Siguiente**.

- d. Haga clic en **Examinar** junto a **Almacén de certificados** y, a continuación, seleccione **Entidades de certificación raíz de confianza**. A continuación, haga clic en **Aceptar**.
- e. Haga clic en **Finalizar**.
- f. Cierre y vuelva a abrir el navegador Chrome y, a continuación, abra XClarity Orchestrator.

- **Firefox**

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



- b. Expanda Conexión no protegida y, a continuación, haga clic en Más información para mostrar un cuadro de diálogo.
 - c. Haga clic en **Ver certificados**.
 - d. Desplácese hacia abajo a la sección Descargar y haga clic en el enlace **PEM (cert)**.
 - e. Seleccione **Guardar archivo** y, a continuación, haga clic en **Aceptar**.
2. Importe el certificado de servidor XClarity Orchestrator en la lista de certificados de confianza de la autoridad raíz del navegador.
 - a. Abra el navegador y haga clic en **Herramientas → Opciones → Avanzado**.
 - b. Haga clic en la pestaña **Certificados**.
 - c. Haga clic en **Ver certificados**.
 - d. Haga clic en **Importar** y vaya a la ubicación donde se descargó el certificado.
 - e. Seleccione el certificado y haga clic en **Abrir**.

Gestión de la autenticación

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

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

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

Configuración de un servidor de autenticación LDAP externo

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

Antes de empezar

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

Solo Microsoft Active Directory se admite como servidor LDAP externo.

XClarity Orchestrator no clona automáticamente los grupos de usuarios que se definen en el servidor LDAP externo. Sin embargo, puede clonar el grupo de usuarios LDAP de forma manual (consulte [Creación de grupos de usuario](#)).

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

Acerca de esta tarea

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

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

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

Procedimiento

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

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

ไคลเอ็นต์ LDAP

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

ข้อมูลเซิร์ฟเวอร์

โดเมน* ที่อยู่เซิร์ฟเวอร์* พอร์ต*

Active Directory LDAP แบบกำหนดค่า LDAP ผ่าน SSL

การกำหนดค่า

ชื่อที่ประทับพื้นที่สำหรับผู้ใช้*

ชื่อที่ประทับพื้นที่สำหรับกลุ่ม*

การผูกข้อมูลประจำตัว ⓘ

วิธีการแยก

การแยกชื่อผู้ใช้*

การเข้ารหัสลับ*

ตั้งข้อมูลใบรับรองหรือวางใบรับรองที่อยู่ในรูปแบบ PEM (ตรวจสอบว่าการมีเครื่องหมาย BEGIN และ END): ⓘ

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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


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

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

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

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

Después de finalizar

Puede quitar una configuración del servidor LDAP pulsando el icono **Eliminar** () que se encuentra situado junto a la configuración. Cuando se elimina una configuración de servidor LDAP, si no hay otras configuraciones de servidor LDAP en el mismo dominio, también se quitan los clones de usuarios y los grupos de clones de usuario de dicho dominio.

Gestión de usuarios y sesiones de usuarios

Las *cuentas de usuario* se utilizan para iniciar sesión y gestionar Lenovo XClarity Orchestrator.

Creación de usuarios

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

Acerca de esta tarea

Los usuarios de un servidor LDAP externo se clonan automáticamente en el servidor de autenticación local con el nombre *{username}@{domain}* la primera vez que inician sesión. Esta cuenta de usuario clonada solo se puede usar para autorizar el acceso a los recursos. La autenticación sigue produciéndose a través del servidor de autenticación LDAP para estos usuarios, mientras que los cambios a la cuenta de usuario (aparte de la descripción y los roles) se deben realizar a través de LDAP.

XClarity Orchestrator controla el acceso a las funciones (acciones) utilizando roles. Puede asignar un rol distinto a usuarios locales y clonados agregando estos usuarios a uno o varios grupos de usuarios asociados con los roles deseados. De forma predeterminada, todos los usuarios son miembros del grupo de usuarios **OperatorGroup** (consulte [Creación de grupos de usuario](#)).

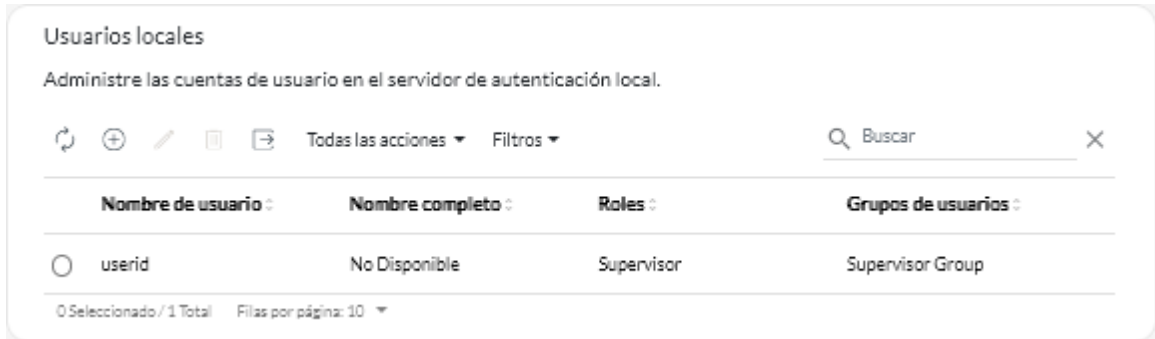
Al menos un usuario debe ser miembro de un grupo de usuarios *local* al que esté asignado el rol de **Supervisor** predefinido (consulte [Control de acceso a funciones](#)).

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

Procedimiento

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

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



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

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

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

Nota: Los nombres de usuario no distinguen entre mayúsculas y minúsculas.

- Introduzca la nueva contraseña y confírmela. De manera predeterminada, las contraseñas deben contener los caracteres **8 - 256** y deben cumplir los siguientes criterios.

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

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

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

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

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

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

La cuenta de usuario se agrega a la tabla.

Después de finalizar

Puede realizar las acciones siguientes desde la tarjeta Usuarios locales.

- Ver las propiedades de usuario haciendo clic en la fila de la tabla de un usuario para mostrar el cuadro de diálogo Detalles de usuario.
- Modifique las propiedades de un usuario seleccionado, incluida la contraseña y los grupos de usuario, haciendo clic en el icono de **Editar** (✎).
- Elimine un usuario seleccionado haciendo clic en el icono de **Eliminar** (🗑). No puede eliminar el grupo de usuarios de LDAP existente de los usuarios de LDAP.
- Exporte los detalles del usuario, como el nombre de usuario, el nombre o los apellidos, haciendo clic en el icono de **Exportar** (📤).

Creación de grupos de usuario

Los grupos de usuarios se utilizan para autorizar el acceso a los recursos.

Antes de empezar

Más información:  [Cómo crear un grupo de usuarios](#)

Puede crear manualmente grupos de usuarios en el repositorio local. Los grupos de usuarios locales contienen usuarios locales y clonados.

También puede clonar cualquier grupo de usuarios que se defina en un servidor LDAP externo. El grupo de usuarios LDAP clonado se denomina *{domain}\{groupName}* en el repositorio local. Este grupo de usuarios clonado solo se puede utilizar para autorizar el acceso a los recursos. Los cambios en el nombre del grupo, la descripción y la membresía se deben realizar a través de LDAP.

Antes de que un usuario LDAP externo pueda iniciar sesión en XClarity Orchestrator, el usuario debe ser miembro directo de un grupo de usuarios LDAP que se haya clonado en XClarity Orchestrator.

Si el servidor LDAP se configura para utilizar credenciales de inicio de sesión y usted inicia sesión en XClarity Orchestrator con una ID de usuario local de XClarity Orchestrator, se le solicita que proporcione las credenciales de usuario de LDAP cuando clone un grupo de usuarios LDAP. En todos los demás casos, no son necesarias sus credenciales.

Acerca de esta tarea

XClarity Orchestrator proporciona los siguientes grupos de usuarios predefinidos, uno para cada rol predefinido. Para obtener más información sobre los roles, consulte [Control de acceso a funciones](#).

- **Grupo de supervisores.** A los usuarios de este grupo de usuarios se les asigna el rol de **Supervisor**.
- **Grupo de gestores de hardware.** A los usuarios de este grupo de usuarios se les asigna el rol de **Gestor de hardware**.
- **Grupo de gestores de seguridad.** A los usuarios de este grupo de usuarios se les asigna el rol de **Gestor de seguridad**.
- **Grupo de informadores.** A los usuarios de este grupo de usuarios se les asigna el rol de **Informador**.
- **Grupo de gestores de actualizaciones.** A los usuarios de este grupo de usuarios se les asigna el rol de **Gestor de actualizaciones**.
- **Grupo de operadores.** A los usuarios de este grupo de usuarios se les asigna el rol de **Operador**.

- **Grupo de legado del operador.** A los usuarios de este grupo de usuarios se les asigna el rol de **OperatorLegacy**. Tenga en cuenta que este grupo de usuarios se desechará en una versión futura.

Al menos un usuario debe ser miembro de un grupo de usuarios *local* al que esté asignado el rol de **Supervisor** predefinido (consulte [Control de acceso a funciones](#)).

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

Procedimiento

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

- **Crear un grupo de usuarios local**

1. En la barra de menús de XClarity Orchestrator, haga clic en **Administración** (⚙️) → **Seguridad** y, a continuación, haga clic en **Grupos de usuarios** en el panel de navegación izquierdo para mostrar la tarjeta de Grupos de usuarios.

Nombre	Descripción	Roles
<input type="radio"/> Configuration Patterns Administra...	Allows users to configure servers u...	Configuration Patterns Administrato
<input type="radio"/> Hardware Administrator Group	Allows users to view data, manage ...	Hardware Administrator
<input type="radio"/> OS Administrator Group	Allows users to deploy operating s...	OS Administrator
<input type="radio"/> Operator Group	Allows user to only view the orches...	Operator
<input type="radio"/> Operator Legacy Group	Allows user to view the orchestrat...	Operator Legacy
<input type="radio"/> Reporter Group	Allows users to view the orchestrat...	Reporter
<input type="radio"/> Security Administrator Group	Allows user to modify security setti...	Security Administrator
<input type="radio"/> Supervisor Group	Allows user to view data about and...	Supervisor
<input type="radio"/> Updates Administrator Group	Allows user to manage the updates...	Updates Administrator

0 Seleccionado / 9 Total Filas por página: 10

2. Haga clic en el icono de **Crear** (+) para mostrar el cuadro de diálogo Crear grupo.
3. Seleccione **Grupo de usuarios locales** como tipo de grupo.
4. Especifique el nombre y una descripción opcional para este grupo de usuarios.
5. Haga clic en la pestaña **Usuarios disponibles** y seleccione los usuarios que desee incluir en este grupo de usuarios.
6. Haga clic en la pestaña **Roles** y seleccione los roles que desee asignar en este grupo de usuarios. Si un rol no está seleccionado, el rol **Operador** se asigna de forma predeterminada.

7. Haga clic en **Crear**.

- **Clone un grupo de usuarios desde un servidor LDAP externo**

1. En la barra de menú de XClarity Orchestrator, haga clic en **Administración** (⚙️) → **Seguridad** y luego haga clic en **Grupos de usuario** en el panel de navegación izquierdo para mostrar la tarjeta de Grupos de usuario.
2. Haga clic en el icono de **Crear** (+) para mostrar el cuadro de diálogo Crear grupo.
3. Seleccione **Grupo de usuarios LDAP** como tipo de grupo.
4. Opcionalmente, especifique una descripción para el grupo.
5. Seleccione la configuración de LDAP para el servidor LDAP externo que contiene el grupo de usuarios que desea añadir.

Consejo: comience a escribir para buscar todos los nombres de grupo que contengan una palabra clave especificada

6. Si el servidor LDAP externo se configura con credenciales de inicio de sesión, especifique el nombre de usuario y la contraseña para iniciar sesión en el servidor LDAP externo.
7. Especifique una cadena de búsqueda (con al menos tres caracteres) en el campo **Grupo de búsqueda** y, a continuación, haga clic en **Buscar** para buscar grupos de usuarios en el servidor LDAP externo que coincidan con la cadena de búsqueda. Luego, seleccione el grupo que desea agregar.
8. Haga clic en la pestaña **Roles** y seleccione los roles que desee asignar en este grupo de usuarios. Si un rol no está seleccionado, el rol **Operador** se asigna de forma predeterminada.
9. Haga clic en **Crear**.

Después de finalizar

Puede llevar a cabo las siguientes acciones desde la tarjeta Grupos de usuario.

- Modifique las propiedades, la membresía local y los roles de un grupo de usuarios seleccionado haciendo clic en el icono **Editar** (✎).
- Cuando agrega o quita un usuario de un grupo, el usuario se registra automáticamente si los roles (permisos) cambian después de la asignación de grupos nuevos. Cuando el usuario inicia sesión de nuevo, el usuario puede realizar acciones basadas en los roles agregados de los grupos de usuarios asignados.
- Cada usuario debe ser miembro al menos de un grupo de usuarios. Si establece este atributo en una matriz vacía o en cero, **OperatorGroup** se asigna de forma predeterminada.
- Para los grupos de usuarios predefinidos, solo puede modificar la membresía del grupo.
- Para el grupo de usuarios LDAP, puede modificar solo la descripción y los roles. Utilice el servidor LDAP externo para cambiar otras propiedades y membresía.
- Elimine un grupo de usuario seleccionado haciendo clic en el icono de **Eliminar** (🗑️).

Nota: No puede eliminar los grupos de usuarios predefinidos.

- Consulte los miembros de un grupo de usuario haciendo clic en el nombre del grupo para mostrar el cuadro de diálogo Ver grupo y luego haga clic en la pestaña **Resumen de miembros**.

Cambio de detalles de su cuenta de usuario


Puede cambiar la contraseña, el nombre completo, la dirección de correo electrónico y el número de teléfono de la cuenta de usuario.

Acerca de esta tarea

Las contraseñas de usuario caducan, de forma predeterminada, después de **0** días.

Procedimiento

Para cambiar la contraseña y otros atributos, lleve a cabo los pasos siguientes.

- Paso 1. Desde la barra de título de XClarity Orchestrator, haga clic en el menú de **Cuenta del usuario**  en la esquina superior derecha y haga clic en **Cambiar contraseña**. Se muestra el cuadro de diálogo Cambiar contraseña.
- Paso 2. Especifique la contraseña actual.
- Paso 3. Introduzca la nueva contraseña y confírmela. De manera predeterminada, las contraseñas deben contener los caracteres **8 - 256** y deben cumplir los siguientes criterios.
 - Debe contener al menos un carácter alfabético y no debe tener más de dos caracteres secuenciales, incluidas las secuencias de caracteres alfabéticos, dígitos y las teclas del teclado QWERTY (por ejemplo “abc”, “123” y “asd” no están permitidos)
 - Debe contener por lo menos un número
 - Deben contener al menos dos de los siguientes caracteres.
 - Caracteres alfabéticos en mayúscula (A - Z)
 - Caracteres alfabéticos en minúscula (a - z)
 - Caracteres especiales ; @ _ ! ' \$ & +Los espacios en blanco no están permitidos.
 - No se debe repetir ni invertir el nombre de usuario.
 - No debe contener más de dos caracteres iguales consecutivamente (por ejemplo, “aaa”, “111” y “...” no están permitidos).
- Paso 4. Cambie su nombre completo, la dirección de correo electrónico y el número de teléfono, si corresponde.
- Paso 5. Haga clic en **Cambiar**.

Cambio de los detalles de otro usuario

Los usuarios supervisores puede cambiar los detalles, incluida la contraseña, de otro usuario.


Acerca de esta tarea

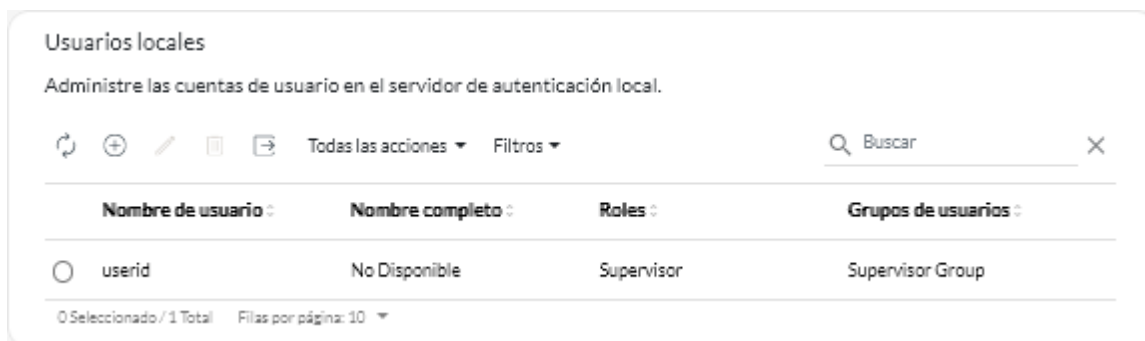
Las contraseñas de usuario caducan, de forma predeterminada, después de **0** días.

Puede configurar el periodo de caducidad de la contraseña y las reglas de complejidad de las contraseñas (consulte [Configuración de los valores de seguridad del usuario](#)).

Procedimiento

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

- Paso 1. En la barra de menú de XClarity Orchestrator, haga clic en **Administración**  → **Seguridad** y luego haga clic en **Usuarios locales** en el panel de navegación izquierdo para mostrar la tarjeta de Usuarios locales.



Paso 2. Seleccione la cuenta de usuario.

Paso 3. Haga clic en el icono **Editar** (✎) para modificar las propiedades del usuario. Se muestra el cuadro de diálogo Editar usuario.

Paso 4. Introduzca la nueva contraseña y confírmela. De manera predeterminada, las contraseñas deben contener los caracteres **8 - 256** y deben cumplir los siguientes criterios.

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

Paso 5. Haga clic en **Editar**.

Configuración de los valores de seguridad del usuario

Los valores de seguridad de la cuenta de usuario configuran la contraseña, el inicio de sesión y los valores de sesión de usuario para usuarios locales.-

Más información:  [Cómo configurar los valores de seguridad del usuario](#)

Procedimiento

Para configurar los valores de seguridad para los usuarios locales, lleve a cabo los pasos siguientes.

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

Paso 2. Configure los siguientes valores de seguridad.

Valor de seguridad	Descripción	Valores permitidos	Valores predeterminados
Periodo de caducidad de la contraseña	<p>Cantidad de tiempo, en días que un usuario puede utilizar una contraseña antes de que tenga que cambiarla</p> <p>Los valores menores reducen la cantidad de tiempo que los piratas informáticos tienen para adivinar las contraseñas.</p> <p>Si se establece en 0, las contraseñas no caducan nunca.</p>	0 – 365	0
Periodo de advertencia de caducidad de la contraseña	<p>Cantidad de tiempo, en días, antes de la fecha de caducidad de la contraseña en que los usuarios empiezan a recibir advertencias sobre una inminente caducidad de la contraseña de usuario.</p> <p>Si se establece en 0, los usuarios no reciben advertencias.</p>	0 – 30	0
Ciclo mínimo de reutilización de la contraseña	<p>Número mínimo de veces que un usuario debe especificar una contraseña única cuando se cambia la contraseña antes de poder empezar a reutilizar contraseñas</p> <p>Si se establece en 0, los usuarios pueden reutilizar las contraseñas inmediatamente.</p>	0 – 10	5
Intervalo mínimo de cambio de contraseña	<p>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.</p> <p>El valor especificado no puede superar el valor especificado en el valor Periodo de caducidad de la contraseña.</p> <p>Si se establece en 0, los usuarios pueden cambiar las contraseñas inmediatamente.</p>	0 – 240	1
Número máximo de errores de inicio de sesión	<p>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</p> <p>Nota: Intentos de inicio de sesión consecutivos con el mismo nombre de usuario y contraseña que un solo inicio de sesión fallido.</p> <p>Si se establece en 0, las cuentas no se bloquean nunca.</p>	0 – 10	5

Valor de seguridad	Descripción	Valores permitidos	Valores predeterminados
Error al restablecer el contador de inicio de sesión	<p>Cantidad de tiempo transcurrido desde el último intento de inicio de sesión con error antes de que el contador de Número máximo de errores de inicio de sesión se restablezca en 0.</p> <p>Si se establece en 0, el contador no se restablece nunca. Por ejemplo, si el número máximo de errores de inicio de sesión es 2 y comete un error de inicio de sesión y luego vuelve a cometer un error de inicio de sesión 24 horas después, el sistema registrará que se ha equivocado dos veces y su cuenta se bloqueará.</p> <p>Nota: Esta configuración solo se aplica cuando el valor Número máximo de errores de inicio de sesión se establece en 1 o más.</p>	0 – 60	15
Periodo de bloqueo tras superar el número máximo de errores de inicio de sesión	<p>Cantidad mínima de tiempo, en minutos, después del cual un usuario bloqueado pueda intentar iniciar sesión de nuevo. Una cuenta de usuario que está bloqueado no se pueden utilizar para acceder a XClarity Orchestrator aunque se proporcione una contraseña válida.</p> <p>Si se establece en 0, las cuentas de usuario no se bloquean nunca.</p> <p>Nota: Esta configuración solo se aplica cuando el valor Número máximo de errores de inicio de sesión se establece en 1 o más.</p>	0 – 2880	60

Valor de seguridad	Descripción	Valores permitidos	Valores predeterminados
Tiempo de espera por inactividad de sesión web	<p>Cantidad de tiempo, en minutos, que una sesión de usuario establecida con el servidor de organización puede permanecer inactiva antes de que la sesión del usuario caduque y el usuario salga de la sesión automáticamente. Este tiempo de espera se aplica a todas las acciones (como abrir una página, actualizar la página actual o modificar datos). Este es el tiempo de espera principal para la sesión de usuario.</p> <p>Cuando una sesión está activa, este temporizador se restablece cada vez que el usuario realiza cualquier acción. Una vez que se supera el valor del tiempo de espera, se muestra la página de inicio de sesión la próxima vez que el usuario intenta realizar una acción.</p> <p>Si se establece en 0, este tiempo de espera se deshabilita.</p> <p>Nota: Cambiar esta configuración afecta inmediatamente a todas las sesiones de usuario, independientemente del tipo de autenticación. Las sesiones existentes que han estado inactivas por un tiempo mayor al nuevo valor del tiempo de espera han caducado.</p>	0, 60 – 1440	1440
Tiempo de espera por inactividad web para operaciones completas	<p>Cantidad de tiempo, en minutos, que una sesión de usuario establecida con el servidor organizador puede estar inactiva antes de que las acciones que modifican los datos (como la creación, la actualización o la eliminación de un recurso) estén deshabilitadas. Este es un tiempo de espera secundario opcional y es más corto que el valor de Tiempo de espera por inactividad de sesión web principal.</p> <p>Cuando una sesión está activa, este temporizador se restablece cada vez que el usuario realiza cualquier acción. Si se supera este valor de tiempo de espera pero <i>no</i> se supera el valor de Tiempo de espera por inactividad de sesión web principal, el usuario está restringido a acciones de solo lectura (como abrir o actualizar una página) hasta que se supere el valor de Tiempo de espera por inactividad de sesión web principal; sin embargo, si el usuario intenta realizar una acción que modifica los datos, la sesión del usuario caduca y se muestra la página de inicio de sesión.</p>	0, 15 – 60	30

Valor de seguridad	Descripción	Valores permitidos	Valores predeterminados
	<p>Si se establece en 0, este tiempo de espera se deshabilita.</p> <p>Nota: Cambiar esta configuración afecta inmediatamente a todas las sesiones de usuario, independientemente del tipo de autenticación. Las sesiones existentes que han estado inactivas por un tiempo mayor al nuevo valor del tiempo de espera han caducado.</p>		
Duración máxima con que una sesión basada en web pueda estar abierta	<p>Cantidad de tiempo, en horas, que una sesión de usuario establecida con el servidor de Orchestrator puede permanecer abierta antes de que el usuario salga de la sesión automáticamente, sin importar la actividad del usuario</p> <p>Nota: Cambiar esta configuración afecta inmediatamente a todas las sesiones de usuario, independientemente del tipo de autenticación. Las sesiones existentes que han estado inactivas por un tiempo mayor al nuevo valor del tiempo de espera han caducado.</p>	24 – 240	24
Longitud mínima de la contraseña	Número mínimo de caracteres que se pueden utilizar para especificar una contraseña válida	8 – 256	256
Longitud máxima de la contraseña	Número máximo de caracteres que se pueden utilizar para especificar una contraseña válida	8 – 128	128
Máximo de sesiones activas simultáneas para un usuario específico	<p>Número máximo de sesiones activas simultáneas para un usuario específico que se permiten a la vez. Cuando se alcanza el número máximo, se quita la sesión activa más antigua de un usuario (según la marca de tiempo de creación) antes de crear una nueva sesión para dicho usuario.</p> <p>Si se define en 0, se permite un número ilimitado de sesiones activas para un usuario específico.</p> <p>Nota: Solo se ven afectadas las sesiones de usuario que se inician después de cambiar el valor.</p>	0 – 20	20

Valor de seguridad	Descripción	Valores permitidos	Valores predeterminados
Número reglas de complejidad que se deben seguir al crear una contraseña nueva	<p>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.</p> <p>XClarity Orchestrator admite las siguientes reglas de complejidad de contraseña.</p> <ul style="list-style-type: none"> • Debe contener al menos un carácter alfabético y no debe tener más de dos caracteres secuenciales, incluidas las secuencias de caracteres alfabéticos, dígitos y las teclas del teclado QWERTY (por ejemplo “abc”, “123” y “asd” no están permitidos) • Debe contener por lo menos un número • Deben contener al menos dos de los siguientes caracteres. <ul style="list-style-type: none"> – Caracteres alfabéticos en mayúscula (A - Z) – Caracteres alfabéticos en minúscula (a - z) – Caracteres especiales ; @ _ ! ' \$ & + • Los espacios en blanco no están permitidos. • No se debe repetir ni invertir el nombre de usuario. • No debe contener más de dos caracteres iguales consecutivamente (por ejemplo, “aaa”, “111” y “...” no están permitidos). <p>Si se establece en 0, las contraseñas no se requieren para cumplir con ninguna regla de complejidad.</p>	0 – 5	4
Obligar al usuario a cambiar la contraseña en el primer acceso	Indica si se requiere que el usuario cambie la contraseña cuando inicie sesión en XClarity Orchestrator por primera vez.	Sí o No	Sí

Paso 3. Haga clic en **Aplicar**.

Una vez que se aplican los cambios, los nuevos valores surten efecto de inmediato. Si cambia las políticas de la contraseña, dichas políticas se aplicarán la próxima vez que el usuario inicie sesión o cambie la contraseña.

Después de finalizar

Puede realizar la siguiente acción desde la tarjeta Valores de seguridad de la cuenta.

- Para restablecer estos valores a los valores predeterminados, haga clic en **Restaurar valores predeterminados**.

Supervisión de sesiones de usuario activas

Puede determinar los usuarios que han iniciado sesión en la interfaz web de XClarity Orchestrator.

Antes de empezar

De forma predeterminada, las sesiones de usuario que no tienen actividad por más de 24 horas se cierran automáticamente. Puede configurar el tiempo de espera por inactividad de sesión web (consulte [Configuración de los valores de seguridad del usuario](#)).

Procedimiento

Para ver una lista de todas las sesiones de usuario activas (incluida la sesión actual), haga clic en **Administración** (⚙️) → **Seguridad** en la barra de menú de XClarity Orchestrator y luego haga clic en **Sesiones activas** en el menú de navegación izquierdo para mostrar la tarjeta de Sesiones activas.

Nombre de usuario	Dirección IP	Último acceso
userid	No Disponible	4/10/22 2:36
userid	No Disponible	4/10/22 13:04

Después de finalizar

Puede realizar la siguiente acción desde la tarjeta de Sesiones activas.

- Desconecte una sesión de usuario seleccionada haciendo clic en el icono de **Eliminar** (🗑️).

Nota: No puede desconectar la sesión actual.

Control de acceso a funciones

Lenovo XClarity Orchestrator utiliza *roles* y *grupos de usuarios* para determinar qué funciones (acciones) tiene permitido realizar un usuario.

Acerca de esta tarea

Un *rol* es un conjunto de funciones. Cuando un rol se asigna a un grupo de usuarios, todos los usuarios de dicho grupo pueden realizar las funciones que se incluyen en dicho rol.

XClarity Orchestrator proporciona los siguientes roles.

- **Supervisor.** Permite a los usuarios ver datos y realizar todas las acciones disponibles en el servidor de organización y todos los recursos gestionados (gestores de recursos y dispositivos). Los usuarios

asignados a este rol siempre tienen acceso a todos los recursos (dispositivos y gestores de recursos) y a todas las funciones. No se puede restringir el acceso a los recursos o funciones para este rol.

Debe tener privilegios de supervisor para llevar a cabo las siguientes acciones.

- Reiniciar el servidor de Orchestrator
- Realizar tareas de mantenimiento, como la instalación de licencias y la actualización a una versión más reciente
- Conectar y desconectar gestores de recursos
- Modificar valores del sistema, como las preferencias de red y la fecha y la hora
- Aceptar enviar datos periódicos a Lenovo

Debe haber al menos un usuario con privilegios de supervisor.

Importante: Cuando se actualiza desde XClarity Orchestrator v1.0 a una versión posterior, todos los usuarios que se crearon en XClarity Orchestrator v1.0 reciben privilegios de supervisor de manera predeterminada. Un usuario supervisor puede quitar los privilegios de supervisor a los usuarios que no deben tener esos privilegios.

- **Gestor de hardware.** Permite a los usuarios ver datos, gestionar y desplegar patrones de configuración, gestionar y desplegar sistemas operativos mediante perfiles de SO, visualizar y personalizar análisis y realizar acciones sobre recursos accesibles. Este rol prohíbe a los usuarios actualizar el software o el firmware en los recursos gestionados y gestionar los grupos de recursos.
- **Administrador de configuración del servidor.** Permite a los usuarios configurar servidores usando patrones de configuración, ver análisis predefinidos y ver datos de los recursos accesibles. Este rol prohíbe a los usuarios acceder de forma remota a los dispositivos y encenderlos o apagarlos.
- **Administrador del SO.** Permite a los usuarios desplegar sistemas operativos utilizando perfiles de SO, ver análisis predefinidos y ver datos de los recursos accesibles. Este rol prohíbe a los usuarios acceder de forma remota a los dispositivos y encenderlos o apagarlos.
- **Administrador de actualizaciones.** Permite a los usuarios actualizar el firmware en dispositivos y software en gestores de recursos, ver datos de los recursos accesibles y ver análisis predefinidos.
- **Administrador de seguridad.** Permite a los usuarios modificar los valores de seguridad y realizar acciones relacionadas con la seguridad en el servidor de organización, ver los datos de todos los recursos gestionados, gestionar el grupo de recursos y ver análisis predefinidos. Los usuarios asignados a este rol siempre tienen acceso a todos los recursos (dispositivos y gestores de recursos). No se puede restringir el acceso a los recursos para este rol.
- **Informador.** Permite a los usuarios ver la configuración del servidor de organización, ver los datos sobre los recursos accesibles, crear consultas para generar informes personalizados y crear despachadores de datos para programar y enviar informes por correo electrónico. Este rol prohíbe a los usuarios el aprovisionamiento de recursos y el encendido y apagado de dispositivos.
- **Operador.** Permite a los usuarios ver la configuración del servidor de organización y ver los datos de los recursos accesibles. Este rol prohíbe a los usuarios realizar acciones o modificar los valores de configuración en el servidor de organización y en los recursos gestionados, crear y ver informes de archivos y crear alertas personalizadas.
- **Heredado del operador.** Permite a los usuarios ver datos y realizar ciertas acciones en los recursos accesibles, como administrar el inventario, las alertas y los informes de servicio. Este rol prohíbe a los usuarios actualizar software o firmware en recursos gestionados, crear grupos de recursos, crear y ver informes de Informadores y crear alertas personalizadas.

Atención: Cuando se actualiza desde XClarity Orchestrator versión 1.2 a una versión posterior, los usuarios que tienen asignado el rol de **Operador** cambian automáticamente al rol **Heredado del operador** y se añaden al grupo de usuarios **OperatorLegacyGroup**. El rol **Heredado del operador** y el grupo de usuarios **OperatorLegacyGroup** se desecharán en una futura versión.

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

Nota: La visualización de datos relacionados con recursos no está restringida según los roles. Todos los usuarios pueden ver datos relacionados con recursos (como inventario, alertas, trabajos e informes de servicio) relativos a los recursos a los que puede acceder.

Procedimiento

Para ver información acerca de los roles predefinidos, haga clic en **Administración** (🔧) → **Seguridad** desde la barra de menú de XClarity Orchestrator y luego haga clic en **Roles** en el panel de navegación izquierdo.

Haga clic en la fila de cualquier rol para mostrar el cuadro de diálogo Roles con información acerca de las propiedades del rol, una lista de funciones del rol y una lista de grupos de usuarios a los que se ha asignado el rol.

Asignación de roles a usuarios

Lenovo XClarity Orchestrator utiliza *roles* y *grupos de usuarios* para determinar qué funciones (acciones) tiene permitido realizar un usuario.

Antes de empezar

Cuando se cambian los roles para un usuario que tiene actualmente una sesión iniciada en una sesión activa, la sesión del usuario se finaliza automáticamente y el usuario finaliza la sesión de la interfaz de usuario. Cuando el usuario vuelve a iniciar sesión, puede realizar las funciones según las nuevas asignaciones de roles.

Acerca de esta tarea

Cuando se asignan varios roles a un grupo de usuarios, se agregan las funciones de cada rol.

Todos los usuarios que son miembros de un grupo de usuarios tienen permiso para realizar las funciones que se incluyen en los roles asignados a ese grupo de usuarios.

Puede modificar los roles de un usuario mediante:

- Adición o eliminación del usuario de un grupo de usuarios
- Adición o eliminación de roles de un grupo de usuarios del que el usuario es miembro
- Eliminación de un grupo de usuarios del que es miembro el usuario

Notas:

- Cuando se agregan o quitan usuarios de LDAP de los grupos de usuarios de LDAP en el servidor LDAP, los cambios en las asociaciones entre el usuario LDAP y el grupo de usuarios LDAP se actualizan automáticamente de acuerdo con los grupos de usuarios LDAP clonados XClarity Orchestrator existentes.
- Cuando cambien los roles asignados a un grupo de usuarios, el usuario debe iniciar sesión de nuevo para que los cambios de roles se realicen.

Control de acceso a recursos

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

Acerca de esta tarea

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

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

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

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

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

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

Procedimiento

Para controlar el acceso a los recursos, lleve a cabo los siguientes pasos.

Paso 1. Cree un grupo de usuarios que puedan acceder a los recursos.

Paso 2. Cree uno o varios grupos de recursos de los que desee controlar el acceso.

Paso 3. Cree una lista de control de acceso que contenga el grupo de usuarios y uno o más grupos de recursos.

Paso 4. Habilite el control de acceso basado en recursos.

Habilitación de acceso basado en recursos

Si desea limitar los recursos a los que pueden acceder los usuarios, habilite el acceso basado en recursos.

Acerca de esta tarea

Los usuarios que son miembros de un grupo al que se asigna el rol de **Supervisor** predefinido siempre tienen acceso a todos los recursos. No puede limitar el acceso a recursos para los usuarios supervisor.

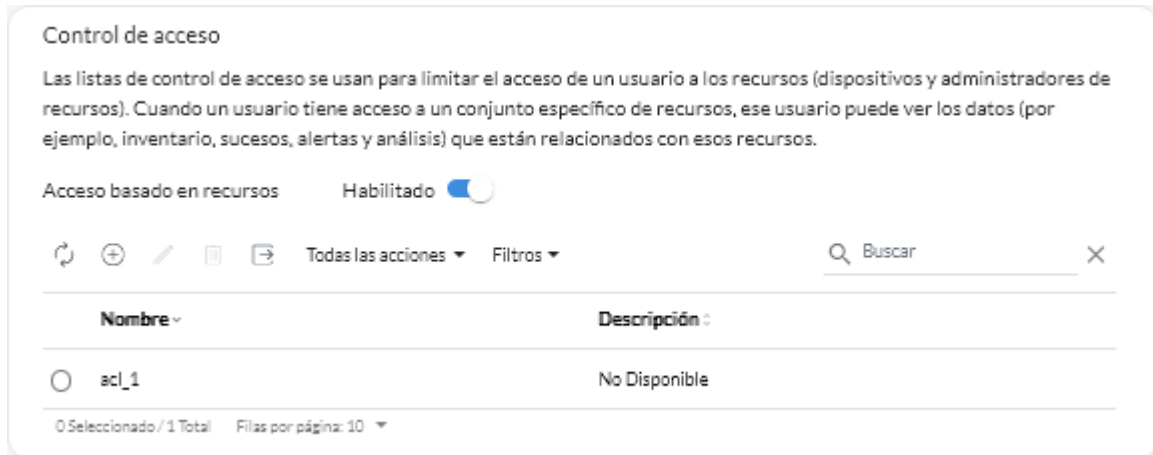
Cuando el acceso basado en recursos está habilitado, los usuarios que *no son* miembros de un grupo al que se ha asignado el rol de **Supervisor** predefinido no tienen acceso a ningún recurso (dispositivos y gestores de recursos) de manera predeterminada. Debe añadir usuarios no supervisor a un grupo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

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

Procedimiento

Para habilitar los controles de acceso basado en recursos, lleve a cabo los siguientes pasos.

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



Paso 2. Haga clic en el alternador **Acceso basado en recursos** para habilitar el control de acceso a recursos usando listas de control de acceso.

Creación de listas de control de acceso

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

Antes de empezar

Más información:  [Cómo crear listas de control de acceso](#)

Asegúrese de que los grupos de usuarios que desee asociar con el ACL estén definidos (consulte [Creación de grupos de usuario](#)).

Asegúrese de que todos los grupos de recursos que desee asociar con este ACL estén definidos (consulte [Creación de grupos de recursos](#)).

Acerca de esta tarea

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

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

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

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

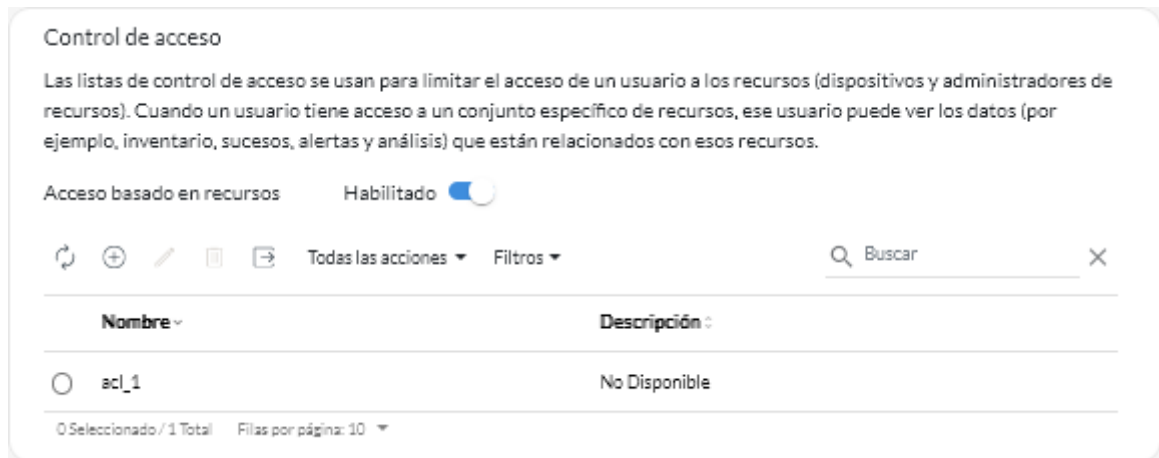
- *Los grupos de recursos* identifican los recursos (dispositivos, administradores de recursos y XClarity Orchestrator) a los que se puede acceder. El ACL debe contener al menos un grupo de recursos.

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

Procedimiento

Para crear una lista de control de acceso, lleve a cabo los siguientes pasos.

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



- Paso 2. Haga clic en el icono de **Añadir** (+) para agregar un ACL. Se muestra el cuadro de diálogo Crear control de acceso
- Paso 3. Especifique el nombre y descripción opcional del ACL.
- Paso 4. Haga clic en **Grupo de usuarios** y seleccione los grupos de usuarios que desee incluir en este ACL.
- Paso 5. Haga clic en **Grupos de recursos** y seleccione los grupos de recursos que desee incluir en este ACL.
- Paso 6. Haga clic en **Crear**.

La lista de control de acceso se agrega a la tabla

Después de finalizar

Puede realizar las siguientes acciones en esta página.

- Ver el grupo de usuarios y los grupos de recursos en un ACL específico haciendo clic en cualquier parte de la fila de ese ACL.
- Modifique las propiedades y la membresía de un ACL seleccionado haciendo clic en el icono de **Editar** (✎).
- Elimine un ACL seleccionado haciendo clic en el icono de **Eliminar** (🗑).
- Si un usuario no puede acceder a los datos de un recurso específico o si un usuario puede acceder a los datos de un recurso específico al que no debe accederse, identifique las listas de control de acceso que están asociadas con el usuario y, a continuación, consulte la membresía de cada grupo de recursos que

también esté asociado con esas listas de control de acceso. Asegúrese de que el recurso en cuestión esté o no esté incluido en esos grupos de recursos.

Gestión del espacio en el disco duro

Puede gestionar la cantidad de espacio de disco que usa Lenovo XClarity Orchestrator al eliminar archivos que no son necesarios

Acerca de esta tarea

Procedimiento

Para eliminar archivos innecesarios, lleve a cabo uno o más de los siguientes procedimientos.

Archivos de datos del servicio del dispositivo

1. En la barra de menús de Lenovo XClarity Orchestrator, haga clic en **Administración** (⚙️) → **Servicio y soporte** y, a continuación, haga clic en la pestaña **Datos de servicio** para mostrar la tarjeta Datos de servicio de dispositivo.
2. Seleccione uno o varios archivos de datos de servicio que desee eliminar y, a continuación, haga clic en el icono **Eliminar** (🗑️).

Imágenes del sistema operativo

1. En la barra de menús de Lenovo XClarity Orchestrator, haga clic en **Administración** (⚙️) → **Despliegue del SO** y, a continuación, haga clic en la pestaña **Gestión de SO** para mostrar la tarjeta Imágenes de SO.
2. Seleccione una o más imágenes del SO que desee eliminar y, a continuación, haga clic en el icono de **Eliminar** (🗑️).

Actualizar los archivos de carga útil

Asegúrese de que las actualizaciones no estén en uso en una política de conformidad de actualización. Puede quitar una actualización de una política de la tarjeta Aplicar y activar (consulte [Creación y asignación de políticas de conformidad de actualización](#)).

1. En la barra de menús de XClarity Orchestrator, haga clic en **Aprovisionamiento** (🔧) → **Actualizaciones** y, a continuación, haga clic en la pestaña **Gestión de repositorio** para mostrar la tarjeta Gestión de repositorio.
2. Seleccione una o más paquetes o archivos de actualización a eliminar.
3. Haga clic en el icono de **Eliminar únicamente los archivos de carga útil** (🗑️) para eliminar solo el archivo de imágenes (carga útil) para cada actualización seleccionada. La información acerca de la actualización (el archivo de metadatos XML) permanece en el repositorio y el estado de descarga cambia a “No descargado”.

Actualizaciones de XClarity Orchestrator

Puede eliminar actualizaciones del servidor de Orchestrator que están en estado Descargado. La columna **Estado aplicado** en la tabla indica el estado de la actualización.

1. En la barra del menú de XClarity Orchestrator, haga clic en **Mantenimiento** (🔧) y luego haga clic en la pestaña **Actualización de Orchestrator Server** para mostrar la tarjeta Actualización de Orchestrator Server.
2. Seleccione una o más actualizaciones que desee eliminar y, a continuación, haga clic en el icono **Eliminar** (🗑️). La columna **Adquirir estado** de las actualizaciones eliminadas cambia a “No descargado”.

Reiniciar XClarity Orchestrator

Existen ciertas situaciones en las que es posible que tenga que reiniciar Lenovo XClarity Orchestrator, como cuando se vuelve a generar o cargar un certificado de servidor. Puede reiniciar Lenovo XClarity Orchestrator desde la interfaz de web.

Antes de empezar

Debe tener permiso de **Supervisor** para reiniciar XClarity Orchestrator.

Considere la posibilidad de hacer una copia de seguridad del servidor de Orchestrator antes de reiniciarlo (consulte [Creación de copia de seguridad y restauración de datos de servidor de organización](#)).

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](#).

Durante el proceso de reinicio, los trabajos se detienen, se cierra la sesión de todos los usuarios y se pierde la conectividad con el servidor de Orchestrator. Espere 15 minutos o más (en función del número de dispositivos gestionados) para que el servidor de Orchestrator se reinicie antes de volver a iniciar sesión ([Inicio de sesión en XClarity Orchestrator](#)).

Cuando XClarity Orchestrator 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.

Procedimiento

Para reiniciar XClarity Orchestrator, lleve a cabo uno de los siguientes procedimientos.

En la interfaz de usuario

1. En la barra de menús de XClarity Orchestrator, haga clic en **Mantenimiento → Reinicio del dispositivo**.
2. Haga clic en **Reiniciar**.
3. Haga clic en **Sí**.
4. Actualice el navegador.

Desde el hipervisor

Microsoft Hyper-V

1. En el Panel de Server Manager, haga clic en **Hyper-V**.
2. Haga clic con el botón derecho del ratón en el servidor y haga clic en **Administrador de Hyper-V**.
3. Haga clic con el botón derecho en la máquina virtual y en **Restablecer**.

VMware ESXi

1. Conéctese al host a través de VMware vSphere Client.
2. Haga clic con el botón derecho del ratón en la máquina virtual y, a continuación, haga clic en **Alimentación → Restablecer**.
3. Haga clic en la pestaña **Consola**.

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

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

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

```
=====
```

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

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

... ..

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

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

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

Creación de copia de seguridad y restauración de datos de servidor de organización

Lenovo XClarity Orchestrator no incluye funciones integradas de copia de seguridad y restauración. En su lugar, utilice las funciones de copia de seguridad disponibles según el sistema operativo del host virtual donde esté instalado XClarity Orchestrator.

Acerca de esta tarea

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

- Antes de actualizar XClarity Orchestrator
- Después de realizar cambios en la red
- Después de agregar usuarios al servidor de autenticación local de XClarity Orchestrator
- Después de gestionar nuevos gestores de recursos

Si dispone de procedimientos de copia de seguridad y restauración para hosts virtuales, asegúrese de que sus procedimientos incluyan XClarity Orchestrator.

Importante:

- Asegúrese de que todos los trabajos en ejecución se han completado y de que ha apagado XClarity Orchestrator antes de crear una copia de seguridad.
- Asegúrese de realizar una copia de seguridad de XClarity Orchestrator de forma periódica. Si el sistema operativo del host se apaga de forma inesperada, puede que no pueda autenticarse con XClarity Orchestrator después de reiniciar el sistema operativo del host. Para resolver este problema, restaure XClarity Orchestrator a partir de la última copia de seguridad realizada.

Creación de copia de seguridad y restauración de datos de servidor de organización en un host VMware ESXi

Es posible que, en ocasiones, deba restaurar los datos del servidor de organización desde una copia de seguridad. Hay varias alternativas disponibles para crear copias de seguridad y restaurar un dispositivo virtual de XClarity Orchestrator que se ejecuta en un host VMware ESXi. El proceso específico que se utiliza para restaurar a partir de una copia de seguridad normalmente está basado en el proceso que se haya utilizado para crear la copia de seguridad. En este tema se analiza cómo crear copias de seguridad y restaurar utilizando el cliente VMware vSphere Client.

Acerca de esta tarea

Si VMware vCenter Server está instalado, puede utilizar la capacidad de copia de seguridad que se proporciona con VMware vCenter para crear una copia de seguridad de XClarity Orchestrator.

Si no tiene instalado VMware vCenter Server, puede utilizar VMware vSphere Client para crear una copia de seguridad de la máquina virtual copiando los archivos desde la carpeta XClarity Orchestrator hasta otra carpeta del mismo almacén de datos. También puede copiar los archivos en un almacén de datos distinto o incluso en un host distinto para obtener una protección de copia de seguridad adicional.

Nota: No es necesario que VMware vCenter Server realice una copia de seguridad mediante este procedimiento.

Procedimiento

- **Creación de copia de seguridad de XClarity Orchestrator** Lleve a cabo los pasos siguientes para crear una copia de seguridad de XClarity Orchestrator utilizando VMware vSphere Client.
 1. Apague XClarity Orchestrator.
 2. Inicie VMware vSphere Client y conéctese al host ESXi en el que se ubica XClarity Orchestrator.
 3. Cree una nueva carpeta en el mismo almacén de datos utilizado por XClarity Orchestrator.
 - a. Seleccione el host ESXi en el árbol de navegación y haga clic en la pestaña **Configurar** que se encuentra en la ventana de la derecha.
 - b. Haga clic en **Hardware → Almacenamiento**.
 - c. Pulse con el botón derecho en el almacén de datos de XClarity Orchestrator y, a continuación, pulse **Examinar almacén de datos**.
 - d. Seleccione la carpeta raíz y luego cree una carpeta nueva para incluir una copia de los archivos de XClarity Orchestrator.
 4. Pulse la carpeta XClarity Orchestrator.
 5. Seleccione todos los archivos de la carpeta y cópielos en la carpeta de copia de seguridad que acaba de crear.
 6. Reinicie XClarity Orchestrator.
- **Restauración de XClarity Orchestrator** Lleve a cabo el siguiente procedimiento para restaurar XClarity Orchestrator utilizando la copia de seguridad creada en el paso anterior.
 1. Inicie VMware vSphere Client y conéctese al host ESXi en el que se instala XClarity Orchestrator.

2. En el árbol de navegación izquierdo, haga clic con el botón derecho del mouse en XClarity Orchestrator y, a continuación, haga clic en **Alimentación → Apagar**.
3. En el árbol de navegación izquierdo, pulse de nuevo con el botón derecho del ratón en XClarity Orchestrator y, a continuación, pulse **Quitar de inventario**.
4. Elimine los archivos de la carpeta de XClarity Orchestrator en el almacén de datos utilizado por XClarity Orchestrator.
 - a. Seleccione el host ESXi en el árbol de navegación y, a continuación, pulse la pestaña **Configurar** en la ventana de la derecha.
 - b. Haga clic en **Hardware → Almacenamiento**.
 - c. Pulse con el botón derecho en el almacén de datos de XClarity Orchestrator y, a continuación, pulse **Examinar almacén de datos**.
 - d. Seleccione la carpeta XClarity Orchestrator.
 - e. Seleccione todos los archivos de la carpeta, pulse con el botón derecho del ratón en los archivos y, a continuación, pulse **Eliminar elementos seleccionados**.
5. Seleccione la carpeta donde se almacenarán los archivos de copia de seguridad.
6. Seleccione todos los archivos de la carpeta y cópielos en la carpeta de XClarity Orchestrator.
7. En la carpeta de XClarity Orchestrator, pulse con el botón derecho en el archivo VMX y, a continuación, pulse **Añadir a inventario**.
8. Complete el asistente para añadir datos de XClarity Orchestrator.
9. Reinicie XClarity Orchestrator desde VMware vSphere Client.
10. Cuando el sistema le solicite que elija si la MV se ha movido o copiado, seleccione **movida**.

Importante: Si selecciona **copiada**, la MV recibe un UUID que es diferente del de la MV original, lo que hace que la MV actúe como una instancia nueva y sea incapaz de ver dispositivos gestionados con anterioridad.

Creación de copia de seguridad y restauración de datos de servidor de organización en un host Microsoft Hyper-V

Es posible que, en ocasiones, deba restaurar los datos del servidor de organización de Lenovo XClarity Orchestrator desde una copia de seguridad. Hay varias alternativas disponibles para crear copias de seguridad y restaurar un dispositivo virtual de XClarity Orchestrator que se ejecuta en un host Microsoft Hyper-V. El proceso específico que se utiliza para restaurar a partir de una copia de seguridad normalmente está basado en el proceso que se haya utilizado para crear la copia de seguridad. En este tema se analiza cómo crear copias de seguridad y restaurar utilizando Windows Server Backup.

Antes de empezar

Asegúrese de que Windows Server Backup esté correctamente configurado siguiendo los pasos que se indican a continuación.

1. Inicie Windows Server Manager.
2. Pulse **Gestionar → Añadir roles y características**.
3. Avance por el asistente hasta llegar a la página de **Seleccionar características**.
4. Seleccione el recuadro de selección **Copia de seguridad de Windows Server**.
5. Complete el asistente.

Procedimiento

- **Creación de copia de seguridad de XClarity Orchestrator** Para crear una copia de seguridad de XClarity Orchestrator utilizando Windows Server Backup, complete los siguientes pasos.

1. Inicie Copia de seguridad de Windows Server y vaya a **Copia de seguridad local**.
 2. En el panel de acciones, pulse **Copia de seguridad única** para iniciar el asistente de Copia de seguridad única.
 3. En la página Opciones de copia de seguridad, pulse **Opciones diferentes** y, a continuación, pulse **Siguiente**
 4. En la página Seleccionar configuración de copia de seguridad, pulse **Personalizado** y, a continuación, pulse **Siguiente**.
 5. En la página Seleccionar elementos para la copia de seguridad, pulse **Añadir elementos** para mostrar la ventana Seleccionar elementos.
 6. Expanda el elemento Hyper-V, pulse la máquina virtual de XClarity Orchestrator y luego da clic en **Aceptar**.
 7. Haga clic en **Siguiente** para continuar.
 8. En la página Especificar tipo de destino, elija el tipo de almacenamiento para la copia de seguridad (en una unidad local o en una carpeta remota compartida) y pulse **Siguiente**.
 9. En la página Seleccionar destino de copia de seguridad o Especificar carpeta remota, especifique la ubicación en la que desea almacenar la copia de seguridad y, a continuación, pulse **Siguiente**.
 10. Haga clic en **Copia de seguridad** para iniciar el proceso de copia de seguridad.
- **Restauración de XClarity Orchestrator** Lleve a cabo el siguiente procedimiento para restaurar XClarity Orchestrator utilizando la copia de seguridad creada en el paso anterior.
 1. Inicie Copia de seguridad de Windows Server y vaya a **Copia de seguridad local**.
 2. En el panel Acción, pulse **Recuperar** para iniciar el asistente de recuperación.
 3. En la página Introducción, especifique la ubicación donde está almacenada la copia de seguridad y, a continuación, pulse **Siguiente**.
 4. En la página Seleccionar fecha de copia de seguridad, elija la copia de seguridad que desea restaurar y, a continuación, pulse **Siguiente**.
 5. En la página Seleccionar tipo de recuperación, seleccione la **Opción de Hyper-V** y luego haga clic en **Siguiente**.
 6. En la página Seleccionar elementos para recuperar, expanda Hyper-V y seleccione la máquina virtual de XClarity Orchestrator. A continuación, haga clic en **Siguiente**.
 7. En la página Especificar opciones de recuperación, seleccione recuperar la ubicación original de la MV y, a continuación, pulse **Siguiente**.
 8. En la página Confirmación, pulse **Recuperar**. La máquina virtual se restaurará y registrará en Hyper-V.
 9. Reinicie XClarity Orchestrator desde el Administrador de Hyper-V.

Capítulo 3. Supervisión de recursos y actividades

Puede utilizar Lenovo XClarity Orchestrator para supervisar inventarios de activos, cumplimiento de firmware y configuración, estado e historial de sucesos de sus dispositivos gestionados.

Visualización de un resumen del estado de su entorno

El panel es el centro de Lenovo XClarity Orchestrator que le brinda acceso a la información importante para usted. Contiene tarjetas de informe que resumen el estado de los recursos y las actividades en su entorno, incluidos el estado, el cumplimiento y las alertas de los dispositivos.

Para tener acceso al panel, haga clic en **Panel** (88) en el menú XClarity Orchestrator.

Puede cambiar el ámbito del resumen a solo los dispositivos gestionados por un gestor de recursos específico o en un grupo de recursos específico mediante el uso del menú desplegable **Seleccionar gestor**.

Puede hacer clic en cualquiera de las estadísticas vinculadas en el Panel para ver una lista filtrada de los datos que se ajustan a los criterios.

Garantía

La tarjeta de Garantía resume el periodo de garantía de los dispositivos gestionados, incluidos los siguientes datos.

- Número de dispositivos para los que la garantía ha caducado
- Número de dispositivos para los que la garantía está activa
- Número de dispositivos para los que los datos de garantía no están disponibles

Informes de servicio

La tarjeta de Informes de servicio resume el gestionado, incluidos los datos siguientes.

- Número total de informes de servicio activos
- Número de informes de servicio abiertos
- Número de informes de servicio en curso
- Número de informes de servicio en espera
- Número de informes de servicio cerrados
- Número de informes de servicio en otros estados

Cumplimiento de firmware

La tarjeta de Cumplimiento de firmware resume el cumplimiento con la política de cumplimiento de firmware asignada a los dispositivos gestionados en XClarity Orchestrator, incluidos los siguientes datos.

- Número de dispositivos *no* conformes.
- Número de dispositivos conformes
- Número de dispositivos que *no* tienen una política de cumplimiento de firmware asignada
- Número de dispositivos *no* conformes.
- Número de dispositivos para los que se está verificando la conformidad con la política asignada

Nota: Estos datos representan la conformidad del firmware basándose en las políticas asignadas por XClarity Orchestrator. No representa las políticas asignadas por gestores de recursos gestionados de Lenovo XClarity Administrator.

Cumplimiento de configuración

La tarjeta de Cumplimiento de configuración resume el cumplimiento con los patrones de configuración del servidor en dispositivos gestionados, incluidos los siguientes datos.

- Número de dispositivos que *no* son conformes con sus patrones asignados
- Número de dispositivos que cumplen con sus patrones asignados
- Número de dispositivos que *no* tienen un patrón asignado
- Número de dispositivos para los que hay una revisión de cumplimiento de configuración en curso
- Número de dispositivos para los que se requiere un reinicio manual para completar el despliegue del patrón (reinicio pendiente)
- Número de dispositivos para los que falló la última implementación de patrón

Nota: Estos datos representan el cumplimiento de configuración del servidor de todos los dispositivos en función de patrones asignados por XClarity Orchestrator. No representa patrones asignados por gestores de recursos gestionados de XClarity Administrator.

Correcciones de seguridad

La tarjeta Correcciones de seguridad resume el número de dispositivos gestionados que tienen vulnerabilidades y exposiciones comunes (CVE) para las cuales hay disponible una corrección de seguridad, según la máxima gravedad de CVE.

- Número de dispositivos con vulnerabilidades, como mínimo, críticas
- Número de dispositivos que tienen al menos una o más vulnerabilidades altas, medias o bajas, pero que no tienen vulnerabilidades críticas
- Número de dispositivos sin vulnerabilidades conocidas y protegidos

Antigüedad de firmware

La tarjeta de Antigüedad de firmware resume la antigüedad del firmware por tipo de componente.

- Número de firmware con más de 2 años de antigüedad para cada tipo de componente
- Número de firmware entre 1 y 2 años de antigüedad para cada tipo de componente
- Número de firmware entre 6 meses y 1 año de antigüedad para cada tipo de componente
- Número de firmware con menos de 6 meses de antigüedad para cada tipo de componente

Estado de condición general

La tarjeta de Estado general resume los dispositivos gestionados que actualmente están en buen y mal estado en su entorno.



Esta tarjeta incluye los datos siguientes.

- Un gráfico circular que representa el porcentaje de dispositivos gestionados en buen estado (normal) y en mal estado (crítico, advertencia y desconocido)

Consejo: cada barra coloreada en el gráfico circular indica el número de dispositivos en un estado específico. Puede pasar el cursor sobre cada barra coloreada para obtener más información sobre el estado.

- Número total y porcentaje de dispositivos en buen y mal estado
- Número de dispositivos de cada tipo que actualmente están en estado crítico, de advertencia, normal y desconocido

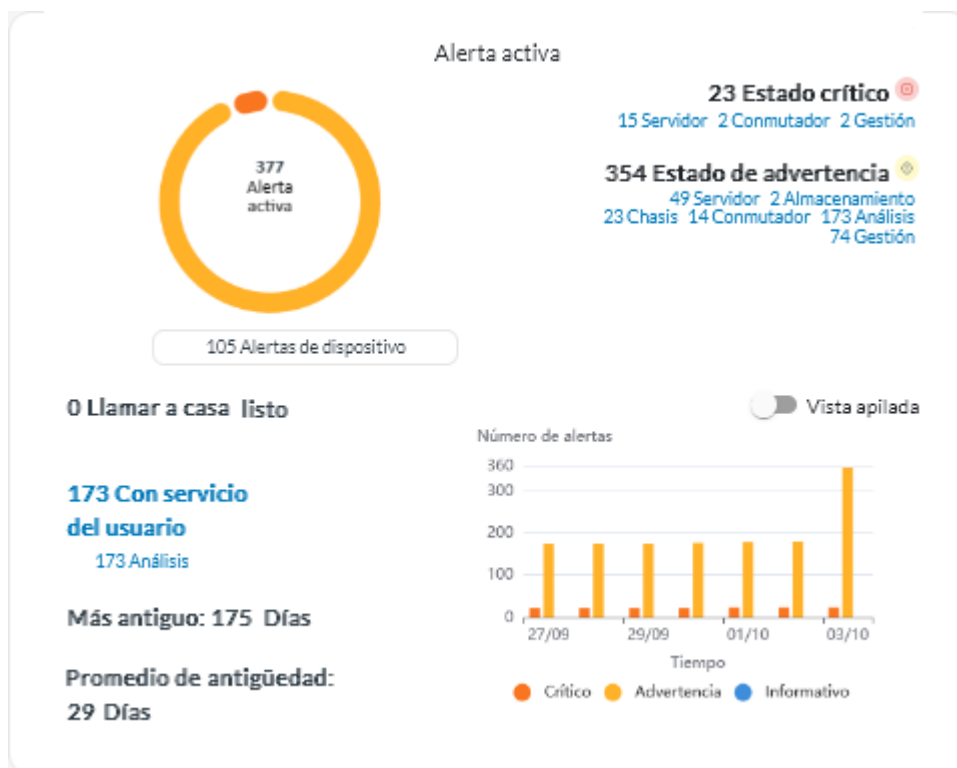
Consejo: puede hacer clic en el número de dispositivos de un estado específico para abrir una página con una lista filtrada de dispositivos que cumplen los criterios.

- Un gráfico de línea que representa el número de dispositivos en estados incorrecto, con el tiempo

Consejo: cada barra coloreada en el gráfico de barras indica el número de dispositivos en un estado específico. Puede pasar el cursor sobre cada barra coloreada para obtener más información sobre el estado.

Alertas activas

La tarjeta de Alertas activas de dispositivos resume las alertas activas generadas por los dispositivos gestionados.



Esta tarjeta incluye los datos siguientes.

- Gráfico circular que representa el porcentaje de las alertas activas de cada gravedad (crítico, advertencia, informativo y desconocido)

Consejo: cada barra coloreada en el gráfico circular indica el número de alertas con una gravedad específica. Puede pasar el cursor sobre cada barra coloreada para obtener más información sobre la gravedad.

- Número total de alertas activas
- Número de dispositivos que tienen alertas activas
- Número total de alertas activas para cada gravedad y el número de dispositivos de cada tipo que tienen alertas activas para cada gravedad

Consejo: puede hacer clic en el número de dispositivos de un estado específico para abrir una página con una lista filtrada de dispositivos que cumplen los criterios.

- Un gráfico de línea que representa el número de dispositivos en estados incorrecto, con el tiempo

Consejo: cada barra coloreada en el gráfico de barras indica el número de alertas con una gravedad específica. Puede pasar el cursor sobre cada barra coloreada para obtener más información sobre la gravedad.

- Número de alertas activas que abrieron un informe de servicio con el Centro de Soporte de Lenovo (Llamar a casa)
- Número total de alertas activas que requieren acción del usuario (reparables por el usuario) y el número de dispositivos de cada tipo que tienen alertas activas reparables por el usuario
- Antigüedad de la alerta activa más antigua
- Antigüedad promedio de todas las alertas activas

Visualización del estado y los detalles del gestor de recursos

Puede ver el tipo, la versión, el estado y la conectividad de cada gestor de recursos.

Acerca de esta tarea

La columna **Estado** identifica el estado general de un gestor de recursos. Se utilizan los siguientes estados.

- (✓) Normal
- (⚠) Advertencia
- (✗) Crítico

Procedimiento

Para ver los detalles de los gestores de recursos, haga clic en **Recursos** (🔗) → **Gestor de recursos** desde la barra de menú de XClarity Orchestrator para mostrar la tarjeta de Gestores de recursos.

Gestores de recursos

Define los administradores de recursos a través de los cuales XClarity Orchestrator recibe información del dispositivo y realiza funciones de gestión.






 Todas las acciones ▾ Filtros ▾ X

<input type="checkbox"/>	Gestor de re	Estado :	Tipo :	Versión :	Build :	Conectado :	Datos de aná	Grupos :
<input type="checkbox"/>	XClarity ...	No...	XClarity ...	2.0.0	279	No Disponi	No Disponi	No Disponi
<input type="checkbox"/>	host-10-...	No...	XClarity ...	3.6.0	108	16/2/23 10		No Disponi

0 Seleccionado / 2 Total Filas por página: 10 ▾

Después de finalizar

Puede realizar las siguientes acciones desde la tarjeta Gestores de recursos.

- Conecte un gestor de recursos haciendo clic en el icono de **Conectar** (+) (consulte [Conexión de gestores de recursos](#)).
- Desconecte y quite un gestor de recursos seleccionado haciendo clic en el icono de **Eliminar** (☒).

Nota: Si XClarity Orchestrator no puede conectarse con el gestor de recursos (por ejemplo, si las credenciales han caducado o si hay problemas de red), seleccione **Forzar desconexión**.

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

Quando se quita el gestor de recursos, todos los dispositivos que gestiona dicho gestor de recursos también se quitan. Esto incluye el inventario de dispositivos, los registros, los datos de métrica y los informes analíticos.

- Para ver un resumen del estado de todos los gestores de recursos para un gestor de recursos seleccionado, haga clic en **Panel** (📄) en la barra de menú de XClarity Orchestrator. Puede restringir el alcance a un solo gestor de recursos o grupo de recursos mediante el menú desplegable **Seleccionar gestor**.

Visualización del estado de los dispositivos

Puede ver el estado de todos los dispositivos gestionados en todos los gestores de recursos.

Procedimiento

Para ver el estado de los dispositivos gestionados, lleve a cabo los pasos siguientes.

- **Resumen de estado de todos los dispositivos** Desde la barra de menú de XClarity Orchestrator, haga clic en **Panel** (📄) para mostrar las tarjetas del panel con una descripción general y el estado de todos los dispositivos gestionados y otros recursos (consulte [Visualización de un resumen del estado de su entorno](#)).

Puede cambiar el ámbito del resumen a solo los dispositivos gestionados por un gestor de recursos específico o en un grupo de recursos específico mediante el uso del menú desplegable **Seleccionar gestor**.



Cada barra coloreada en el gráfico circular y de barras indica el número de dispositivos en un estado específico. Puede pasar el cursor sobre cada barra coloreada para obtener más información sobre el estado. También puede hacer clic en el número de dispositivos en cada estado para ver una lista de todos los dispositivos que se ajustan a los criterios.

- **Estado de todos los dispositivos de un tipo específico** Para ver los resúmenes de alertas globales activas, haga clic en **Recursos** (🔍) en la barra de menú de XClarity Orchestrator y luego haga clic en el tipo de dispositivo para mostrar una tarjeta con una vista de tabla de todos los dispositivos de ese tipo. Por ejemplo, si selecciona **Servidores**, se muestra una lista de todos los bastidores, torres y servidores compactos, además de todos los servidores Flex System y ThinkSystem en un chasis.

Puede cambiar el alcance del resumen basado en la propiedad del dispositivo desde la lista desplegable **Analizar por**.

- **Modelo de tipo de equipo.** (Predeterminado) Este informe resume el estado del dispositivo por modelo de tipo de equipo (MTM).
- **Tipo de máquina.** Este informe resume el estado del dispositivo por tipo de equipo.
- **Nombre del producto.** Este informe resume el estado del dispositivo por producto.



XClarity Orchestrator resume el estado del dispositivo basándose en criterios específicos. Cada resumen incluye la siguiente información.

- Un gráfico circular que muestra el número total de dispositivos que están en mal estado y porcentaje de dispositivos en cada estado incorrecto (crítico, advertencia o desconocido).

Cada barra coloreada en el gráfico circular indica el número de dispositivos en un estado específico. Puede pasar el cursor sobre cada barra coloreada para obtener más información sobre el estado.

- Un gráfico de líneas que muestra el número de dispositivos para cada tipo de estado de condición por día sobre el número especificado de días.

Cada barra coloreada en el gráfico de líneas indica el número de dispositivos en un estado específico. Puede pasar el cursor sobre cada barra coloreada para obtener más información sobre el estado.

- El número de dispositivos de cada tipo que no están en un estado correcto en un día específico. El día actual se muestra de manera predeterminada. Puede cambiar el día pasando el cursor sobre cada día en el gráfico de líneas.

- **Estado de un dispositivo específico** Desde la barra de menú de XClarity Orchestrator, haga clic en **Recursos** (🔍) y luego haga clic en el tipo de dispositivo para mostrar una tarjeta con una vista de tabla de todos los dispositivos de ese tipo. Por ejemplo, si selecciona **Servidores**, se muestra una lista de todos los bastidores, torres y servidores compactos, además de todos los servidores Flex System y ThinkSystem en un chasis.

Servidores

Q Buscar X

Iniciar Control remoto
 Acciones de alimentación

 Todas las acciones

Filtros ▼

<input type="checkbox"/>	Servidor	Estado	Conectiv	Alimenta	Direccio	Nombre	Tipo-Mo	Firmwar	Aviso	Grupos
<input type="checkbox"/>	New...				10.24:	Leno...	719...	N3E1f	No ...	No Dis
<input type="checkbox"/>	ite-b...				10.24:	Leno...	716...	CGE1:	No ...	No Dis
<input type="checkbox"/>	Blac...				10.24:	Leno...	716...	A3EG:	No ...	No Dis
<input type="checkbox"/>	nod...				10.24:	IBM ...	791...	No Dis	No ...	No Dis
<input type="checkbox"/>	IM...				10.24:	IBM ...	873...	B2E11	No ...	No Dis
<input type="checkbox"/>	Cara...				10.24:	Eagl...	791...	No Dis	No ...	No Dis
<input type="checkbox"/>	blad...				10.24:	IBM ...	790...	No Dis	No ...	No Dis
<input type="checkbox"/>	New...				10.24:	Leno...	719...	N3E1f	No ...	No Dis
<input type="checkbox"/>	New...				10.24:	Leno...	719...	N3E1f	No ...	No Dis
<input type="checkbox"/>	New...				10.24:	Leno...	719...	N3E1f	No ...	No Dis

0 Seleccionado / 60 Total Filas por página: 10

La columna **Estado** identifica el estado general de un dispositivo. Se utilizan los siguientes estados. Si un dispositivo está en mal estado, use el registro de alertas para ayudar a identificar y resolver los problemas (consulte [Supervisión de alertas activas](#)).

- Normal
- Advertencia
- Crítico

En la columna **Conectividad** se identifica el estado de la conexión entre el dispositivo y XClarity Orchestrator. Se utilizarán los siguientes estados de conectividad.

- Fuera de línea
- Gestionado sin conexión
- En línea
- Parcial
- Pendiente

La columna **Alimentación** identifica el estado de alimentación. Se utilizan los siguientes estados de alimentación.

- Activado
- Desactivado

La columna **Asesoría** identifica el número de asesorías del cliente (consejos técnicos) en línea relacionados con cada servidor. Haga clic en el número para mostrar la tarjeta Asesoría en la página de detalles del dispositivo para mostrar una lista de asesorías de cliente en línea, incluido el resumen y el enlace de cada asesoría. Haga clic en un enlace para abrir una página web con los detalles de esa asesoría.

Después de finalizar

Puede llevar a cabo las siguientes acciones desde las tarjetas de dispositivo.

- Agregue un dispositivo seleccionado a un grupo haciendo clic en **Todas las acciones → Añadir elementos a un grupo**.
- Reenvía los informes sobre tipos de dispositivos específicos de forma periódica a una o varias direcciones de correo electrónico haciendo clic en el icono **Crear despachador de informes** (+). El informe se envía utilizando los filtros de datos aplicados actualmente a la tabla. Todas las columnas de la tabla mostradas y ocultas se incluyen en el informe. Para obtener más información, consulte el apartado [Reenvío de informes](#).
- Añada un informe acerca de un tipo de dispositivo específico a un despachador de informes específico utilizando los filtros de datos aplicados actualmente a la tabla haciendo clic en el icono de **Agregar a despachador de informes** (↗). Si el despachador de informes ya incluye un informe para ese tipo de dispositivo, este se actualiza para utilizar los filtros de datos actuales.

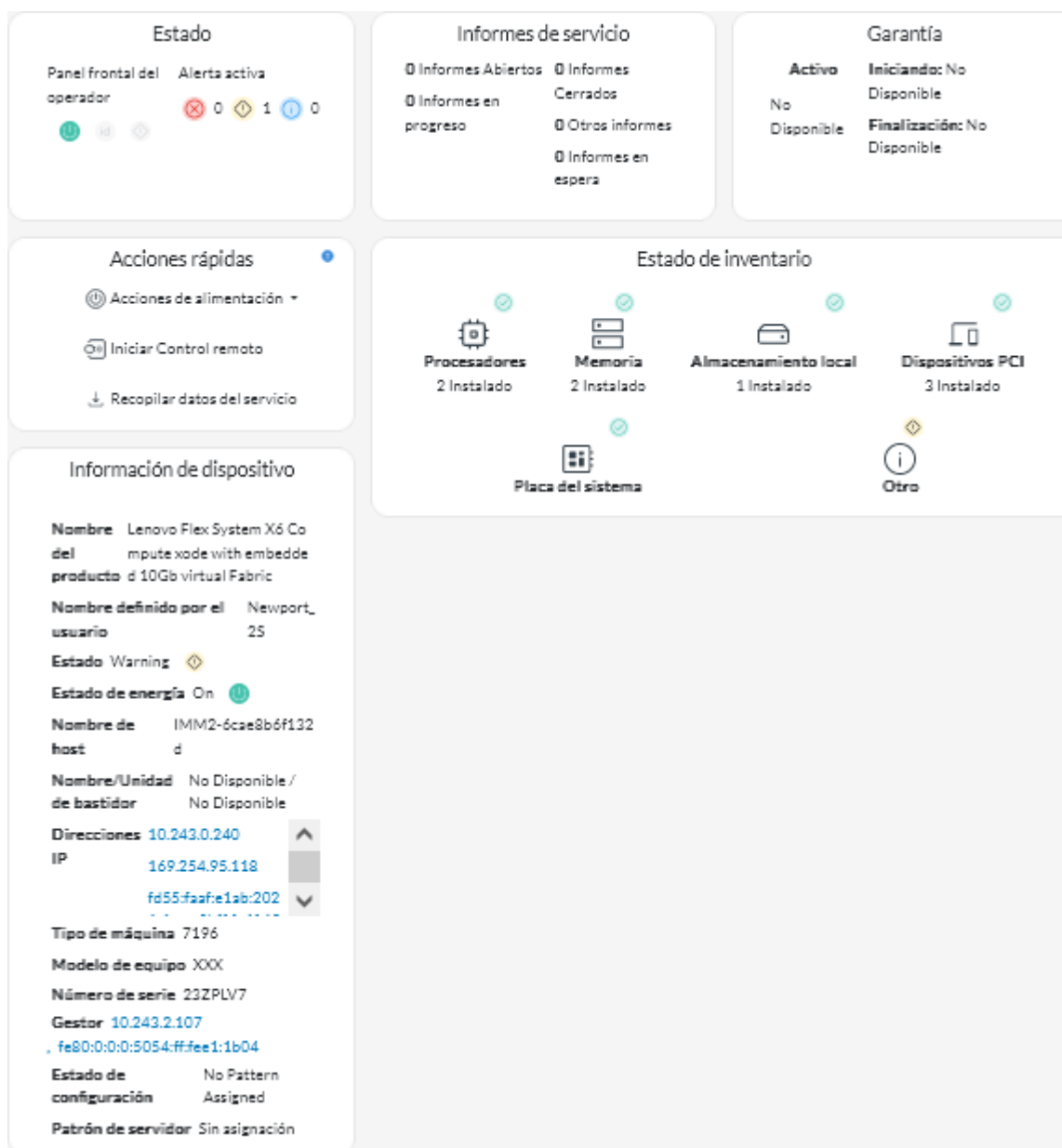
Visualización de los detalles del dispositivo

Puede ver información detallada sobre cada dispositivo, incluido el resumen general de estado del dispositivo, inventario, alertas y sucesos, métricas del sistema y firmware.

Procedimiento

Para ver los detalles de un dispositivo, lleve a cabo los pasos siguientes.






- Paso 1. Desde la barra de menú de XClarity Orchestrator, haga clic en **Recursos** (🔍) y luego haga clic en el tipo de dispositivo para mostrar una tarjeta con una vista de tabla de todos los dispositivos gestionados de ese tipo.
- Paso 2. Haga clic en la fila del dispositivo para mostrar las tarjetas de resumen del dispositivo para dicho dispositivo.



Paso 3. Lleve a cabo una o más de las acciones siguientes.

Los detalles en cada tarjeta pueden variar según el tipo de dispositivo.

- Haga clic en **Resumen** para ver un resumen general del dispositivo, incluida la información del dispositivo, el inventario, el estado, la información del SO, las métricas del sistema, los informes de servicio y la garantía. Esta página también incluye la tarjeta de **Acciones rápidas** que enumera las acciones que puede realizar en el dispositivo (como ejecutar acciones de alimentación, recopilar datos del servicio e iniciar una sesión de control remoto). Esta página muestra el estado de cada uno de los LED del panel frontal del operador.
 - **LED de encendido**
 - **Activado** (🟢). El dispositivo está encendido.
 - **Desactivado** (⚪). El dispositivo está apagado.
 - **LED de ubicación**

- **Activado** (). El LED de ubicación del panel de control también se ilumina.
- **Parpadeante** (). El LED de ubicación del panel de control también se ilumina o parpadea.
- **Desactivado** (). El LED de ubicación del panel de control no se ilumina.
- **LED de falla**
 - **Activado** (). El LED de error del panel de control también se ilumina.
 - **Desactivado** (). El LED de error del panel de control no se ilumina.
- Haga clic en **Inventario** para ver detalles sobre los componentes de hardware en el dispositivo (como procesadores, módulos de memoria, unidades, fuentes de alimentación, dispositivos PCI y placa del sistema).

Notas:

- El inventario *no* es compatible con estos dispositivos de almacenamiento: ThinkSystem DS2200, Lenovo Storage S2200 y S3200 y Nodo de almacenamiento V7000 Flex System.
- Los detalles de firmware *no están* disponibles para estos dispositivos de almacenamiento: ThinkSystem DS4200 y DS6200 y Lenovo Storage DX8200C, DX8200D y DX8200N.
- Haga clic en **Registro de alertas** para mostrar la lista de alertas activas y estadísticas de alertas para el dispositivo (consulte [Supervisión de alertas activas](#)).
- Haga clic en **Registro de sucesos** para mostrar la lista de los sucesos del dispositivo(consulte [Supervisión de sucesos](#)).
- Haga clic en **Firmware** para mostrar una lista de niveles de firmware actuales del dispositivo y los componentes del dispositivo.
- Haga clic en **Servicio** para mostrar información sobre los archivos de datos del servicio y los informes de servicio del dispositivo.
- Haga clic en **Utilización** para mostrar las métricas de utilización, temperatura y alimentación del sistema a lo largo del tiempo para los dispositivos ThinkAgile y ThinkSystem.
- Haga clic en **Asesoría** para mostrar una lista de asesorías de clientes en línea, incluidos el resumen y el enlace de cada asesoría. Haga clic en un enlace para abrir una página web con los detalles de esa asesoría.

Después de finalizar

Además de mostrar un resumen e información detallada acerca de un dispositivo, también puede realizar las siguientes acciones en un dispositivo de esta página.

- Inicie la interfaz web del controlador de gestión de la placa base desde la pestaña **Resumen**, haciendo clic en la dirección IP principal del dispositivo.
- Haga clic en la dirección IP para iniciar la interfaz web del dispositivo en la pestaña **Resumen**.
- Inicie la interfaz web del gestor de recursos que gestiona el dispositivo desde la pestaña **Resumen**, haciendo clic en el nombre o la dirección IP del gestor de recursos.

Visualización del estado y los detalles de los recursos de infraestructura

Puede ver el estado e información detallada de los recursos de la infraestructura del centro de datos (como PDU y SAI), que se gestionan mediante un gestor de recursos de Schneider Electric EcoStruxure IT Expert.

Antes de empezar

La columna **Estado** identifica el estado general de un recurso de infraestructura. Se utilizan los siguientes estados. Si los recursos de una infraestructura están en mal estado, use el registro de alertas para ayudar a identificar y resolver los problemas (consulte [Supervisión de alertas activas](#)).

- (🟢) Normal
- (🟡) Advertencia
- (🔴) Crítico

Procedimiento


- **Estado de un recurso de infraestructura específico** Para ver el estado de los recursos de infraestructura, haga clic en **Recursos** (⚙️) → **Infraestructura** desde la barra de menús de XClarity Orchestrator para mostrar la tarjeta de Infraestructura. Si el recurso de una infraestructura está en mal estado, use el registro de alertas para ayudar a identificar y resolver los problemas (consulte [Supervisión de alertas activas](#)).

Nombre	Estado	Nombre de host	Fabricante	Modelo	Tipo	Grupos
APC_R18	🔴 Crítico	APC_R18	Server Tec...	Sentry Swit...	Rack PDU	No Disponi...
APC_R21	🟢 Normal	APC_R21	Server Tec...	Sentry Swit...	Rack PDU	No Disponi...
EcoStruxur...	🟢 Normal	No Disponi...	Schneider ...	EcoStruxur...	Gateway	No Disponi...
Sentry3_5...	🟢 Normal	Sentry3_5...	Server Tec...	Sentry Swit...	Rack PDU	bangalore-gr
Sentry3_5...	🔴 Crítico	Sentry3_5...	Server Tec...	Sentry Swit...	Rack PDU	Andrei-Testir
Sentry3_5...	🟢 Normal	Sentry3_5...	Server Tec...	Sentry Swit...	Rack PDU	Romania-PDI
Sentry3_5...	🟢 Normal	Sentry3_5...	Server Tec...	Sentry Swit...	Rack PDU	TestRefreshG
Sentry3_5...	🟢 Normal	Sentry3_5...	Server Tec...	Sentry Swit...	Rack PDU	DemoGroup
UPSR11	🔴 Crítico	UPSR11	MGE	9135 6000	UPS	Work group1

0 Seleccionado / 9 Total Filas por página: 10

- **Detalles de un recurso de infraestructura específico**

1. En la barra de menú de XClarity Orchestrator, haga clic en **Recursos** (⚙️) → **Infraestructura** para mostrar la tarjeta Infraestructura.
2. Haga clic en la fila del recurso de infraestructura para mostrar la tarjeta de resumen de ese recurso.
3. Lleve a cabo una o más de las acciones siguientes.
 - Haga clic en **Resumen** para ver un resumen general del recurso, incluida la información del dispositivo y el estado.

- Haga clic en **Registro de alertas** para mostrar la lista de alertas activas y estadísticas de alertas para el recurso (consulte [Supervisión de alertas activas](#)).
- Haga clic en **Registro de sucesos** para mostrar la lista de los sucesos del recurso (consulte [Supervisión de sucesos](#)).
- Haga clic en **Sensores** para mostrar la lista de sensores del recurso. Puede determinar la medición más reciente del sensor en la tarjeta Sensores, o bien puede seleccionar uno o más sensores y luego hacer clic en el icono de **Gráfico** () para ver los gráficos de línea a lo largo del tiempo para cada sensor seleccionado. Los sensores con la misma unidad (como vatios o amperios) se generan en el mismo gráfico.

Nota: Schneider Electric EcoStruxure IT Expert recopila datos del sensor cada 5 minutos y XClarity Orchestrator sincroniza estos datos cada hora. Actualmente, XClarity Orchestrator solo guarda los últimos 60 minutos de datos.

Después de finalizar

Además de mostrar un resumen e información detallada acerca de un recurso de infraestructura, también puede realizar las siguientes acciones desde esta página.

- Haga clic en la dirección IP del recurso para iniciar la interfaz web de determinados recursos de infraestructura desde la pestaña **Resumen**.

Supervisión de trabajos

Los *Trabajos* son tareas de ejecución prolongada que se ejecutan en segundo plano. Puede ver un registro de todos los trabajos iniciados mediante Lenovo XClarity Orchestrator.

Acerca de esta tarea



Si una tarea de larga ejecución apunta a varios recursos, se crea un trabajo independiente para cada recurso.

Puede ver el estado y detalles acerca de cada trabajo en el registro de trabajos. El registro de trabajos puede contener como máximo 500 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.

Nota: Los trabajos que están en ejecución durante más de 24 horas se detienen y se colocan en el estado Caducado.




Procedimiento

Para ver los trabajos, lleve a cabo uno o más de los pasos siguientes.

- **Ver programados** Haga clic en **Supervisión** () → **Trabajos** en la barra de menús de XClarity Orchestrator y, a continuación, haga clic en la pestaña **Trabajos programados** para mostrar la tarjeta Trabajos programados. Esta tarjeta muestra información acerca de cada trabajo programado, incluido el estado, la indicación de hora cuando el trabajo está programado para ejecutarse y la indicación de hora cuando se inició el trabajo.
- **Ver trabajo** Haga clic en **Supervisión** () → **Trabajos** desde la barra de menú de XClarity Orchestrator para mostrar la tarjeta de Trabajos. Esta tarjeta enumera la información acerca de cada trabajo, incluidos el estado, el progreso, las marcas de tiempo de inicio y fin y el recurso de destino.

Trabajos

Los trabajos son tareas de larga ejecución realizadas en uno o varios sistemas de destino. Puede elegir si eliminar un trabajo o ver sus detalles.









 Todas las acciones ▾ Filtros ▾ Q Buscar








	Nombre del	Estado	Progreso	Hora de inic	Hora de fins	Destino	Categoría	Creado por
<input type="radio"/>	Asignar p	Completado	100%	5 oct 202:	5 oct 202:	No Disp...	Actuali...	Orches...
<input type="radio"/>	Asignar p	Completado	100%	5 oct 202:	5 oct 202:	No Disp...	Actuali...	Orches...
<input type="radio"/>	Asignar p	Completado	100%	5 oct 202:	5 oct 202:	No Disp...	Actuali...	Orches...
<input type="radio"/>	Asignar p	Completado	100%	5 oct 202:	5 oct 202:	No Disp...	Actuali...	Orches...
<input type="radio"/>	Asignar p	Completado	100%	5 oct 202:	5 oct 202:	No Disp...	Actuali...	Orches...
<input type="radio"/>	Procesar	Anulado	100%	5 oct 202:	5 oct 202:	SN#Y0...	Servicio	Orches...
<input type="radio"/>	Procesar	Anulado	100%	4 oct 202:	4 oct 202:	SN#Y0...	Servicio	Orches...
<input type="radio"/>	Procesar	Anulado	100%	4 oct 202:	4 oct 202:	SN#Y0...	Servicio	Orches...
<input type="radio"/>	Procesar	Anulado	100%	4 oct 202:	4 oct 202:	SN#Y0...	Servicio	Orches...
<input type="radio"/>	Descarga	Completado	100%	4 oct 202:	4 oct 202:	XClarit...	Actuali...	Orches...

0 Seleccionado / 15 Total Filas por página: 10 ▾ ◀ 1 2 ▶ ▶▶

Para ver información detallada acerca de un trabajo, haga clic en la fila correspondiente a ese trabajo en la tabla. Se muestran tarjetas que enumeran información acerca de cada subtarea en el trabajo (incluido el estado, el progreso, las marcas de tiempo de inicio y fin, los dispositivos de destino y el registro de trabajos).

Conectar el administrador 10.243.10.122





 Todas las acciones ▾ Filtros ▾
 Buscar 

Nombre del trabajaj	Estado	Progreso	Hora de inicio	Hora de finalizaci	Destino
▾ Conectar el ac	 Completo	<div style="width: 100%;"><div style="width: 100%; background-color: #00a651; height: 10px;"></div></div> 100%	4 oct 2022 8:20>	4 oct 2022 8:20>	No Disponible
Importar c	 Completo	<div style="width: 100%;"><div style="width: 100%; background-color: #00a651; height: 10px;"></div></div> 100%	4 oct 2022 8:20>	4 oct 2022 8:20>	No Disponible
Comprobe	 Completo	<div style="width: 100%;"><div style="width: 100%; background-color: #00a651; height: 10px;"></div></div> 100%	4 oct 2022 8:20>	4 oct 2022 8:20>	No Disponible
Comprobe	 Completo	<div style="width: 100%;"><div style="width: 100%; background-color: #00a651; height: 10px;"></div></div> 100%	4 oct 2022 8:20>	4 oct 2022 8:20>	No Disponible
Comprobe	 Completo	<div style="width: 100%;"><div style="width: 100%; background-color: #00a651; height: 10px;"></div></div> 100%	4 oct 2022 8:20>	4 oct 2022 8:20>	No Disponible
> Configura	 Completo	<div style="width: 100%;"><div style="width: 100%; background-color: #00a651; height: 10px;"></div></div> 100%	4 oct 2022 8:20>	4 oct 2022 8:20>	No Disponible
Guardand	 Completo	<div style="width: 100%;"><div style="width: 100%; background-color: #00a651; height: 10px;"></div></div> 100%	4 oct 2022 8:20>	4 oct 2022 8:20>	No Disponible

7 Total Filas por página: 10 ▾

Después de finalizar

Puede llevar a cabo las siguientes acciones desde la tarjeta Trabajos.

- Para eliminar un trabajo o subtarea *completado* o *caducado* del registro de trabajos seleccione el trabajo o subtarea y haga clic en el icono de **Eliminar** ().

Supervisión de alertas activas

Las *Alertas* son sucesos de hardware o de organización que se deben investigar y necesitan la acción del usuario. Lenovo XClarity Orchestrator sondea los gestores de recursos en modo asíncrono y muestra las alertas que se reciben de dichos gestores.

Acerca de esta tarea

No existe un límite en el número de alertas activas que se almacenan en el repositorio local.

En la tarjeta de Alertas, puede ver una lista de todas las alertas activas.

Alertas

Las alertas indican condiciones de hardware o de gestión que necesitan investigación y alguna acción por parte del usuario.

Todas las acciones Filtros

	Fecha y hora	Gravedad	Alerta	Recurso	Capacidad de servicio	Tipo de recurso	Tipo de origen	Grupos
<input type="radio"/>	5/10/2...	Ad...	La conexión	XClarity...	Ni...	Chasis	Gestión	No Disponi...
<input type="radio"/>	5/10/2...	Ad...	La conexión	XClarity...	Ni...	Chasis	Gestión	No Disponi...
<input type="radio"/>	5/10/2...	Ad...	La conexión	XClarity...	Ni...	Conmu...	Gestión	No Disponi...
<input type="radio"/>	5/10/2...	Ad...	La conexión	XClarity...	Ni...	Conmu...	Gestión	No Disponi...
<input type="radio"/>	5/10/2...	Ad...	La conexión	XClarity...	Ni...	Conmu...	Gestión	No Disponi...
<input type="radio"/>	5/10/2...	Ad...	La conexión	XClarity...	Ni...	Conmu...	Gestión	No Disponi...
<input type="radio"/>	5/10/2...	Ad...	La conexión	XClarity...	Ni...	Conmu...	Gestión	No Disponi...
<input type="radio"/>	5/10/2...	Ad...	La conexión	XClarity...	Ni...	Conmu...	Gestión	No Disponi...
<input type="radio"/>	5/10/2...	Ad...	La conexión	XClarity...	Ni...	Conmu...	Gestión	No Disponi...
<input type="radio"/>	5/10/2...	Ad...	La conexión	XClarity...	Ni...	Conmu...	Gestión	No Disponi...

312 Total Filas por página: 10

La columna **Gravedad** identifica la gravedad de la alerta. Se utilizan las siguientes gravedades.

- **Informativo**. No se requiere ninguna acción.
- **Advertencia**. La acción se puede aplazar o no se requiere ninguna acción.
- **Crítico**. Se requiere una acción inmediata.

La columna **Capacidad de servicio** indica si el dispositivo requiere servicio y quién realiza ese servicio normalmente. Se utilizan los siguientes tipos de capacidad de servicio.

- **Ninguno**. La alerta es informativa y no requiere servicio.
- **Usuario**. Adopte las medidas de recuperación necesarias para resolver el problema.
- **Soporte**. Si la opción Llamar a casa está habilitada para XClarity Orchestrator o para el Gestor de recursos que gestiona el dispositivo asociado, la alerta normalmente se envía al Centro de Soporte de Lenovo, salvo que ya exista un informe de servicio abierto para el mismo Id. de alerta del dispositivo (consulte [Apertura automática de informes de servicio mediante la función Llamar a casa](#) en la documentación en línea de XClarity Orchestrator). Si la opción Llamar a casa no está habilitada, se recomienda que abra manualmente un informe de servicio para resolver el problema (consulte [Apertura manual de un informe de servicio en el Centro de Soporte de Lenovo](#) en la documentación en línea de XClarity Orchestrator).

Si existen alertas activas, las estadísticas de alertas se muestran en la tarjeta Análisis de alertas. Puede ver estadísticas de alertas por gravedad, origen, recurso y capacidad de servicio para el día actual y a lo largo de un período específico (consulte [Análisis de alertas activas](#)).



Procedimiento

Para ver las alertas activas, lleve a cabo uno o más de los siguientes pasos.

- **Ver todas las alertas activas** Haga clic en **Supervisión** (📊) → **Alertas** desde la barra de menús de XClarity Orchestrator para mostrar la tarjeta de Alertas.

Para ver información sobre una alerta específica, haga clic en la descripción de la columna **Alerta**. Se muestra una ventana emergente con información acerca del origen de la alerta, la explicación y las acciones de recuperación.

- **Ver alertas activas para un dispositivo específico**

1. Desde la barra de menú de XClarity Orchestrator, haga clic en **Recursos** (🔍) y luego haga clic en el tipo de dispositivo para mostrar una tarjeta con una vista de tabla de todos los dispositivos gestionados de ese tipo.
2. Haga clic en la fila de un dispositivo para mostrar las tarjetas de resumen del dispositivo para dicho dispositivo.
3. Haga clic en **Registro de alertas** para mostrar la lista de alertas activas para el dispositivo en la tarjeta de Análisis de alertas. Para ver información sobre una alerta específica, haga clic en la descripción de la columna **Alerta**. Se muestra una ventana emergente con información acerca del origen de la alerta, la explicación y las acciones de recuperación.

Supervisión de sucesos

Desde Lenovo XClarity Orchestrator, tiene acceso a una lista histórica de todos los sucesos de recursos y auditoría.

Más información:  [Cómo monitorear sucesos de dispositivo específico](#)




Acerca de esta tarea

Un *suceso de recursos* identifica una condición de hardware o de organización que se produjo en un dispositivo gestionado, un gestor de recursos o XClarity Orchestrator. Puede utilizar estos sucesos de auditoría para realizar seguimientos y analizar problemas relacionados con hardware y el servidor de organización.



Un *suceso de auditoría* es un registro de actividades del usuario que se realizaron desde un gestor de recursos o XClarity Orchestrator. Puede utilizar estos sucesos de auditoría para realizar seguimientos y analizar problemas relacionados con la autenticación.

El registro de sucesos contiene sucesos de recursos y de auditoría. Puede contener un máximo de 100.000 sucesos de todos los orígenes. Un máximo de 50.000 sucesos pueden ser de un único gestor de recursos y sus dispositivos gestionados. Un máximo de 1.000 sucesos pueden ser de un único dispositivo gestionado. Cuando se alcanza el número máximo de sucesos, el suceso más antiguo se elimina cuando se recibe el siguiente suceso.

La columna **Gravedad** identifica la gravedad del suceso. Se utilizan las siguientes gravedades.

-  **Informativo**. No se requiere ninguna acción.
-  **Advertencia**. La acción se puede aplazar o no se requiere ninguna acción.
-  **Crítico**. Se requiere una acción inmediata.

La columna **Capacidad de servicio** indica si el dispositivo requiere servicio y quién realiza ese servicio normalmente. Se utilizan los siguientes tipos de capacidad de servicio.

- **Ninguno**. La alerta es informativa y no requiere servicio.
-  **Usuario**. Adopte las medidas de recuperación necesarias para resolver el problema.
-  **Soporte**. Si la opción Llamar a casa está habilitada para XClarity Orchestrator o para el Gestor de recursos que gestiona el dispositivo asociado, la alerta normalmente se envía al Centro de Soporte de Lenovo, salvo que ya exista un informe de servicio abierto para el mismo Id. de alerta del dispositivo (consulte [Apertura automática de informes de servicio mediante la función Llamar a casa](#) en la documentación en línea de XClarity Orchestrator). Si la opción Llamar a casa no está habilitada, se recomienda que abra manualmente un informe de servicio para resolver el problema (consulte [Apertura manual de un informe de servicio en el Centro de Soporte de Lenovo](#) en la documentación en línea de XClarity Orchestrator).

Procedimiento

Para ver los sucesos, lleve a cabo uno o más de los pasos siguientes.

- **Ver todos los sucesos de recursos o auditoría** Haga clic en **Supervisión**  → **Sucesos** desde la barra de menú de XClarity Orchestrator para mostrar la tarjeta de Sucesos. A continuación, haga clic en la pestaña **Sucesos de recursos** o **Sucesos de auditoría** para ver las entradas de registro.

Sucesos

El registro de sucesos proporciona un historial de las condiciones de hardware y gestión que se han detectado (sucesos de recursos) y una pista de auditoría de las acciones de usuario (sucesos de auditoría).

Sucesos de recursos **Sucesos de auditoría**

Todas las acciones ▼ Filtros ▼

Fecha y hora	Gravedad	Suceso	Recurso	Capacidad de	Tipo de recur	Grupos
5/10/22 ...	Infor...	No se detec	IO Module :	Ning...	Conmutado	No Disponit
5/10/22 ...	Infor...	Se canceló l	Not Availab	Ning...	No Disponit	No Disponit
5/10/22 ...	Infor...	No se detec	IO Module :	Ning...	Conmutado	No Disponit
5/10/22 ...	Adve...	Se declaró u	Not Availab	Ning...	No Disponit	No Disponit
5/10/22 ...	Infor...	Se canceló l	Not Availab	Ning...	No Disponit	No Disponit
5/10/22 ...	Infor...	Se canceló l	Not Availab	Ning...	No Disponit	No Disponit
5/10/22 ...	Adve...	El estado de	Not Availab	Ning...	No Disponit	No Disponit
5/10/22 ...	Adve...	Se declaró u	Not Availab	Ning...	No Disponit	No Disponit
5/10/22 ...	Infor...	No se detec	IO Module :	Ning...	Conmutado	No Disponit
5/10/22 ...	Adve...	El estado de	Not Availab	Ning...	No Disponit	No Disponit

9396 Total Filas por página: 10 ▼

- **Ver recursos o sucesos de auditoría para un dispositivo específico**

1. Haga clic en **Recursos** (🔍) desde la barra de menú de XClarity Orchestrator y luego haga clic en el tipo de dispositivo para mostrar una tarjeta con una vista de tabla de todos los dispositivos gestionados de ese tipo.
2. Haga clic en la fila de un dispositivo para mostrar las tarjetas de resumen del dispositivo para dicho dispositivo.
3. Haga clic en la pestaña **Registro de sucesos** para mostrar la página Sucesos para ese dispositivo.

Exclusión de alertas y sucesos

Si hay sucesos específicos y alertas activas que no son de su interés, puede excluirlos de todas las páginas y resúmenes en los que se muestran sucesos y alertas. Las alertas y sucesos excluidos siguen en el registro, pero se ocultan en todas las páginas en las que se muestran sucesos y alertas, incluidas las vistas de los registros y el estado del recurso.

Acerca de esta tarea

Los sucesos excluidos están ocultos para todos los usuarios, no solo para el usuario que ha establecido la configuración.

Cuando excluye un suceso que tiene una alerta asociada, dicha alerta también se excluye.

Procedimiento

Lleve a cabo los pasos siguientes para excluir alertas y sucesos.

Paso 1. En la barra de menú de XClarity Orchestrator, haga clic en **Supervisión** (📡) → **Alertas o Supervisión** (📡) → **Sucesos** para mostrar la página Alertas o Sucesos.

Paso 2. Seleccione las alertas o sucesos que se van a excluir y pulse el icono **Excluir** (🗑️). Se muestra el cuadro de diálogo Excluir alertas o Excluir sucesos.

Paso 3. Seleccione una de las opciones siguientes.

- **Excluir sucesos seleccionados de todos los dispositivos.** Excluye los sucesos seleccionados de todos los dispositivos gestionados.
- **Excluir solo sucesos de los dispositivos 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, XClarity Orchestrator crea reglas de exclusión basadas en la información indicada.

- Vea una lista de las reglas de exclusión y las alertas o sucesos excluidos haciendo clic en el icono **Ver exclusiones** (🗑️) para mostrar el cuadro de diálogo alertas excluidas o sucesos excluidos. Haga clic en la pestaña **Reglas de exclusión** para ver las reglas de exclusión, o en la pestaña **Alertas excluidas o Sucesos excluidos** para ver las alertas o los sucesos excluidos.

Sucesos excluidos

Use el botón Quitar para quitar las reglas de exclusión y restaurar los sucesos excluidos en el registro de eventos.

Reglas de exclusión Sucesos excluidos

🔄 🗑️ 📄 Todas las acciones ▼ Filtros ▼ 🔍 Buscar ✕

Suceso	Sistema	ID de suceso
Power supply Power Supply 04 power meter is offli	Todos los sistemas afectados	00038504

0 Seleccionado / 1 Total Filas por página: 10 ▼

Cerrar

- Restablezca los sucesos excluidos en los registros al quitar la regla de exclusión correspondiente. Para quitar una regla de exclusión, haga clic en el icono **Ver exclusiones** (🗑️) para visualizar el cuadro de diálogo Alertas excluidas o Sucesos excluidos, seleccione las reglas de exclusión que desee restaurar y, a continuación, haga clic en el icono **Eliminar** (🗑️).

Reenvío de datos de sucesos, inventario y métricas

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

Acerca de esta tarea

Datos de sucesos

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

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

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

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

Datos de inventario y de sucesos

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

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

Datos de métrica

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

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

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

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

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

Procedimiento

Para reenviar datos, siga estos pasos.

Paso 1. Cree un destino del despachador.

Los *destinos del despachador* son configuraciones comunes que se pueden utilizar en varios despachadores de datos. El destino del despachador identifica dónde deben enviarse los datos para un tipo específico de despachador.

Paso 2. Cree filtros de sucesos y recursos (solo para despachadores de sucesos).

Si lo desea, puede asignar *filtros de despachadores de datos* a varios despachadores de datos. Estos filtros se utilizan para definir criterios específicos a fin de determinar qué sucesos se deben reenviar para qué recursos.

Si no asigna filtros al despachador de datos, todos los sucesos de todos los recursos se reenviarán al destino del despachador seleccionado.

Paso 3. Cree y habilite un despachador de datos.

Puede crear y habilitar despachadores de datos para reenviar datos de sucesos a una aplicación externa específico. Debe elegir un destino del despachador que se aplique al tipo de despachador que está creando.

Creación de filtros de reenvío de datos

Puede definir *filtros de reenvío de datos* comunes que múltiples despachadores pueden utilizar para activar el reenvío de datos que coincidan con criterios específicos.

Acerca de esta tarea

Puede crear los siguientes tipos de filtros.

- Los *filtros de sucesos* reenvían sucesos que coinciden con códigos de sucesos o propiedades específicos (incluidos los códigos de suceso, las clases de suceso, los niveles de gravedad del suceso y los tipos de servicio)
 - Todos los códigos y las propiedades se aplican a todas las fuentes de sucesos.
 - Si no se seleccionan propiedades de clase, se hace coincidir con todas las propiedades de clase.
 - Si no se seleccionan propiedades que se puedan reparar, se hace coincidir con todas las propiedades que se puedan reparar.
 - Si no se seleccionan propiedades de gravedad, se hace coincidir con todas las propiedades de gravedad.
 - Si no se especifica ningún código de suceso, se hace coincidir con todos los códigos de sucesos.
- Los *filtros de recursos* reenvían datos que se generan mediante recursos específicos (XClarity Orchestrator, gestores de recursos y dispositivos). Puede elegir un subconjunto de recursos seleccionando uno o varios grupos de recursos.
 - Si un tipo de recurso está deshabilitado, no se reenvía ningún dato de ese tipo de recurso.
 - Si un tipo de recurso está habilitado y no hay grupos seleccionados, se envían todos los datos de ese tipo de recurso.
 - Si un tipo de recursos está habilitado y se han seleccionado uno o más grupos, solo se reenvían los datos generados por los recursos de los grupos seleccionados.

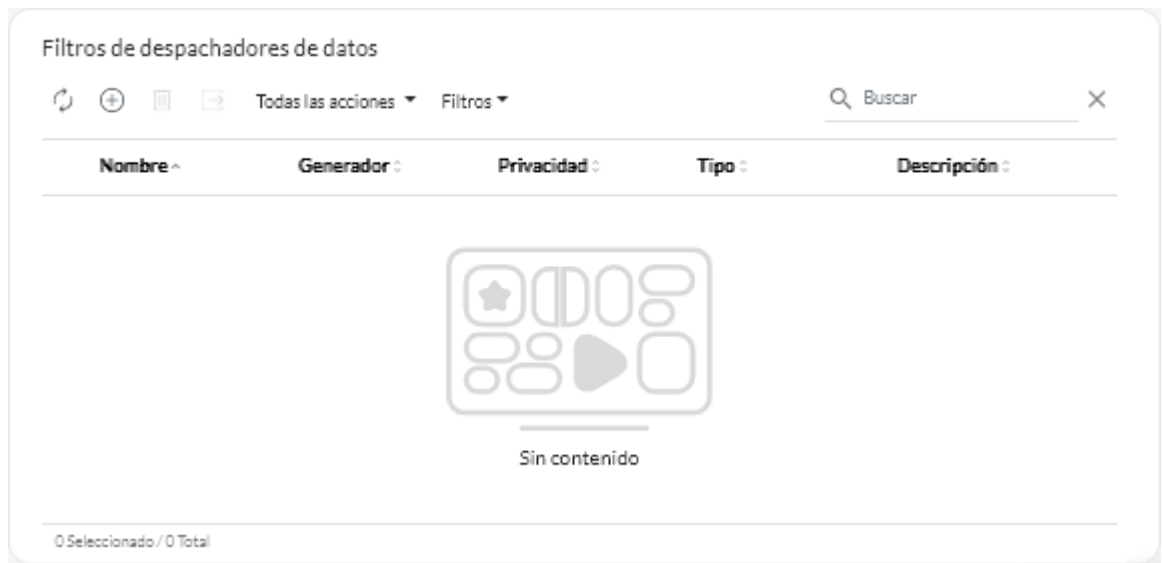
Puede reutilizar los filtros y recursos en varios reenviadores de sucesos; no obstante, puede añadir un filtro de sucesos y un filtro de recursos a cada despachador.

Procedimiento

Para crear un filtro de reenvío de datos, lleve a cabo uno de los pasos siguientes, según el tipo de filtro que desee crear.

- **Filtros de sucesos**

1. En la barra de menús de XClarity Orchestrator, haga clic en **Supervisión** (📺) → **Reenvío** y, a continuación, haga clic en **Filtros de despachadores de datos** en el menú de navegación izquierdo para mostrar la tarjeta de Filtros de despachadores de datos.



2. Haga clic en el icono de **Crear** (+) para mostrar el cuadro de diálogo Crear filtro de despachador de datos.

3. Especifique el nombre del filtro y una descripción opcional.
 4. Seleccione **Filtro de sucesos** como el tipo de filtro.
 5. Seleccione el tipo de privacidad.
 - **Privado.** Solo el usuario que creó el filtro puede utilizar el filtro.
 - **Público.** Cualquier usuario puede utilizar el filtro.
 6. Elija propiedades de sucesos o códigos de sucesos como criterios para este filtro.
 7. Haga clic en **Reglas** y seleccione los criterios para este filtro en función del tipo de criterio que ha seleccionado en el paso anterior.
 - **Hacer coincidir sucesos por propiedades.** Seleccione una o más propiedades de gravedad, capacidad de servicio y clase. Solo se reenvían los sucesos que coinciden con las propiedades seleccionadas. Por ejemplo, si elige la gravedad de advertencias y crítica y las clases de adaptador y memoria, los datos de sucesos se reenvían únicamente para sucesos de memoria de advertencia, sucesos de memoria crítica, sucesos de adaptador de advertencia y sucesos de adaptador crítico, independientemente de la capacidad de servicio del suceso. Si selecciona solo servicio de usuario, los datos de sucesos se reenvían únicamente para los sucesos que puede reparar el usuario, independientemente de la gravedad o la clase.
- Notas:**
- Si no selecciona una propiedad de clase, se hace coincidir con todas las propiedades de clase.
 - Si no selecciona una propiedad que se pueda reparar, se hace coincidir con todas las propiedades que se pueden reparar.
 - Si no selecciona una propiedad de gravedad, se hace coincidir con todas las propiedades de gravedad.
 - **Hacer coincidir sucesos por código.** Introduzca un código de suceso que desee filtrar y haga clic en el icono **Añadir** (+) para añadir el código de suceso a la lista. Repita este paso para cada código de suceso que desee añadir. Puede eliminar un código de suceso pulsando el icono

Eliminar (III) que se encuentra situado junto al código específico. Solo se reenvían los sucesos que coinciden con uno de los códigos de sucesos enumerados.

Puede especificar un código de suceso completo o parcial. Por ejemplo, FQXXOCO0001I coincide con el suceso específico, FQXXOSE coincide con todos los sucesos de seguridad de XClarity Orchestrator y CO001 coincide con todos los sucesos que contienen dichos caracteres.

Si no especifica un código de suceso, se hacen coincidir con todos los códigos de suceso.

Para obtener una lista de los códigos de sucesos disponibles, consulte [Mensajes de sucesos y alertas](#) en la documentación en línea de XClarity Orchestrator.

8. Haga clic en **Crear** para crear el filtro. El filtro se agregará a la tabla.

- **Filtros de recurso**

1. En la barra de menú de XClarity Orchestrator, haga clic en **Supervisión** (☰) → **Reenvío** y, a continuación, haga clic en **Filtros de despachadores de datos** en el menú de navegación izquierdo para mostrar la tarjeta de Filtros de despachadores de datos.
2. Haga clic en el icono de **Crear** (+) para mostrar el cuadro de diálogo Crear filtro de despachador de datos.
3. Especifique el nombre del filtro y una descripción opcional.
4. Seleccione **Filtro de recursos** como el tipo de filtro.
5. Seleccione el tipo de privacidad.
 - **Privado**. Solo el usuario que creó el filtro puede utilizar el filtro.
 - **Público**. Cualquier usuario puede utilizar el filtro.
6. Haga clic en **Recursos** y seleccione el origen de los sucesos para este filtro.
 - **Hacer coincidir cualquier suceso de XClarity Orchestrator**. Reenvía los sucesos generados por este XClarity Orchestrator. Esta opción está deshabilitada de forma predeterminada.
 - **Hacer coincidir cualquier suceso del gestor de recursos**. Reenvía los sucesos generados por un gestor de recursos. Esta opción está deshabilitada de forma predeterminada.
 - Si deshabilita esta opción, los sucesos no se reenvían desde ningún gestor de recursos.
 - Si habilita esta opción pero no selecciona ningún grupo de directores, se reenvían los sucesos generados por todos los administradores de recursos.
 - Si habilita esta opción y selecciona uno o más grupos de gestores, solo los sucesos generados por gestores de recursos en los grupos seleccionados se reenvían.

Consejo: puede crear grupos de gestores desde esta tarjeta haciendo clic en el icono **Crear** (+).

- **Hacer coincidir cualquier suceso de dispositivo**. Reenvía los sucesos generados por un dispositivo. Esta opción está habilitada de forma predeterminada.
 - Si deshabilita esta opción, los sucesos no se reenvían desde ningún dispositivo.
 - Si habilita esta opción pero no selecciona ningún grupo de dispositivos, se reenvían los sucesos generados por todos los dispositivos.
 - Si habilita esta opción y selecciona uno o más grupos de dispositivos, solo los sucesos generados por dispositivos en los grupos seleccionados se reenvían.

Consejo: puede crear grupos de dispositivos desde esta tarjeta haciendo clic en el icono **Crear** (+).

7. Haga clic en **Crear** para crear el filtro. El filtro se agregará a la tabla.

Después de finalizar

Puede realizar la siguiente acción desde la tarjeta Filtros de despachadores de datos.

- Quitar un filtro seleccionado pulsando el icono **Eliminar** (🗑️). No se puede eliminar un filtro que esté asignado a un despachador.

Reenvío de sucesos a SAP Data Intelligence

Puede configurar Lenovo XClarity Orchestrator para que despache sucesos a SAP Data Intelligence (Intelligent Insights).

Antes de empezar

Atención: La conexión entre XClarity Orchestrator y SAP Data Intelligence utiliza un transporte cifrado, pero no verifica el certificado TLS del sistema remoto.

Acerca de esta tarea

Si el control de acceso basado en recursos está habilitado, los datos se reenvían solo para aquellos recursos a los que puede acceder mediante listas de control de acceso. Si no es miembro de un grupo al que se ha asignado el rol de **Supervisor** predefinido, debe asignar una o varias listas de control de acceso a los despachadores que cree. Si desea enviar datos para todos los recursos a los que puede acceder, seleccione todas las listas de control de acceso que están asociadas a su disposición. Si es miembro de un grupo al que se ha asignado el rol de **Supervisor** predefinido, puede elegir enviar los datos para todos los recursos o puede asignar listas de control de acceso para limitar los recursos.

No puede filtrar los datos que se reenvían a SAP Data Intelligence.

En el siguiente ejemplo se muestra el formato predeterminado para datos que se reenvían a SAP Data Intelligence. Las palabras entre corchetes dobles son los atributos que se sustituyen con los valores reales cuando se reenvían datos.

```
{\"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]]\", \"failFRUUIDs\": \"[[EventFailFRUUIDs]]\", \"eventClass\": \"[[EventClassNumber]]\", \"componentID\": \"[[EventComponentUUID]]\", \"mtm\": \"[[EventMachineTypeModel]]\", \"msgID\": \"[[EventMessageID]]\", \"sequenceNumber\": \"[[EventSequenceID]]\", \"timestamp\": \"[[EventTimeStamp]]\", \"args\": \"[[EventMessageArguments]]\", \"service\": \"[[EventServiceNumber]]\", \"commonEventID\": \"[[CommonEventID]]\", \"eventDate\": \"[[EventDate]]\"}
```

Procedimiento

Para reenviar datos de suceso a SAP Data Intelligence, lleve a cabo los pasos siguientes.

- Paso 1. En la barra de menú de XClarity Orchestrator, haga clic en **Supervisión** (👤) → **Reenvío** y, luego haga clic en **Despachadores de datos** en el menú de navegación izquierdo para mostrar la tarjeta Despachadores de datos.
- Paso 2. Haga clic en el icono de **Crear** (+) para mostrar el cuadro de diálogo Crear despachador de datos.
- Paso 3. Especifique el nombre del despachador y una descripción opcional.
- Paso 4. Elija habilitar o deshabilitar el despachador haciendo clic en el icono de alternación de **Estado**.
- Paso 5. Seleccione **Intelligent Insights** como el tipo de despachador.
- Paso 6. Haga clic en **Configuración** y llene la información específica del protocolo.

- Ingrese el nombre de host o dirección IP de SAP Data Intelligence.
- Especifique el puerto que se usará para reenviar sucesos. El valor predeterminado es 443.
- Ingrese la ruta de acceso de recursos en el que el reenviador publicará los sucesos (por ejemplo, /rest/test).
- Seleccione el método REST. Puede presentar uno de los valores siguientes.
 - **PUT**
 - **POST**
- Seleccione el protocolo que se utilizará para reenviar sucesos. Puede presentar uno de los valores siguientes.
 - **HTTP**
 - **HTTPS**
- Especifique el período de desconexión (en segundos) para la solicitud. El valor predeterminado es 30 segundos.
- Si se requiere autenticación, seleccione uno de los siguientes tipos de autenticación.
 - **Básico**. Se autentica en el servidor especificado usando el inquilino, el Id. de usuario y la contraseña especificados.
 - **Token**. Se autentica en el servidor especificado usando el nombre de encabezado de token y valor.

Paso 7. Haga clic en **Listas de control de acceso** y seleccione una o varias listas de control de acceso que desee asociar con este despachador.

Si el acceso basado con recursos está habilitado, debe seleccionar al menos una lista de control de acceso.

Consejo: De manera opcional, los usuarios que son miembros de un equipo al que se ha asignado el rol de **Supervisor** predefinido, pueden seleccionar **Hacer coincidir todo** en lugar de seleccionar una lista de control de acceso de forma que los datos reenviados no se restrinjan.

Paso 8. Haga clic en **Crear** para crear el despachador.

Después de finalizar

Puede realizar las siguientes acciones desde la tarjeta Despachadores de datos.

- Habilite o deshabilite un despachador seleccionado seleccionando el conmutador de la columna **Estado**.
- Modifique un despachador seleccionado haciendo clic en el icono **Editar** (✎).
- Elimine un despachador seleccionado haciendo clic en el icono **Eliminar** (🗑).

Reenvío de sucesos a un servicio web REST

Puede configurar Lenovo XClarity Orchestrator para que reenvíe sucesos específicos a un servidor web REST.

Antes de empezar

Atención: No se establece una conexión segura al reenviar datos a este servicio. Los datos se envían a través de un protocolo no cifrado.

Acerca de esta tarea

Si el control de acceso basado en recursos está habilitado, los datos se reenvían solo para aquellos recursos a los que puede acceder mediante listas de control de acceso. Si no es miembro de un grupo al que se ha

asignado el rol de **Supervisor** predefinido, debe asignar una o varias listas de control de acceso a los despachadores que cree. Si desea enviar datos para todos los recursos a los que puede acceder, seleccione todas las listas de control de acceso que están asociadas a su disposición. Si es miembro de un grupo al que se ha asignado el rol de **Supervisor** predefinido, puede elegir enviar los datos para todos los recursos o puede asignar listas de control de acceso para limitar los recursos.

Los *filtros de reenvío de datos* comunes se utilizan para definir el alcance de los sucesos que desea reenviar, según los códigos de suceso, las clases de suceso, los niveles de gravedad del suceso, los tipos de servicio y el recurso que generó el suceso. Asegúrese de que los filtros de suceso y recurso que desee utilizar para este despachador ya se hayan creado (consulte [Creación de filtros de reenvío de datos](#)).

En el siguiente ejemplo se muestra el formato predeterminado para los datos que se reenvían a un servicio web REST. Las palabras entre corchetes dobles son los atributos que se sustituyen con los valores reales cuando se reenvían datos.

```
{\ "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]]\ "}
```

Procedimiento

Para reenviar datos a un servicio web REST, lleve a cabo los pasos siguientes.

- Paso 1. En la barra de menú de XClarity Orchestrator, haga clic en **Supervisión** (📧) → **Reenvío** y, luego haga clic en **Despachadores de datos** en el menú de navegación izquierdo para mostrar la tarjeta Despachadores de datos.
- Paso 2. Haga clic en el icono de **Crear** (⊕) para mostrar el cuadro de diálogo Crear despachador de datos.
- Paso 3. Especifique el nombre del despachador y una descripción opcional.
- Paso 4. Elija habilitar o deshabilitar el despachador haciendo clic en el icono de alternación de **Estado**.
- Paso 5. Seleccione **REST** como el tipo de despachador.
- Paso 6. Haga clic en **Configuración** y llene la información específica del protocolo.
 - Ingrese el nombre de host o dirección IP del servidor REST.
 - Especifique el puerto que se usará para reenviar sucesos. El valor predeterminado es 80.
 - Ingrese la ruta de acceso de recursos en el que el reenviador publicará los sucesos (por ejemplo, /rest/test).
 - Seleccione el método REST. Puede presentar uno de los valores siguientes.
 - **PUT**
 - **POST**
 - Seleccione el protocolo que se utilizará para reenviar sucesos. Puede presentar uno de los valores siguientes.
 - **HTTP**
 - **HTTPS**
 - Especifique el período de desconexión (en segundos) para la solicitud. El valor predeterminado es 30 segundos.

- 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.
 - **Token.** Se autentica en el servidor especificado usando el nombre de encabezado de token y valor.

Paso 7. Haga clic en **Filtros** y, opcionalmente, seleccione los filtros que desea utilizar para este despachador.

Puede seleccionar como máximo un filtro de sucesos y un filtro de recursos.

Si no selecciona un filtro, los datos se despachan para todos los sucesos generados por todos los recursos (dispositivos, gestores de recursos y XClarity Orchestrator).

En esta pestaña, también puede elegir reenviar sucesos excluidos configurando el alternador **Sucesos excluidos** en **Sí**.

Paso 8. Haga clic en **Listas de control de acceso** y seleccione una o varias listas de control de acceso que desee asociar con este despachador.

Si el acceso basado con recursos está habilitado, debe seleccionar al menos una lista de control de acceso.

Consejo: De manera opcional, los usuarios que son miembros de un equipo al que se ha asignado el rol de **Supervisor** predefinido, pueden seleccionar **Hacer coincidir todo** en lugar de seleccionar una lista de control de acceso de forma que los datos reenviados no se restrinjan.

Paso 9. Haga clic en **Crear** para crear el despachador.

Después de finalizar

Puede realizar las siguientes acciones desde la tarjeta Despachadores de datos.

- Habilite o deshabilite un despachador seleccionado seleccionando el conmutador de la columna **Estado**.
- Modifique un despachador seleccionado haciendo clic en el icono **Editar** (✎).
- Elimine un despachador seleccionado haciendo clic en el icono **Eliminar** (🗑).

Reenvío de sucesos a un servicio de correo electrónico mediante SMTP

Puede configurar Lenovo XClarity Orchestrator para reenviar sucesos específicos a una o más direcciones de correo electrónico mediante SMTP.

Antes de empezar

Atención: No se establece una conexión segura al reenviar datos a este servicio. Los datos se envían a través de un protocolo no cifrado.

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 [Reenvío de sucesos a un servicio SMTP de Gmail](#).

Acerca de esta tarea

Si el control de acceso basado en recursos está habilitado, los datos se reenvían solo para aquellos recursos a los que puede acceder mediante listas de control de acceso. Si no es miembro de un grupo al que se ha asignado el rol de **Supervisor** predefinido, debe asignar una o varias listas de control de acceso a los despachadores que cree. Si desea enviar datos para todos los recursos a los que puede acceder, seleccione todas las listas de control de acceso que están asociadas a su disposición. Si es miembro de un grupo al que se ha asignado el rol de **Supervisor** predefinido, puede elegir enviar los datos para todos los recursos o puede asignar listas de control de acceso para limitar los recursos.

Los *filtros de reenvío de datos* comunes se utilizan para definir el alcance de los sucesos que desea reenviar, según los códigos de suceso, las clases de suceso, los niveles de gravedad del suceso, los tipos de servicio y el recurso que generó el suceso. Asegúrese de que los filtros de suceso y recurso que desee utilizar para este despachador ya se hayan creado (consulte [Creación de filtros de reenvío de datos](#)).

En el siguiente ejemplo se muestra el formato predeterminado para los datos que se reenvían a un servicio de correo electrónico. Las palabras entre corchetes dobles son los atributos que se sustituyen con los valores reales cuando se reenvían datos.

Asunto de correo electrónico

Event Forwarding

Cuerpo de correo electrónico

```
{
  "groups": [],
  "acls": [],
  "local": null,
  "eventID": "FQXHMEMO216I",
  "severity": "Warning",
  "sourceID": "FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF",
  "componentID": "FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF",
  "msg": "The event forwarder destination cannot be reached. Therefore new events are not being forwarded.",
  "description": "The event forwarder destination cannot be reached. Therefore new events are not being forwarded.",
  "userAction": "Look in the online documentation to determinate more information about this event based on the eventID. At the moment the orchestrator server can not offer more information.",
  "recoveryURL": null,
  "flags": [],
  "userid": null,
  "action": "None",
  "eventClass": "System",
  "args": [],
  "service": "None",
  "lxcaUUID": "23C87F0A2CB6491097489193447A655C",
  "managerID": "23C87F0A2CB6491097489193447A655C",
  "failFRUNumbers": null,
  "failFRUSNs": null,
  "failFRUUUIDs": "[FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF]",
  "msgID": null,
  "timeStamp": "2021-03-12T18:32:14.000Z",
  "eventDate": "2021-03-12T18:32:14Z",
  "commonEventID": "FQXHMEMO216I",
  "sequenceNumber": "17934247",
  "details": null,
  "device": {
    "name": "xhmc194.labs.lenovo.com",
    "mtm": null,
    "serialNumber": null
  }
},
```

```

"resourceType": "XClarity Administrator",
"componentType": "XClarity Administrator",
"sourceType": "Management",
"resourceName": "xhmc194.labs.lenovo.com",
"fruType": "other",
"ipAddress": "10.243.2.107",
"_id": 252349
}

```

Procedimiento

Para reenviar datos a un servicio de correo electrónico mediante SMTP, lleve a cabo los pasos siguientes.

- Paso 1. En la barra de menú de XClarity Orchestrator, haga clic en **Supervisión** (📊) → **Reenvío** y, luego haga clic en **Despachadores de datos** en el menú de navegación izquierdo para mostrar la tarjeta Despachadores de datos.
- Paso 2. Haga clic en el icono de **Crear** (+) para mostrar el cuadro de diálogo Crear despachador de datos.
- Paso 3. Especifique el nombre del despachador y una descripción opcional.
- Paso 4. Elija habilitar o deshabilitar el despachador haciendo clic en el icono de alternación de **Estado**.
- Paso 5. Seleccione **Correo electrónico** como el tipo de despachador.
- Paso 6. Haga clic en **Configuración** y llene la información específica del protocolo.

- Ingrese el nombre de host o dirección IP del servidor SMTP.
- 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.
- **Opcional:** ingrese la dirección de correo electrónico del remitente del correo electrónico (por ejemplo, john@company.com) y el dominio del remitente. Si no especifica una dirección de correo electrónico, la dirección del remitente es `LXCO.<source_identifier>@<smtp_host>` de manera predeterminada.

Si especifica solo el dominio del remitente, el formato de la dirección del remitente es `<LXCO_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 un correo electrónico y no configura un nombre de host para XClarity Orchestrator, es posible que el servidor SMTP rechace los sucesos reenviados. Si XClarity Orchestrator 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 (`LXCO.<source_identifier>@<smtp_host>`). En este caso, debe especificar al menos un nombre de dominio en el campo **Usuario remitente**.
- Para establecer una conexión segura al servidor SMTP, seleccione uno de los tipos de conexión siguientes.

- **SSL.** Utiliza el protocolo SSL para crear una comunicación segura.
- **STARTTLS.** Utiliza el protocolo TLS para formar una comunicación segura en un canal no seguro.

Si se selecciona uno de estos tipos de conexión, XClarity Orchestrator intenta descargar e importar el certificado de servidor SMTP a su almacén de confianza de XClarity Orchestrator. Se le pedirá que acepte este certificado.

- 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.
 - **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 especificados. 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 7. Haga clic en **Filtros** y, opcionalmente, seleccione los filtros que desea utilizar para este despachador.

Puede seleccionar como máximo un filtro de sucesos y un filtro de recursos.

Si no selecciona un filtro, los datos se despachan para todos los sucesos generados por todos los recursos (dispositivos, gestores de recursos y XClarity Orchestrator).

En esta pestaña, también puede elegir reenviar sucesos excluidos configurando el alternador **Sucesos excluidos** en **Sí**.

Paso 8. Haga clic en **Listas de control de acceso** y seleccione una o varias listas de control de acceso que desee asociar con este despachador.

Si el acceso basado con recursos está habilitado, debe seleccionar al menos una lista de control de acceso.

Consejo: De manera opcional, los usuarios que son miembros de un equipo al que se ha asignado el rol de **Supervisor** predefinido, pueden seleccionar **Hacer coincidir todo** en lugar de seleccionar una lista de control de acceso de forma que los datos reenviados no se restrinjan.

Paso 9. Haga clic en **Crear** para crear el despachador.

Después de finalizar

Puede realizar las siguientes acciones desde la tarjeta Despachadores de datos.

- Habilite o deshabilite un despachador seleccionado seleccionando el conmutador de la columna **Estado**.
- Modifique un despachador seleccionado haciendo clic en el icono **Editar** (✎).
- Elimine un despachador seleccionado haciendo clic en el icono **Eliminar** (🗑).

Reenvío de sucesos a un servicio SMTP de Gmail

Puede configurar Lenovo XClarity Orchestrator para reenviar sucesos 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”. Haga clic en **GMAIL API** en los resultados de búsqueda.
 - e. Haga clic en **Habilitar**.
 - f. Haga clic en la pestaña **Credenciales**.
 - g. Haga clic en la **pantalla de consentimiento de OAuth**.
 - h. Escriba un nombre en el campo de **Nombre de producto que se muestra a los usuarios** y haga clic en **Guardar**.
 - i. Haga clic en **Crear credenciales → Id. de cliente de OAuth**.
 - j. Seleccione **Otro** e introduzca un nombre.
 - k. Haga clic en **Crear**. Se muestra el cuadro de diálogo Cliente de OAuth con su Id. de cliente y secreto del cliente.
 - l. Registre el Id. de cliente y el secreto del cliente para utilizarlo en el futuro.
 - m. 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=3tnyXgEiBIbT2m00zqnlTszk --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&redirect_uri=
urn%3Aietf%3Awg%3Aoauth%3A2.0%3Aaob&response_type=code&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/K8lPGx6UQQajj7tQGyKq8mVG8LVvGIVzHqzxFIMEYEQMEudVrK5jSpoR30zcrFq6
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 Orchestrator con el nuevo token.

3. En la interfaz web de Lenovo XClarity Orchestrator, 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)

Reenvío de inventario y sucesos a Splunk

Puede configurar Lenovo XClarity Orchestrator para reenviar inventarios y sucesos en un formato predefinido a una aplicación Splunk. A continuación, puede utilizar Splunk para crear gráficos y tablas basándose en esos datos para analizar las condiciones y predecir los problemas en su entorno.

Antes de empezar

Atención: No se establece una conexión segura al reenviar datos a este servicio. Los datos se envían a través de un protocolo no cifrado.

Acerca de esta tarea

Splunk es una herramienta para operadores de centros de datos para realizar un seguimiento y analizar los registros de sucesos y otros datos. Lenovo proporciona una aplicación de XClarity Orchestrator para Splunk que analiza los sucesos reenviados por XClarity Orchestrator y presenta el análisis en un conjunto de paneles. Puede supervisar los paneles de esta aplicación como una ayuda para detectar posibles problemas en su entorno, de modo que pueda reaccionar antes de que ocurran problemas graves. Para obtener más información, consulte la [Guía del usuario de la aplicación XClarity Orchestrator para Splunk](#) en la documentación en línea de XClarity Orchestrator.



Puede definir múltiples configuraciones de Splunk; sin embargo, XClarity Orchestrator puede reenviar sucesos solo a una instancia de Splunk. Por lo tanto, solo se puede habilitar una configuración de Splunk a la vez.

Si el control de acceso basado en recursos está habilitado, los datos se reenvían solo para aquellos recursos a los que puede acceder mediante listas de control de acceso. Si no es miembro de un grupo al que se ha asignado el rol de **Supervisor** predefinido, debe asignar una o varias listas de control de acceso a los despachadores que cree. Si desea enviar datos para todos los recursos a los que puede acceder, seleccione todas las listas de control de acceso que están asociadas a su disposición. Si es miembro de un grupo al que se ha asignado el rol de **Supervisor** predefinido, puede elegir enviar los datos para todos los recursos o puede asignar listas de control de acceso para limitar los recursos.

No pueden filtrar datos que se reenvían a aplicaciones Splunk.

Procedimiento

Para reenviar datos de inventario y de suceso a una aplicación Splunk, lleve a cabo los pasos siguientes.

- Paso 1. En la barra de menú de XClarity Orchestrator, haga clic en **Supervisión**  → **Reenvío** y, luego haga clic en **Despachadores de datos** en el menú de navegación izquierdo para mostrar la tarjeta Despachadores de datos.
- Paso 2. Haga clic en el icono de **Crear**  para mostrar el cuadro de diálogo Crear despachador de datos.
- Paso 3. Especifique el nombre del despachador y una descripción opcional.
- Paso 4. Elija habilitar o deshabilitar el despachador haciendo clic en el icono de alternación de **Estado**.
- Paso 5. Seleccione **Splunk** como el tipo de despachador.
- Paso 6. Haga clic en **Configuración** y llene la información específica del protocolo.
 - Ingrese el nombre de host o dirección IP de la aplicación Splunk.
 - Especifique la cuenta de usuario y contraseña que utilizará para iniciar sesión en el servicio Splunk.
 - Especifique la API REST y los números de puerto de datos que se utilizarán para conectarse al servicio Splunk.
 - Especifique uno o más índices del recopilador de sucesos HTTP. El índice predeterminado es **lxco**.
 - Especifique el período de desconexión (en segundos) para la solicitud. El valor predeterminado es 30 segundos.
- Paso 7. Haga clic en **Listas de control de acceso** y seleccione una o varias listas de control de acceso que desee asociar con este despachador.



Si el acceso basado con recursos está habilitado, debe seleccionar al menos una lista de control de acceso.

Consejo: De manera opcional, los usuarios que son miembros de un equipo al que se ha asignado el rol de **Supervisor** predefinido, pueden seleccionar **Hacer coincidir todo** en lugar de seleccionar una lista de control de acceso de forma que los datos reenviados no se restrinjan.

- Paso 8. Haga clic en **Crear** para crear el despachador.

Después de finalizar

Puede realizar las siguientes acciones desde la tarjeta Despachadores de datos.

- Habilite o deshabilite un despachador seleccionado seleccionando el conmutador de la columna **Estado**.
- Modifique un despachador seleccionado haciendo clic en el icono **Editar** .
- Elimine un despachador seleccionado haciendo clic en el icono **Eliminar** .

Reenvío de sucesos a un syslog

Puede configurar Lenovo XClarity Orchestrator para que reenvíe sucesos específicos a un syslog.

Antes de empezar

Atención: No se establece una conexión segura al reenviar datos a este servicio. Los datos se envían a través de un protocolo no cifrado.

Acerca de esta tarea

Si el control de acceso basado en recursos está habilitado, los datos se reenvían solo para aquellos recursos a los que puede acceder mediante listas de control de acceso. Si no es miembro de un grupo al que se ha asignado el rol de **Supervisor** predefinido, debe asignar una o varias listas de control de acceso a los despachadores que cree. Si desea enviar datos para todos los recursos a los que puede acceder, seleccione todas las listas de control de acceso que están asociadas a su disposición. Si es miembro de un grupo al que se ha asignado el rol de **Supervisor** predefinido, puede elegir enviar los datos para todos los recursos o puede asignar listas de control de acceso para limitar los recursos.

Los *filtros de reenvío de datos* comunes se utilizan para definir el alcance de los sucesos que desea reenviar, según los códigos de suceso, las clases de suceso, los niveles de gravedad del suceso, los tipos de servicio y el recurso que generó el suceso. Asegúrese de que los filtros de suceso y recurso que desee utilizar para este despachador ya se hayan creado (consulte [Creación de filtros de reenvío de datos](#)).

En el siguiente ejemplo se muestra el formato predeterminado para datos que se reenvían a un syslog. Las palabras entre corchetes dobles son los atributos que se sustituyen con los valores reales cuando se reenvían datos.

```
{
  "appl": "LXCO",
  "groups": [],
  "acls": [],
  "local": null,
  "eventID": "FQXMEM0216I",
  "severity": "Warning",
  "sourceID": "FFFFFFFFFFFFFFFFFFFFFFFFFFFF",
  "componentID": "FFFFFFFFFFFFFFFFFFFFFFFFFFFF",
  "msg": "The event forwarder destination cannot be reached. Therefore new events are not being
        forwarded.",
  "description": "The event forwarder destination cannot be reached. Therefore new events are not
                 being forwarded.",
  "userAction": "Look in the online documentation to determinate more information about this event
                based on the eventID. At the moment the orchestrator server can not offer more
                information.",
  "recoveryURL": null,
  "flags": [],
  "userid": null,
  "action": "None",
  "eventClass": "System",
  "args": [],
  "service": "None",
  "lxcaUUID": "23C87FOA2CB6491097489193447A655C",
  "managerID": "23C87FOA2CB6491097489193447A655C",
  "failFRUNumbers": null,
  "failFRUSNs": null,
  "failFRUUUIDs": "[FFFFFFFFFFFFFFFFFFFFFFFFFFFF]",
  "msgID": null,
  "timeStamp": "2021-03-12T18:32:14.000Z",
  "eventDate": "2021-03-12T18:32:14Z",
  "commonEventID": "FQXMEM0216I",
  "sequenceNumber": "17934247",
  "details": null,
  "device": {
    "name": "xhmc194.labs.lenovo.com",
    "mtm": null,
    "serialNumber": null
  },
  "resourceType": "XClarity Administrator",
  "componentType": "XClarity Administrator",
  "sourceType": "Management",
  "resourceName": "xhmc194.labs.lenovo.com",
}
```

```
"fruType": "other",
"ipAddress": "10.243.2.107",
"_id": 252349
}
```

Procedimiento

Para reenviar datos a un syslog, lleve a cabo los pasos siguientes.

- Paso 1. En la barra de menú de XClarity Orchestrator, haga clic en **Supervisión** (📧) → **Reenvío** y, luego haga clic en **Despachadores de datos** en el menú de navegación izquierdo para mostrar la tarjeta Despachadores de datos.
- Paso 2. Haga clic en el icono de **Crear** (+) para mostrar el cuadro de diálogo Crear despachador de datos.
- Paso 3. Especifique el nombre del despachador y una descripción opcional.
- Paso 4. Elija habilitar o deshabilitar el despachador haciendo clic en el icono de alternación de **Estado**.
- Paso 5. Seleccione **Syslog** como el tipo de despachador.
- Paso 6. Haga clic en **Configuración** y llene la información específica del protocolo.
 - Ingrese el nombre de host o dirección IP del syslog.
 - 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.
 - **Opcional:** 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 7. Haga clic en **Filtros** y, opcionalmente, seleccione los filtros que desea utilizar para este despachador.

Puede seleccionar como máximo un filtro de sucesos y un filtro de recursos.

Si no selecciona un filtro, los datos se despachan para todos los sucesos generados por todos los recursos (dispositivos, gestores de recursos y XClarity Orchestrator).

En esta pestaña, también puede elegir reenviar sucesos excluidos configurando el alternador **Sucesos excluidos** en **Sí**.

- Paso 8. Haga clic en **Listas de control de acceso** y seleccione una o varias listas de control de acceso que desee asociar con este despachador.

Si el acceso basado con recursos está habilitado, debe seleccionar al menos una lista de control de acceso.

Consejo: De manera opcional, los usuarios que son miembros de un equipo al que se ha asignado el rol de **Supervisor** predefinido, pueden seleccionar **Hacer coincidir todo** en lugar de seleccionar una lista de control de acceso de forma que los datos reenviados no se restrinjan.

- Paso 9. Haga clic en **Crear** para crear el despachador.

Después de finalizar

Puede realizar las siguientes acciones desde la tarjeta Despachadores de datos.

- Habilite o deshabilite un despachador seleccionado seleccionando el conmutador de la columna **Estado**.
- Modifique un despachador seleccionado haciendo clic en el icono **Editar** (✎).
- Elimine un despachador seleccionado haciendo clic en el icono **Eliminar** (🗑).

Reenvío de datos de métricas a Sitio web de Lenovo TruScale Infrastructure Services

Puede configurar Lenovo XClarity Orchestrator para que reenvíe datos de métricas (telemetría) a un archivo Sitio web de Lenovo TruScale Infrastructure Services.

Antes de empezar

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

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

Se establece una conexión segura al reenviar datos a TruScale Infrastructure Services.

Asegúrese de que XClarity Orchestrator esté ejecutando la versión 1.2.0 o posterior.

Asegúrese de que los gestores de recursos de Lenovo XClarity Administrator que gestionan los dispositivos para los que desea reenviar datos de las mediciones estén ejecutando la versión 3.0.0, más el paquete de revisión o una versión posterior.

Asegúrese de que los gestores de recursos de XClarity Administrator adecuados estén conectados con XClarity Orchestrator (consulte [Conexión de gestores de recursos](#)).

Asegúrese de que los dispositivos para los que desea reenviar datos de métricas estén ejecutando el firmware de Lenovo XClarity Controller más reciente (consulte [Aplicar y activar actualizaciones a los gestores de recursos](#)).

Asegúrese de que los valores de datos y hora se configuren correctamente en los recursos siguientes.

- XClarity Orchestrator (consulte [Configuración de fecha y hora](#))
- Gestor de recursos XClarity Administrator (consulte [Establecimiento de la fecha y la hora](#) en la documentación en línea de XClarity Administrator)
- Controladores de gestión de la placa base en cada dispositivo (consulte [Establecimiento de fecha y hora de XClarity Controller](#) en la documentación en línea de Lenovo XClarity Controller)

Asegúrese de que los valores de red en XClarity Orchestrator estén configurados correctamente.

Asegúrese de que se estén recopilando datos de las mediciones para los dispositivos gestionados consultando los gráficos de utilización en la página de resumen de dispositivos (consulte [Visualización de los detalles del dispositivo](#)). Si no se muestran los datos de las métricas, consulte [Resolución de problemas de reenvío de datos](#).

Para obtener más información sobre Sitio web de Lenovo TruScale Infrastructure Services, consulte el [Sitio web de TruScale Infrastructure Services](#).

Acerca de esta tarea

Puede definir múltiples configuraciones de Sitio web de Lenovo TruScale Infrastructure Services; sin embargo, XClarity Orchestrator puede reenviar sucesos solo a una instancia de Sitio web de Lenovo TruScale Infrastructure Services. Por lo tanto, solo se puede habilitar una configuración de Sitio web de Lenovo TruScale Infrastructure Services a la vez.

Si el control de acceso basado en recursos está habilitado, los datos se reenvían solo para aquellos recursos a los que puede acceder mediante listas de control de acceso. Si no es miembro de un grupo al que se ha asignado el rol de **Supervisor** predefinido, debe asignar una o varias listas de control de acceso a los despachadores que cree. Si desea enviar datos para todos los recursos a los que puede acceder, seleccione todas las listas de control de acceso que están asociadas a su disposición. Si es miembro de un grupo al que se ha asignado el rol de **Supervisor** predefinido, puede elegir enviar los datos para todos los recursos o puede asignar listas de control de acceso para limitar los recursos.

No puede filtrar datos que se reenvían a un Sitio web de Lenovo TruScale Infrastructure Services.

En el siguiente ejemplo se muestra el formato predeterminado para datos que se reenvían a un Sitio web de Lenovo TruScale Infrastructure Services. Las palabras entre corchetes dobles son los atributos que se sustituyen con los valores reales cuando se reenvían datos.

```
{\"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]]\"}
```

Procedimiento

Para reenviar datos a un Sitio web de Lenovo TruScale Infrastructure Services, lleve a cabo los pasos siguientes.

Paso 1. Añada los certificados SSL de confianza que proporciona el archivo Sitio web de Lenovo TruScale Infrastructure Services.

1. En la barra de menú de XClarity Orchestrator, haga clic en la barra de menú de XClarity Orchestrator, haga clic en **Administración** (⚙️) → **Seguridad** y luego haga clic en **Certificados de confianza** en el panel de navegación izquierdo para mostrar la tarjeta de Certificados de confianza.
2. Haga clic en el icono de **Agregar** (+) para agregar un certificado. Se muestra el cuadro de diálogo Agregar certificado.
3. Copie y pegue los datos de certificado en formato PEM.
4. Haga clic en **Añadir**.

Paso 2. En la barra de menú de XClarity Orchestrator, haga clic en **Supervisión** (👁️) → **Reenvío** y, luego haga clic en **Despachadores de datos** en el menú de navegación izquierdo para mostrar la tarjeta Despachadores de datos.

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

Paso 4. Especifique el nombre del despachador y una descripción opcional.

Paso 5. Elija habilitar o deshabilitar el despachador haciendo clic en el icono de alternación de **Estado**.

Paso 6. Seleccione **TruScale Infrastructure Services** como el tipo de despachador.

Paso 7. Haga clic en **Configuración** y llene la información específica del protocolo.

- Ingrese el nombre de host o dirección IP de TruScale Infrastructure Service.
- Especifique el puerto que se usará para reenviar sucesos. El valor predeterminado es 9092.
- Opcionalmente, introduzca la frecuencia, en minutos, en la que se insertan los datos. El valor predeterminado es 60 minutos.
- Especifique el nombre del asunto.
- Especifique el período de desconexión (en segundos) para la solicitud. El valor predeterminado es 300 segundos.

Paso 8. Haga clic en **Validar conexión** para asegurarse de que se puede establecer una conexión en función de la configuración.

Atención: La validación de la conexión puede tardar varios minutos en finalizar. Puede cerrar el mensaje emergente y continuar creando el de reenvío sin interrumpir el proceso de validación. Una vez finalizada la validación, aparece otro mensaje emergente para notificarle si la conexión se ha realizado correctamente.

Paso 9. Haga clic en **Listas de control de acceso** y seleccione una o varias listas de control de acceso que desee asociar con este despachador.

Si el acceso basado con recursos está habilitado, debe seleccionar al menos una lista de control de acceso.

Consejo: De manera opcional, los usuarios que son miembros de un equipo al que se ha asignado el rol de **Supervisor** predefinido, pueden seleccionar **Hacer coincidir todo** en lugar de seleccionar una lista de control de acceso de forma que los datos reenviados no se restrinjan.

Paso 10. Haga clic en **Crear** para crear el despachador.

Después de finalizar

Puede realizar las siguientes acciones desde la tarjeta Despachadores de datos.

- Habilite o deshabilite un despachador seleccionado seleccionando el conmutador de la columna **Estado**.
- Modifique un despachador seleccionado haciendo clic en el icono **Editar** (✎).
- Elimine un despachador seleccionado haciendo clic en el icono **Eliminar** (🗑).

Reenvío de informes

Puede reenviar informes periódicamente a una o varias direcciones de correo electrónico utilizando un servicio web SMTP.

Acerca de esta tarea

Un *informe* es cualquier datos que se presenta en forma de tabla en la interfaz de usuario. Actualmente, los siguientes informes son compatibles.


- Alertas activas
- Sucesos de recursos y auditorías
- Dispositivos gestionados (servidores, almacenamiento, conmutadores y chasis).
- Cumplimiento del firmware del dispositivo
- Cumplimiento de configuración del servidor
- Estado de la garantía de los servidores
- Activar informes de servicio


Creación de configuraciones de destino del despachador

Puede definir configuraciones comunes de destino que pueden ser utilizadas por varios despachadores de informes. El destino identifica dónde deben enviarse los informes.

Procedimiento

Para crear una configuración de destino para los despachadores de informes, realice los pasos siguientes.

Paso 1. En la barra de menú de XClarity Orchestrator, haga clic en **Supervisión**  → **Reenvío** y, luego haga clic en **Destinos del despachador** en el menú de navegación izquierdo para mostrar la tarjeta Destinos del despachador.

Paso 2. Haga clic en el icono de **Crear**  para mostrar el cuadro de diálogo Crear destinos del despachador.

Paso 3. Especifique el nombre del despachador de informes y una descripción opcional

Paso 4. Seleccione **SMTP** como el tipo de destino.

Paso 5. Haga clic en **Configuración** y llene la información específica del protocolo.

- Ingrese el nombre de host o dirección IP del servidor SMTP (correo electrónico).
- Especifique el puerto que se usará para el destino. 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.
- **Opcional:** ingrese la dirección de correo electrónico del remitente del correo electrónico (por ejemplo, john@company.com) y el dominio del remitente. Si no especifica una dirección de correo electrónico, la dirección del remitente es `LXCO.{source_identifier}@{smtp_host}` de manera predeterminada.

Si especifica únicamente el dominio del remitente, el formato de la dirección del remitente es `{LXCO_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 un correo electrónico y no configura un nombre de host para XClarity Orchestrator, es posible que el servidor SMTP rechace el correo electrónico. Si XClarity Orchestrator no dispone de un nombre de host, el correo electrónico 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 correo electrónico.
- Si especifica el dominio del remitente, el origen no se identifica en la dirección del remitente. Por el contrario, la información sobre el origen de los datos se incluye en el cuerpo del correo electrónico, incluido el nombre del sistema, la dirección IP, el tipo o modelo de máquina 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 (`LXCO.<source_identifier>@{smtp_host}>`). En este caso, debe especificar al menos un nombre de dominio en el campo **Usuario remitente**.
- Para establecer una conexión segura al servidor SMTP, seleccione uno de los tipos de conexión siguientes.
 - **SSL.** Utiliza el protocolo SSL para crear una comunicación segura.
 - **STARTTLS.** Utiliza el protocolo TLS para formar una comunicación segura en un canal no seguro.

Si se selecciona uno de estos tipos de conexión, XClarity Orchestrator intenta descargar e importar el certificado de servidor SMTP a su almacén de confianza de XClarity Orchestrator. Se le pedirá que acepte este certificado.

- 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.
 - **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 especificados. 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 6. Haga clic en **Crear** para crear la configuración de destino.

Después de finalizar

Puede realizar las siguientes acciones desde la tarjeta Destinos del despachador.

- Modifique un destino seleccionado haciendo clic en el icono **Editar** (✎).
- Elimine un destino seleccionado haciendo clic en el icono **Eliminar** (🗑). No se puede eliminar un destino que esté asignado a un despachador

Reenvío de informes por correo electrónico

Puede reenviar informes periódicamente a una o varias direcciones de correo electrónico utilizando un servicio web SMTP.

Acerca de esta tarea

Un *informe* es cualquier datos que se presenta en forma de tabla en la interfaz de usuario. Actualmente, se admiten los siguientes informes.

- Alertas activas
- Sucesos de recursos y auditorías
- Dispositivos gestionados (servidores, almacenamiento, conmutadores y chasis).
- Cumplimiento del firmware del dispositivo
- Cumplimiento de configuración del servidor
- Estado de la garantía de los servidores
- Activar informes de servicio

Cada despachador de informes solo puede incluir un informe de cada tipo.

El informe se crea como archivo y se guarda en el host del servidor de organización. Si el archivo tiene 10 MB o menos, se reenvía como archivo adjunto por correo electrónico. Si tiene más de 10 MB, el correo electrónico incluye la ubicación de los archivos. También puede descargar el archivo haciendo clic en **Historial de informes** y después en **Descargar**, en la fila correspondiente al informe.

Lenovo XClarity Orchestrator almacena un máximo de 100 informes. Si se alcanza el número máximo de informes, XClarity Orchestrator elimina el informe más antiguo antes de generar uno nuevo.

Procedimiento

Realice uno de los pasos siguientes para reenviar un informe por correo electrónico.

- **Enviar datos no filtrados**

1. En la barra de menú de XClarity Orchestrator, haga clic en **Supervisión** (📧) → **Reenvío** y, luego haga clic en **Despachadores de informes** en el menú de navegación izquierdo para mostrar la tarjeta Informes.
2. Haga clic en el icono de **Crear** (+) para mostrar el cuadro de diálogo Crear informe.
3. Especifique el nombre del despachador de informes y una descripción opcional.
4. Elija habilitar o deshabilitar el despachador de informes haciendo clic en el icono de alternación de **Estado**.
5. Haga clic en **Lista de contenido** y seleccione uno o varios informes que desee reenviar.
6. Haga clic en **Destino del despachador** y seleccione el destino (consulte [Creación de configuraciones de destino del despachador](#)).
7. Haga clic en **Planificaciones** y especifique el día, hora y duración de la semana (fecha de inicio y término) cuando desee que se envíen los informes. El informe se envía el mismo día y hora cada semana durante la duración especificada.
8. Haga clic en **Crear** para crear el despachador.

- **Enviar datos filtrados**

1. En la barra de menú XClarity Orchestrator, abra la tarjeta que contiene el informe que desea enviar. Se admiten los siguientes informes.
 - Datos del dispositivo (haga clic en **Recursos** (📁) → {device_type})
 - Datos de alertas activas (haga clic en **Supervisión** (📧) → **Alertas**)
 - Datos de sucesos de recursos y auditoría (haga clic en **Supervisión** (📧) → **Sucesos**)
 - Cumplimiento de firmware (haga clic en **Aprovisionamiento** (🔧) → **Actualizaciones** → **Aplicar y activar** → **Dispositivos**)
 - Conformidad con la configuración del servidor (haga clic en **Aprovisionamiento** (🔧) → **Configuración de servidor** → **Asignar y desplegar**)
 - Datos de garantía del dispositivo (haga clic en **Administración** (🔧) → **Servicio y soporte** → **Garantía**)
 - Estados de servicio activos (haga clic en **Administración** (🔧) → **Servicio y soporte** → **Informes de servicio**)
2. Opcionalmente, puede incluir los datos configurados únicamente en la información que le interesan, al restringir el alcance de los datos solo a los recursos que están en grupos y gestores de recursos específicos y al utilizar filtros y búsquedas para incluir datos que coincidan con criterios específicos (consulte [Consejos y técnicas de la interfaz de usuario](#)).
3. Haga clic en **Todas las acciones** → **Crear despachador de informes** para mostrar el cuadro de diálogo Crear despachador de informes.
4. Especifique el nombre del despachador de informes y una descripción opcional.
5. Elija habilitar o deshabilitar el despachador de informes haciendo clic en el icono de alternación de **Estado**.
6. Haga clic en **Destino del despachador** y seleccione el destino (consulte [Creación de configuraciones de destino del despachador](#)).
7. Haga clic en **Planificaciones** y especifique el día, hora y duración de la semana (fecha de inicio y término) cuando desee que se envíen los informes. El informe se envía el mismo día y hora cada semana durante la duración especificada.
8. Haga clic en **Crear** para crear el despachador.

Después de finalizar

Puede realizar las siguientes acciones desde la tarjeta Despachador de informes.

- Habilite o deshabilite un despachador de informes seleccionado al seleccionar el icono de alternación de la columna **Estado**.
- Modifique un despachador de informes seleccionado haciendo clic en el icono **Editar** (✎).
- Elimine un despachador de informes seleccionado haciendo clic en el icono **Eliminar** (🗑).
- Guarde los informes en el sistema local haciendo clic en la pestaña **Historial de informes** y luego haciendo clic en **Descargar** en la fila de cada informe.

Puede añadir un informe a un despachador de informes existente desde cualquier tarjeta de informe compatible utilizando los filtros de datos aplicados actualmente a la tabla haciendo clic en **Todas las acciones** → **Añadir contenido al despachador de informes existente** desde dicha tarjeta. Si el despachador de informes ya incluye un informe de ese tipo, este se actualiza para utilizar los filtros de datos actuales.

Capítulo 4. Gestión de recursos

Puede utilizar Lenovo XClarity Orchestrator para gestionar recursos, incluida la visualización de los detalles de los dispositivos sin conexión.

Creación de grupos de recursos

Un *grupo de recursos* es un conjunto de recursos que puede ver y sobre los que puede actuar conjuntamente en Lenovo XClarity Orchestrator. Se admiten varios tipos de grupos de recursos.

Más información:  [Cómo crear un grupo de recursos](#)

Acerca de esta tarea

Se admiten varios tipos de grupos de recursos.

- Los *grupos de dispositivos dinámicos* contienen un conjunto dinámico de dispositivos en función de criterios específicos.
- Los *grupos de dispositivos* contienen un conjunto estático de dispositivos específicos.
- Los *grupos de gestores* contienen un conjunto estático de gestores de recursos específicos y XClarity Orchestrator.
- Los *grupos de infraestructura* contienen un conjunto de dispositivos de red. Cuando gestiona un gestor de recursos de Schneider Electric EcoStruxure IT Expert, XClarity Orchestrator clona automáticamente las recolecciones de “grupo” que se definen en un Experto de TI de EcoStruxure gestionado. El grupo clonado se denomina $\{domain\}\{groupName\}$ en el repositorio local. Tenga en cuenta que las colecciones de tipo ubicación (sitio, edificio, sala, fila o bastidor) no se clonan.

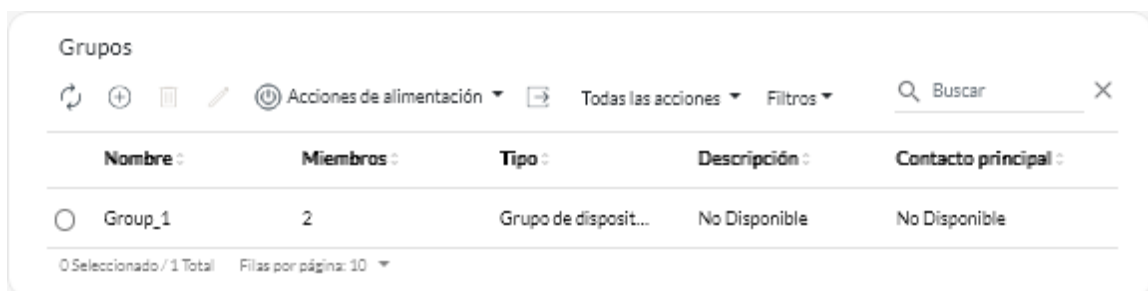
Nota: No puede crear un grupo de recursos con una mezcla de dispositivos, gestores de recursos y recursos de infraestructura.

Procedimiento

Para crear un grupo de recursos y gestionar la membresía, lleve a cabo los pasos siguientes.

- **Cree un grupo de dispositivos dinámicos y agregue dispositivos.**

1. En la barra de menús de XClarity Orchestrator, haga clic en **Recursos** (⚙️) → **Grupos** para mostrar la tarjeta de Grupos.



2. Haga clic en el icono de **Crear** (+) para mostrar el cuadro de diálogo Crear grupo.
3. Seleccione el **Grupo dinámico de dispositivos** como el tipo de grupo.
4. Especifique el nombre y descripción opcional del grupo.

- Haga clic en **Criterios de grupo** y seleccione las reglas que desea utilizar para la membresía de grupo.

Crear grupo

Propiedades Dispositivos disponibles Información de contacto

Tipo de grupo *

Grupo de dispositivos

Nombre de grupo *

Descripción

Dispositivos disponibles > Crear

- Elija si un dispositivo debe coincidir con **cualquiera** (una o más) o con **todas** las reglas de la lista desplegable de coincidencia de **Criterios**.
 - Especifique el atributo, el operador y el valor de cada regla. Haga clic en **Agregar criterios** para agregar otra regla.
- Haga clic en **Información de contacto** y, opcionalmente, seleccione un contacto de soporte principal (en la columna **Contactos principales**) y uno o más contactos secundarios (en la columna **Contactos secundarios**) para asignarlos a todos los dispositivos del grupo.
 - Haga clic en **Crear**. El grupo se agregará a la tabla.
- **Cree un grupo de recursos estático y añada recursos.**
 - Desde la barra de menú de XClarity Orchestrator, haga clic en **Recursos** (⚙️) → **Grupos** para mostrar la tarjeta Grupos.
 - Haga clic en el icono de **Crear** (+) para mostrar el cuadro de diálogo Crear grupo.
 - Seleccione **Grupo de dispositivos** o **Grupo de administradores** como tipo de grupo.
 - Especifique el nombre y descripción opcional del grupo.
 - Haga clic en **Dispositivos disponibles** o **Gestores de recursos disponibles**, según el tipo de grupo y seleccione los recursos que desea incluir en el grupo.
 - Haga clic en **Información de contacto** y, opcionalmente, seleccione un contacto de soporte principal (en la columna **Contactos principales**) y uno o más contactos secundarios (en la columna **Contactos secundarios**) para asignarlos a todos los dispositivos del grupo.
 - Haga clic en **Crear**. El grupo se agregará a la tabla.
 - **Añada dispositivos a un grupo de dispositivos estático.**
 - En la barra de menús de XClarity Orchestrator, haga clic en **Recursos** (⚙️) y, a continuación, haga clic en el tipo de dispositivo (como Servidores o Conmutadores) para mostrar una tarjeta con una lista de todos los dispositivos de ese tipo.

Servidores

Q Buscar X

Iniciar Control remoto
 Acciones de alimentación

 Todas las acciones

Filtros ▼

<input type="checkbox"/>	Servidor	Estado	Conectiv	Alimenta	Direcció	Nombre	Tipo-Mo	Firmwar	Aviso	Grupos
<input type="checkbox"/>	New...				10.24	Leno...	719...	N3E1f	No ...	No Dis
<input type="checkbox"/>	ite-b...				10.24	Leno...	716...	CGE1f	No ...	No Dis
<input type="checkbox"/>	Blac...				10.24	Leno...	716...	A3EGf	No ...	No Dis
<input type="checkbox"/>	nod...				10.24	IBM ...	791...	No Dis	No ...	No Dis
<input type="checkbox"/>	IM...				10.24	IBM ...	873...	B2E11	No ...	No Dis
<input type="checkbox"/>	Cara...				10.24	Eagl...	791...	No Dis	No ...	No Dis
<input type="checkbox"/>	blad...				10.24	IBM ...	790...	No Dis	No ...	No Dis
<input type="checkbox"/>	New...				10.24	Leno...	719...	N3E1f	No ...	No Dis
<input type="checkbox"/>	New...				10.24	Leno...	719...	N3E1f	No ...	No Dis
<input type="checkbox"/>	New...				10.24	Leno...	719...	N3E1f	No ...	No Dis

0 Seleccionado / 60 Total Filas por página: 10

2. Seleccione uno o varios dispositivos para agregar a un grupo.
3. Haga clic en el icono de **Añadir artículo a grupo** ().
4. Seleccione un grupo existente o especifique un nombre y descripción opcional para crear un grupo nuevo y haga clic en **Aplicar**.

- **Añada gestores de recursos a un grupo de gestores estático.**

1. Desde la barra de menú de XClarity Orchestrator, haga clic en **Recursos** () → **Gestores de recursos** para mostrar la tarjeta de Gestores de recursos.
2. Seleccione uno o varios gestores de recursos para agregar a un grupo.
3. Haga clic en el icono de **Añadir artículo a grupo** ().
4. Seleccione un grupo existente o especifique un nombre y descripción opcional para crear un grupo nuevo y haga clic en **Aplicar**.

Después de finalizar

Puede llevar a cabo las siguientes acciones desde la tarjeta Grupos.

- Modifique las propiedades y la membresía de un grupo seleccionado haciendo clic en el icono de **Editar** ().

Nota: Para los grupos de infraestructura que se ha clonado desde Schneider Electric EcoStruxure IT Expert, use Schneider Electric EcoStruxure IT Expert para cambiar el nombre del grupo, la descripción y la membresía.

- Elimine un grupo seleccionado haciendo clic en el icono de **Eliminar** (🗑️).
- Consulte los miembros de un grupo de recursos haciendo clic en el nombre del grupo para mostrar el cuadro de diálogo Ver grupo y luego haga clic en la pestaña **Resumen de miembros**.

Gestión de dispositivos sin conexión

Si un dispositivo no está gestionado actualmente por un gestor de recursos, puede utilizar Lenovo XClarity Orchestrator para gestionar los dispositivos en modo *sin conexión* importando un archivo de datos del servicio asociado con dicho dispositivo.

Acerca de esta tarea

Solo los servidores con controladores de gestión de la placa base IMM2 o XCC pueden gestionarse fuera de línea. Estos dispositivos se identifican en la interfaz web utilizando el estado de conectividad “Gestionado sin conexión”.

Puede realizar las acciones siguientes en dispositivos que son gestionados sin conexión. Todas las demás acciones están deshabilitadas.

- Ver inventario de dispositivo
- Excluir alertas y sucesos
- Gestionar datos de servicio
- Abra informes de servicio en el Centro de soporte de Lenovo mediante la función Llamar a casa y gestione los informes de servicio
- Recupere la información de garantía
- Funciones de análisis para predecir y analizar problemas con esos dispositivos

Importante: XClarity Orchestrator no se comunica con dispositivos sin conexión para recuperar datos actualizados.

Procedimiento

Para gestionar dispositivos sin conexión, lleve a cabo los pasos siguientes.

- Paso 1. En la barra de menús de Lenovo XClarity Orchestrator, haga clic en **Recursos** (🔍) → **Servidores**. Se muestra la página Servidores.
- Paso 2. Haga clic en el icono **Importar** (📁) para importar archivos de datos de servicio.
- Paso 3. Arrastre uno o varios archivos de datos de servicio (en formato .gz, .tzz o .tgz) al cuadro de diálogo Importar o haga clic en **Examinar** para ubicar el archivo.
- Paso 4. Opcionalmente, habilite **Añadir el servidor de los datos de servicio al inventario para ver únicamente** para gestionar el servidor aplicable en el modo de gestión fuera de línea (consulte [Gestión de dispositivos sin conexión](#)).
- Paso 5. Haga clic en el icono **Importar** para importar y analizar el archivo. Cuando se completa el análisis, el **Estado de análisis** del archivo importado cambia a "Analizado".

Puede supervisar el estado del proceso de importación y análisis desde el registro de trabajos ([Supervisión de trabajos](#)).

Después de finalizar

Puede no gestionar un dispositivo seleccionado gestionado fuera de línea haciendo clic en el icono de **No gestionar** (🚫).

Realización de acciones de alimentación en servidores gestionados

Puede utilizar Lenovo XClarity Orchestrator para encender, apagar y reiniciar servidores gestionados.

Antes de empezar








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

Los servidores ThinkSystem requieren un sistema operativo para realizar las operaciones de encendido.


Asegúrese de que el sistema operativo en el servidor cumpla con la interfaz de alimentación y configuración avanzada (ACPI) y que esté configurado para permitir las operaciones de apagado.

Acerca de esta tarea

XClarity Orchestrator admite las siguientes acciones de alimentación.

-  **Encender**. Enciende servidores seleccionados que actualmente están apagados.
-  **Apagar normalmente**. Apaga el sistema operativo y apaga servidores seleccionados que actualmente están encendidos.
-  **Apagar inmediatamente**. Apaga servidores seleccionados que actualmente están encendidos.
-  **Reiniciar normalmente**. Apaga el sistema operativo y reinicia los servidores seleccionados que actualmente están encendidos.
-  **Reiniciar de inmediato**. Reinicia servidores seleccionados que actualmente están encendidos.
-  **Reiniciar a la configuración del sistema**. Se reinicia a la configuración de BIOS/UEFI (F1) para servidores seleccionados.
-  **Reiniciar el controlador de gestión**. Reinicia el controlador de gestión de la placa base para servidores seleccionados.

Notas:


- Para dispositivos del cliente ThinkEdge, solo se admite  **Reiniciar normalmente**.
- El estado de conectividad del servidor debe ser “En línea”. No puede realizar acciones de alimentación en dispositivos que están fuera de línea, incluidos dispositivos gestionados fuera de línea.

Puede realizar acciones de alimentación en un máximo de 25 dispositivos a la vez.


• Procedimiento

Para encender, apagar o reiniciar servidores, lleve a cabo los pasos siguientes

Para un servidor único

- a. En el menú de XClarity Orchestrator, haga clic en **Recursos**  → **Servidores**. Se muestra la tarjeta Servidores con una vista de tabla de todos los servidores gestionados.
- b. Haga clic en la fila del servidor para mostrar las tarjetas de resumen del servidor para dicho servidor.
- c. En la tarjeta Acciones rápidas, haga clic en **Acciones de alimentación** y luego haga clic en la acción de alimentación deseada.
- d. Haga clic en **Confirmar**.

Para varios servidores

- a. En el menú de XClarity Orchestrator, haga clic en **Recursos**  → **Servidores**. Se muestra la tarjeta Servidores con una vista de tabla de todos los servidores gestionados.

- b. Seleccione uno o más servidores. Puede seleccionar un máximo de 25 servidores.
- c. Haga clic en **Acciones de alimentación** y luego en la acción de alimentación deseada.

Se muestra un cuadro de diálogo con una lista de los dispositivos seleccionados. Tenga en cuenta que los dispositivos que no son aplicables (que no admiten acciones de alimentación) están fuera de servicio.

- d. Haga clic en **Confirmar**.

Para todos los servidores de un grupo

- a. En el menú de XClarity Orchestrator, haga clic en **Recursos** (🔍) → **Grupos**. Se muestra la tarjeta Grupos con una vista de tabla de todos los grupos.
- b. Seleccione un grupo de servidores.
- c. En la tarjeta Acciones rápidas, haga clic en **Acciones de alimentación** y luego haga clic en la acción de alimentación deseada.

Se muestra un cuadro de diálogo con una lista de los dispositivos seleccionados. Tenga en cuenta que los dispositivos que no son aplicables (que no admiten acciones de alimentación) están fuera de servicio.

- d. Seleccione los servidores específicos en el grupo sobre los que desea actuar. Puede seleccionar un máximo de 25 servidores.
- e. Haga clic en **Confirmar**.

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

Apertura de una sesión de control remoto para servidores gestionados

Puede abrir una sesión de control remoto a un servidor gestionado como si estuviera en una consola local. Puede utilizar la sesión de control remoto para realizar operaciones como encendido o apagado del servidor y para montar lógicamente una unidad remota o local.

Apertura de una sesión de control remoto para servidores ThinkSystem o ThinkAgile

Puede abrir una sesión de control remoto a un servidor ThinkSystem o ThinkAgile gestionado como si estuviera en una consola local. A continuación, puede utilizar la sesión de control remoto para realizar las operaciones de gestión.

Antes de empezar

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

El servidor gestionado debe tener un estado normal y un estado de conectividad en línea. Para obtener más información acerca de cómo ver el estado del servidor, consulte [Visualización de los detalles del dispositivo](#).

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.

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 para un servidor ThinkSystem o ThinkAgile.

- Paso 1. En el menú de XClarity Orchestrator, haga clic en **Recursos** (🔧) → **Servidores**. Se muestra la tarjeta Servidores con una vista de tabla de todos los servidores gestionados.
- Paso 2. Seleccione el servidor que controlará de forma remota.
- Paso 3. Haga clic en el icono de **Iniciar 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 Orchestrator..

Apertura de una sesión de control remoto para servidores ThinkServer

Puede abrir una sesión de control remoto servidores ThinkServer gestionados como si estuviera en una consola local. Luego, 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, para crear capturas de pantalla y para grabar video.

Antes de empezar

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

El servidor gestionado debe tener un estado normal y un estado de conectividad en línea. Para obtener más información acerca de cómo ver el estado del servidor, consulte [Visualización de los detalles del dispositivo](#).

La clave de características bajo demanda de ThinkServer System Manager Premium Upgrade debe estar instalada en el servidor gestionado. Para obtener más información acerca las claves de característica bajo demanda (FoD) que están instaladas en los servidores, consulte [Visualización de las claves de características bajo demanda](#) en la documentación en línea de Lenovo XClarity Administrator.

Se debe instalar Java Runtime Environment (JRE) con soporte de Java WebStart (como Adopt OpenJDK 8 con el plugin the IcedTea-Web v1.8) en el servidor local.

Acerca de esta tarea

Puede abrir una sesión de control remoto en un solo servidor ThinkServer.

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 para un servidor ThinkSystem o ThinkAgile.

Paso 1. En el menú de XClarity Orchestrator, haga clic en **Recursos** (🔍) → **Servidores**. Se muestra la tarjeta Servidores con una vista de tabla de todos los servidores gestionados.

Paso 2. Seleccione el servidor que controlará de forma remota.

Paso 3. Haga clic en el icono de **Iniciar 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 Orchestrator..

Apertura de una sesión de control remoto para servidores System x

Puede abrir una sesión de control remoto servidores System x gestionados como si estuviera en una consola local. Luego, 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, para crear capturas de pantalla y para grabar video.

Antes de empezar

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](#).

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

El servidor gestionado debe tener un estado normal y un estado de conectividad en línea. Para obtener más información acerca de cómo ver el estado del servidor, consulte [Visualización de los detalles del dispositivo](#).

Utilice su cuenta de usuario de Lenovo XClarity Orchestrator para iniciar sesión en la sesión de control remoto. La cuenta de usuario debe tener suficiente autoridad de usuario para acceder a un servidor y gestionarlo.

Se debe instalar Java Runtime Environment (JRE) con soporte de Java WebStart (como Adopt OpenJDK 8 con el plugin the IcedTea-Web v1.8) en el servidor local.

La clave de Características bajo demanda para presencia remota debe instalarse y habilitarse en el servidor gestionado. Puede determinar si la presencia remota está habilitada o deshabilitada en la página Servidores, haciendo clic en **Filtros** → **Presencia remota**. Si está deshabilitada:

- Asegúrese de que el servidor se encuentra en un estado Normal y en un estado de conectividad En línea.
- Asegúrese de que el nivel de XClarity Controller empresarial o Actualización avanzada de MM estén habilitados para servidores que no tienen estas características ya activadas de forma predeterminada.

En la sesión de control remoto se utilizan los valores de entorno local e idioma de pantalla definidos para el sistema operativo en el sistema local.

Acerca de esta tarea

Puede iniciar varias sesiones de control remoto. Cada sesión puede gestionar varios servidores.

Nota: Para servidores 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

Complete los pasos siguientes para abrir una sesión de control remoto para un servidor System x.

Paso 1. En el menú de XClarity Orchestrator, haga clic en **Recursos** (🔍) → **Servidores**. Se muestra la tarjeta Servidores con una vista de tabla de todos los servidores gestionados.

Paso 2. Seleccione el servidor que controlará de forma remota.

Si no selecciona un servidor, se abre una sesión de control remoto sin destino.

Paso 3. Haga clic en el icono de **Iniciar Control remoto** (🔗).

Paso 4. Acepte las advertencias de seguridad del navegador web.

Paso 5. 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 dicho servidor se bloquean hasta que se desconecta 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 Orchestrator admite hasta seis sesiones de control remoto simultáneas en el mismo servidor.

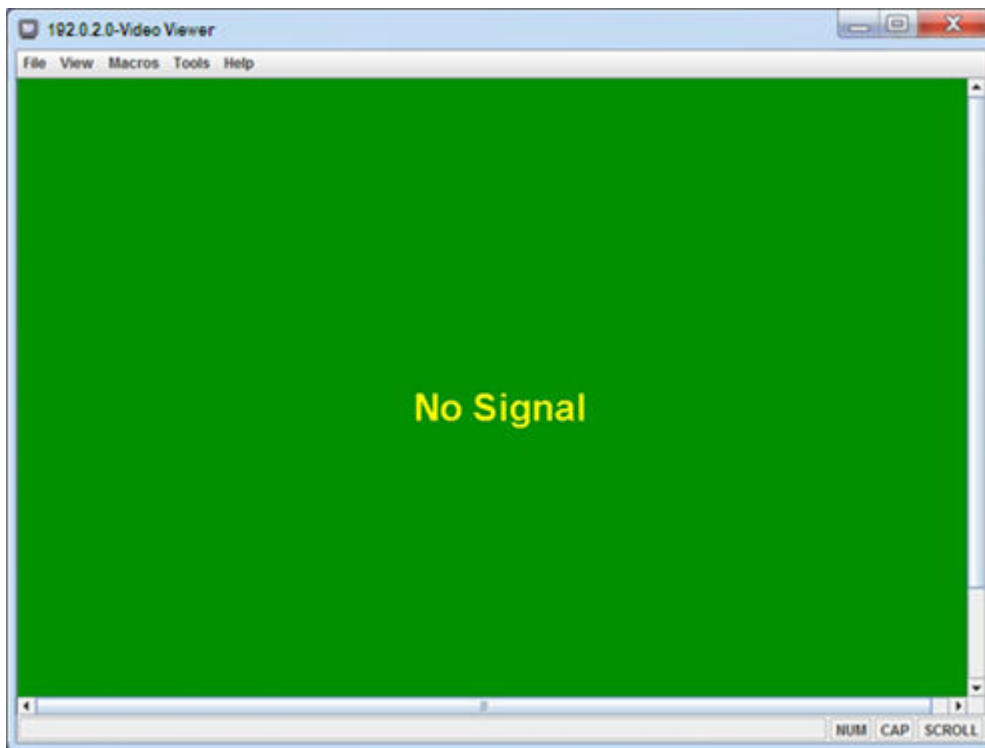
Paso 6. Haga clic en **Iniciar Control remoto**.

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. Puede usar este acceso directo para iniciar una sesión de control remoto sin iniciar sesión en la interfaz web de XClarity Orchestrator. El acceso directo contiene un enlace que abre una sesión de control remoto a la que se pueden añadir servidores manualmente.

Nota: El sistema local debe tener acceso a XClarity Orchestrator para validar la cuenta de usuario con el servidor de autenticación de XClarity Orchestrator.







Después de finalizar

La sesión de control remoto tiene una miniatura (icono) para cada servidor que actualmente se gestiona a través de la sesión.





Si la sesión de control remoto no se abre correctamente, consulte [Problemas con el Control remoto](#) en la documentación en línea de XClarity Orchestrator.





En la sesión de control remoto puede llevar a cabo las siguientes acciones.

- Muestre varias consolas de servidor y desplácese por las consolas de servidor haciendo clic en una miniatura. La consola de servidor se muestra en el área de sesiones de video. Si está accediendo a más servidores de los que caben en el área de icono, haga clic en los iconos **Desplazar a la derecha** () y **Desplazar a la izquierda** () para desplazarse por otras miniaturas de servidores. Haga clic en el icono de **Todas las sesiones** () para ver una lista de todas las sesiones de servidor abiertas.
- Agregue una consola de servidor a la sesión de control remoto actual haciendo clic en el icono de **Añadir servidor** ()
- Oculte o muestre el área de miniaturas haciendo clic en el icono de **Alternar miniaturas** ()
- Muestre la sesión de control remoto en una ventana o a pantalla completa; para ello, haga clic en el icono de **Pantalla** () y haga clic en **Activar pantalla completa** o **Desactivar pantalla completa**.
- Utilice los botones de teclas especiales Ctrl, Alt y Mayús para enviar pulsaciones de tecla directamente al servidor. Cuando hace clic en una tecla especial, la tecla se mantiene activa hasta que presiona una tecla en el teclado o vuelve a hacer clic en el botón. Para enviar combinaciones de las teclas Ctrl o Alt, haga clic en el botón Ctrl o Alt en la barra de herramientas, sitúe el cursor en el área de sesiones de vídeo y presione una tecla 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](#)).

- Defina secuencias de teclas personalizadas, conocidas como teclas programables, haciendo clic en el icono de **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. Puede exportar valores de usuario, incluidas teclas programables, haciendo clic en el icono de **Preferencias** () en la pestaña **Valores de usuario** y luego en **Importar**.

- Haga 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 de **Pantalla** () y, a continuación, en **Captura de pantalla**.
- Monte un medio remoto (como un CD, DVD o dispositivo USB, una imagen de disco o una imagen de CD [ISO]) en el servidor seleccionado, o bien mueva un dispositivo montado a otro servidor haciendo clic en el icono de **Medio remoto** () .
- Cargue imágenes a un servidor desde un medio remoto haciendo clic en el icono de **Medio remoto** () , luego en **Montar medio remoto** y, finalmente, en **Cargar la imagen al IMM**.
- Encender o apagar el servidor desde una consola remota haciendo clic en el icono de **Alimentación** () .
- Cambie las preferencias de control remoto, incluida la frecuencia de actualización del icono de servidor (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 Orchestrator. 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.
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](#).

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 de **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 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 Orchestrator 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 vídeo. 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.
- **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.

Capítulo 5. Aprovisionamiento de recursos

Puede utilizar Lenovo XClarity Orchestrator para aprovisionar los recursos gestionados, como el despliegue de actualizaciones en los gestores de recursos y servidores gestionados de Lenovo XClarity Administrator y la configuración de servidores gestionados.

Aprovisionamiento de configuraciones de servidor

Los patrones de configuración de servidor se utilizan para configurar rápidamente varios servidores desde un solo conjunto de valores de configuración definidos. Cada patrón define las características de configuración de un tipo de servidor específico. Puede crear un patrón de servidor mediante el aprendizaje de la configuración de un servidor existente.

Antes de empezar

Asegúrese de que los servidores que desea configurar estén actualizados con el firmware más reciente.

Acerca de esta tarea

La configuración de servidores utilizando patrones solo es compatible con servidores ThinkSystem (excepto SR635 y SR655).

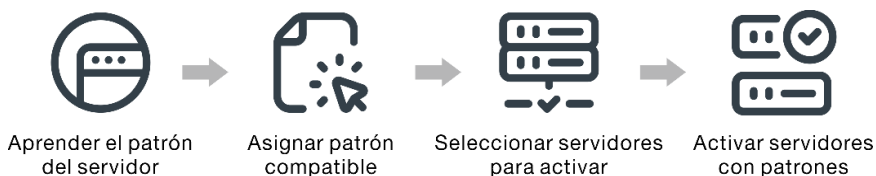
Puede utilizar patrones de configuración de servidor para configurar los valores y las definiciones del controlador de gestión de la placa base y de Unified Extensible Firmware Interface (UEFI) en servidores gestionados. Los patrones integran el soporte para la virtualización de direcciones de E/S, de modo que es posible virtualizar conexiones del entramado del servidor o readaptar servidores sin interrupciones en el entramado.

No puede configurar los valores siguientes.

- Orden de arranque
- Almacenamiento local y función de zonas de SAN
- Adaptadores de E/S
- Cuentas de usuarios locales
- Servidores LDAP

Procedimiento

En la siguiente figura se ilustra el flujo de trabajo para configurar servidores gestionados.



Paso 1. Cree un patrón de servidor

Puede crear patrones para representar las distintas configuraciones que se utilizan en su centro de datos al conocer los valores de configuración y las definiciones de los servidores existentes.

Importante: Considere la posibilidad de crear un patrón de servidor para cada tipo de servidor en su centro de datos. Por ejemplo, cree un patrón de servidor para todos los servidores de ThinkSystem SR650 y otro patrón de servidor para todos los servidores de ThinkSystem SR850.

No despliegue un patrón de configuración de servidor que fue creado para un tipo de servidor en otro tipo de servidor.

Para obtener más información sobre la creación de patrones de servidor, consulte [Aprendizaje de un patrón de configuración de servidor a partir de un servidor existente](#).

Paso 2. **Asigne el patrón a uno o más servidores gestionados**

Puede asignar un patrón a varios servidores; sin embargo, cada servidor puede tener solo un patrón asignado XClarity Orchestrator.

Considere la posibilidad de crear un patrón de servidor para cada tipo de servidor en su centro de datos. Por ejemplo, cree un patrón de servidor para todos los servidores de ThinkSystem SR650 y otro patrón de servidor para todos los servidores de ThinkSystem SR850.

No asigne ni despliegue un patrón de servidor que fue creado para un tipo de servidor en otro tipo de servidor.

Después de asignar un patrón aplicable a uno o más servidores de destino, XClarity Orchestrator ejecuta una comprobación de cumplimiento en los servidores para determinar si la configuración del servidor coincide con el patrón. Los servidores no conformes con su patrón asignado se marcan.

Para obtener más información sobre la creación de patrones de servidor, consulte [Aplicar y activar actualizaciones a los gestores de recursos](#).

Paso 3. **Despliegue el patrón asignado en los servidores de destino**

Puede desplegar patrones asignados a uno o más servidores específicos o a grupos de servidores. Cuando despliega un patrón, los valores de configuración y las definiciones de dicho patrón se escriben en la memoria compartida y luego se activan. Algunos valores requieren reiniciar el sistema antes de que se activen.

Los servidores se deben reiniciar para activar determinados cambios de la configuración, como el controlador de gestión de la placa base y los valores de las configuraciones de Unified Extensible Firmware Interface (UEFI). Puede elegir cuándo activar los cambios:

- **Activación aplazada** activa todos los cambios de la configuración después del siguiente reinicio del servidor. El servidor de destino debe reiniciarse manualmente para continuar con el proceso de despliegue.

Importante: Utilice **Reiniciar normalmente** para reiniciar el servidor y continuar con el proceso de actualización. *No* utilice **Reiniciar de inmediato**.

Nota: Los valores de un servidor pueden llegar a ser no conformes con su patrón si los valores se cambian directamente en el servidor en lugar de hacerlo en los patrones asignados o si se ha producido un problema cuando se desplegaba el patrón asignado, como un problema de hardware o un valor no válido. Puede determinar el estado de cumplimiento de cada servidor en la pestaña **Asignar y desplegar**.

Atención: XClarity Orchestrator no asigna direcciones IP y de E/S a servidores individuales cuando se despliegan los patrones de servidor.

Para obtener más información acerca de la creación de políticas de conformidad de actualizaciones, consulte [Asignación y despliegue de un patrón de configuración de servidor](#).

Paso 4. **Modifique y vuelva a desplegar un patrón**

Puede hacer cambios de configuración posteriormente en un patrón existente. Cuando guarde el patrón, XClarity Orchestrator ejecuta una comprobación

de cumplimiento en los servidores asignados a ese patrón para determinar si la configuración del servidor coincide con el patrón. A continuación, puede volver a desplegar el patrón cambiado en todos los servidores o en un subconjunto de servidores asignados a ese patrón.

Consideraciones sobre la configuración de servidores

Antes de empezar a configurar servidores con Lenovo XClarity Orchestrator, tenga en cuenta las siguientes consideraciones importantes.

Consideraciones sobre el servidor

- La configuración de servidores utilizando patrones solo es compatible con servidores ThinkSystem (excepto SR635 y SR655).
- Asegúrese de que los servidores que desea configurar estén actualizados con el firmware más reciente.

Consideraciones sobre los patrones de configuración

- Puede asignar un patrón a varios servidores; sin embargo, cada servidor puede tener solo un patrón asignado XClarity Orchestrator.

Nota: XClarity Orchestrator no le impide asignar o desplegar un patrón de configuración de servidor a un servidor que tenga un patrón o perfil de servidor asignado en Lenovo XClarity Administrator. El despliegue de un patrón utilizando XClarity Orchestrator puede afectar el cumplimiento del patrón en XClarity Administrator.

- Puede utilizar patrones de configuración de servidor para configurar los valores y las definiciones del controlador de gestión de la placa base y de Unified Extensible Firmware Interface (UEFI) en servidores gestionados. Los patrones integran el soporte para la virtualización de direcciones de E/S, de modo que es posible virtualizar conexiones del entramado del servidor o readaptar servidores sin interrupciones en el entramado.

No puede configurar los valores siguientes.

- Orden de arranque
 - Almacenamiento local y función de zonas de SAN
 - Adaptadores de E/S
 - Cuentas de usuarios locales
 - Servidores LDAP
- Considere la posibilidad de crear un patrón de servidor para cada tipo de servidor en su centro de datos. Por ejemplo, cree un patrón de servidor para todos los servidores de ThinkSystem SR650 y otro patrón de servidor para todos los servidores de ThinkSystem SR850.
 - No asigne ni despliegue un patrón de servidor que fue creado para un tipo de servidor en otro tipo de servidor.
 - Los valores de un servidor pueden estar fuera de cumplimiento con su patrón asignado en las siguientes instancias. Puede determinar el estado de cumplimiento de cada servidor en la pestaña **Asignar y desplegar**.
 - Los valores de configuración se cambiaron directamente en el servidor en lugar de hacerlo en los patrones asignados.
 - Se ha producido un problema durante el despliegue del patrón, como un problema de firmware o un valor no válido.
 - Se actualizó el firmware, que cambió los valores y las definiciones de configuración.

Nota: Se podría producir un error en el despliegue si el patrón asignado se basa en niveles de firmware anteriores. En este caso, se recomienda que elija un nuevo patrón basado en el firmware instalado actualmente o que modifique el patrón existente para excluir la configuración de elementos específicos antes de desplegar el patrón.

Consideraciones sobre el proceso de configuración

- Mientras la configuración está en progreso, el servidor de destino permanece bloqueado. No puede iniciar otras tareas de gestión en el servidor de destino hasta que se complete el proceso de configuración.
- Después de que se ha desplegado un patrón de configuración en un servidor, puede que se deba reiniciar una o más veces para que los cambios se activen por completo. Si elige reiniciar el servidor de inmediato, tiene la opción de activar todos los cambios. Si lo hace, XClarity Orchestrator minimiza el número de reinicios necesarios. Si elige aplazar la activación, todos los cambios se activan la próxima vez que el servidor se reinicia. Si elige la activación parcial, los cambios que no requieren reiniciar el servidor se activan de inmediato, y todos los demás cambios se activan la próxima vez que el servidor se reinicia.
- 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 configuración queda en cola hasta que se completen todos los otros trabajos.
- Algunas funciones avanzadas del servidor se activan utilizando las claves de características bajo demanda. Si las características tienen valores configurables que aparecen durante la configuración de la UEFI, puede configurar los valores utilizando patrones de configuración; no obstante, la configuración resultante no se activa hasta que se instala la clave de características bajo demanda correspondiente.

Aprendizaje de un patrón de configuración de servidor a partir de un servidor existente

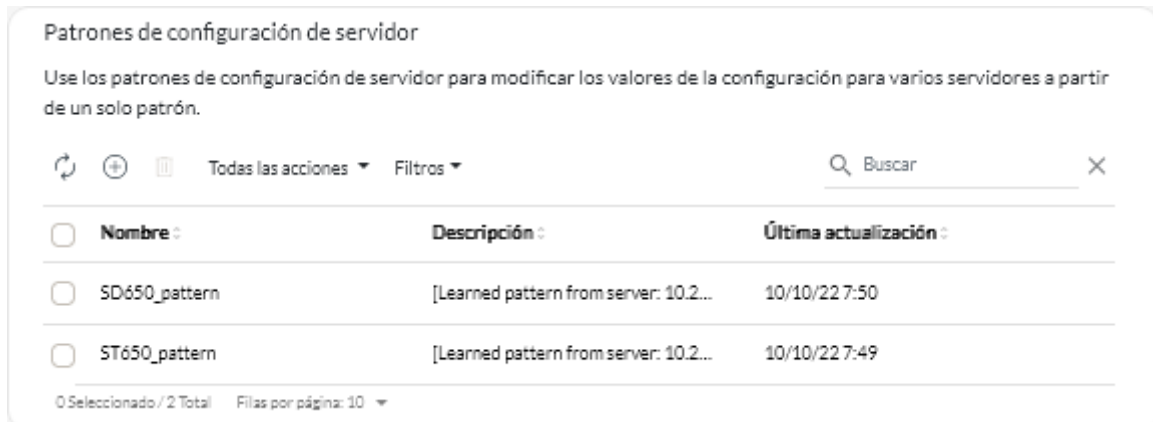
Los patrones de configuración de servidor definen las características de configuración de un tipo de servidor específico. Puede crear un patrón de servidor mediante el aprendizaje de la configuración de un servidor existente

Antes de empezar

- Asegúrese de leer las consideraciones de configuración del servidor antes de crear un patrón de configuración de servidor (consulte [Consideraciones de actualización](#)).
- Asegúrese de que el servidor que desea utilizar para crear el patrón esté en línea.
- 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 desplegar los mismos valores de configuración de varios servidores y, por tanto, controlar una configuración común desde un solo lugar.

Para crear un patrón mediante el aprendizaje de la configuración de un servidor existente, lleve a cabo los pasos siguientes.

- Paso 1. En la barra de menú de XClarity Orchestrator, haga clic en **Aprovisionamiento** (🔑) → **Configuración de servidor** y luego haga clic en la pestaña **Patrones** para mostrar la tarjeta Patrones de configuración de servidor.



Patrones de configuración de servidor

Use los patrones de configuración de servidor para modificar los valores de la configuración para varios servidores a partir de un solo patrón.

🔄 + 🛑 Todas las acciones ▾ Filtros ▾ 🔍 Buscar ✕

<input type="checkbox"/>	Nombre :	Descripción :	Última actualización :
<input type="checkbox"/>	SD650_pattern	[Learned pattern from server: 10.2...	10/10/22 7:50
<input type="checkbox"/>	ST650_pattern	[Learned pattern from server: 10.2...	10/10/22 7:49

0 Seleccionado / 2 Total Filas por página: 10 ▾

Paso 2. Haga clic en el icono de **Crear** (+) para mostrar el cuadro de diálogo Crear patrón de configuración de servidor.

Crear un patrón de configuración del servidor ✕

Especifique el nombre y la descripción del patrón

Nombre

Descripción

Seleccionar servidor para obtener la configuración básica ⓘ

🔄 Todas las acciones ▾ Filtros ▾ ✕

Dispositivos	Direcciones IP	Nombre del producto
<input type="radio"/> Colossus-ST650V2-1	10.240.211.65, 2002:97b:c2bt	ThinkSystem ST650V2
<input type="radio"/> Mehlow-ST250-1	10.240.211.39, 169.254.95.11	ThinkSystem ST250
<input type="radio"/> OceanCat-SDV-6	10.240.211.221, 2002:97b:c2t	Lenovo ThinkSystem SD650

0 Seleccionado / 3 Total Filas por página: 10 ▾

Obtendrá

Paso 3. Especifique el nombre y descripción opcional del patrón.

Paso 4. Seleccione el servidor que desee utilizar como base para este patrón.

Nota: Los modelos de dispositivo no admitidos se muestran en texto gris y no se pueden seleccionar.

Paso 5. Haga clic en **Aprender**.

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

Después de finalizar

Puede llevar a cabo las siguientes acciones desde la tarjeta Patrones.

- Vea los detalles del patrón haciendo clic en la fila del patrón.
- Copie un patrón seleccionado haciendo clic en el icono de **Copiar** (📄).
- Modifique los valores de configuración de un patrón haciendo clic en la fila del patrón para mostrar los detalles de patrones, haciendo los cambios necesarios y luego haciendo clic en **Guardar**. De forma predeterminada, todos los valores aprendidos están incluidos en el patrón. Puede excluir valores del patrón seleccionando los valores **Excluir/incluir valores en este patrón** y, a continuación, borrando los

valores que no desea en el patrón. Los valores que se borran (marcados para la exclusión) se resaltan en amarillo. Al hacer clic en **Guardar**, solo se enumeran los valores incluidos en el patrón. Si ha excluido valores, puede volver a incluirlos haciendo clic en **Excluir/incluir valores en este patrón**, haciendo clic en **Mostrar los valores excluidos** y seleccionando los valores que desea incluir. Los valores que están seleccionados (marcados para la inclusión) se resaltan en verde.

Nota: La comprobación de conformidad se basa solo en los valores incluidos. Los valores excluidos no se marcan.

Cuando guarde el patrón modificado, XClarity Orchestrator ejecuta una comprobación de cumplimiento en los servidores asignados a ese patrón para determinar si la configuración del servidor coincide con el patrón. A continuación, puede desplegar el patrón cambiado en los servidores no conformes (consulte [Asignación y despliegue de un patrón de configuración de servidor](#)).

The screenshot displays the 'Configuración del patrón' (Pattern Configuration) interface. On the left, a sidebar shows a navigation menu with 'Configuración del patrón' selected, and options for 'BMC extendido' and 'UEFI extendido'. Below the menu are toggle switches for 'Excluir/incluir valores en este patrón' and 'Mostrar los valores excluidos', both currently turned on. A legend indicates that 'Excluido' is marked with a red box and 'Incluido' with a green box. The main content area is titled 'Configuración del patrón' and contains a form with 'Nombre*' (SD650_pattern) and 'Descripción' ([Learned pattern from server: 10.240.211.221 on 2022-10-10]). Below the form is a tree view of configuration options, including 'Integrated Management Module' (with sub-items like Login Profile, General Settings, and Network Settings Interface) and 'UEFI' (with sub-items like System Recovery, Devices and I/O Ports, Processors, and Physical Presence Policy Configuration). The 'System Recovery' section is expanded, showing settings for POST Watchdog Timer (Disable, 5), Reboot System on NMI (Disable), Post Load Setup Default (Disable), and <F1> Start Control (Auto).

- Copie un patrón de configuración haciendo clic en la fila del patrón para mostrar los detalles del patrón y luego haciendo clic en **Guardar como**.
- Elimine un patrón seleccionado haciendo clic en el icono de **Eliminar** (🗑️). Si el patrón se asigna a uno o más servidores, se muestra un cuadro de diálogo con una lista de los servidores aplicables. Cuando confirma la solicitud de eliminación, el patrón se desasigna de esos servidores.

Nota: No puede eliminar un patrón que se esté desplegando activamente en los servidores.

- Asigne y despliegue un patrón en uno o varios servidores de destino (consulte [Asignación y despliegue de un patrón de configuración de servidor](#)).

Asignación y despliegue de un patrón de configuración de servidor

Puede asignar y desplegar un patrón de configuración de servidor en uno o más servidores gestionados.

Antes de empezar

- Asegúrese de leer las consideraciones de configuración del servidor antes de asignar o desplegar un patrón a un servidor (consulte [Consideraciones de actualización](#)).
- Asegúrese de que los servidores que desea configurar estén actualizados con el firmware más reciente.
- No asigne ni despliegue un patrón de servidor que fue creado para un tipo de servidor en otro tipo de servidor.
- XClarity Orchestrator no le impide asignar o desplegar un patrón de configuración de servidor a un servidor que tenga un patrón o perfil de servidor asignado en Lenovo XClarity Administrator. El despliegue de un patrón utilizando XClarity Orchestrator puede afectar el cumplimiento del patrón en XClarity Administrator.
- XClarity Orchestrator no asigna direcciones IP y de E/S a servidores individuales cuando se despliegan los patrones de servidor.

Acerca de esta tarea

Cuando se asigna un patrón a un servidor, XClarity Orchestrator ejecuta una comprobación de cumplimiento para comparar los valores de configuración actuales del servidor con los valores del patrón de configuración y actualiza la columna **Estado de cumplimiento** en función de los resultados. El estado de cumplimiento puede ser cualquiera de los siguientes valores.

- **Conformidad.** Todos los valores de configuración del patrón asignado coinciden con los valores del servidor.
- **No conforme.** Uno o más valores de configuración del patrón asignado *no* coinciden con los valores del servidor. Pase el mouse sobre la celda de la tabla para mostrar una ventana emergente que enumera la configuración y los valores no coincidentes.
- **Pendiente.** Hay un despliegue de patrón o una comprobación de cumplimiento en curso.
- **Reinicio pendiente.** Es necesario reiniciar el servidor para activar los cambios de la configuración después del despliegue del patrón.
- **No disponible.** No hay un patrón asignado al servidor.

Cuando despliega un patrón en un servidor, XClarity Orchestrator modifica los valores del servidor para que coincida con su patrón de configuración de servidor asignado. Una vez finalizado el despliegue, XClarity Orchestrator ejecuta la comprobación de cumplimiento para verificar que los valores del patrón asignado coinciden con el valor del servidor, y luego se actualiza el estado de cumplimiento del servidor.

Procedimiento

Para asignar y desplegar un patrón de configuración de servidor en uno o varios servidores, lleve a cabo los pasos siguientes.

- Paso 1. En la barra de menú de XClarity Orchestrator, haga clic en **Aprovisionamiento** (🔑) → **Configuración de servidor** y luego haga clic en la pestaña **Asignar y desplegar** para mostrar la tarjeta Asignar y desplegar patrones de configuración de servidor.

Asignar y desplegar


Para modificar los valores de configuración en varios servidores, asigne un patrón aplicable y luego despliegue ese patrón en los servidores. ⓘ

Todas las acciones ▾ Filtros ▾ ✕

<input type="checkbox"/> Dispositivos :	Estado :	Patrón asignado :	Estado de cumplimie	Grupos :
<input type="checkbox"/> Colossus-ST650V2-	⊗ Crítico	Sin asignación ▾	ⓘ Sin patrón asig	No Disponible
<input type="checkbox"/> Mehlow-ST250-1	⊗ Crítico	Sin asignación ▾	ⓘ Sin patrón asig	No Disponible
<input type="checkbox"/> OceanCat-SDV-6	⊙ Normal	Sin asignación ▾	ⓘ Sin patrón asig	No Disponible

0 Seleccionado / 3 Total Filas por página: 10 ▾

Paso 2. Asigne un patrón a uno o más servidores.

1. Seleccione uno o más servidores.
2. Haga clic en el icono de **Asignar** () para mostrar el cuadro de diálogo Asignar patrones de configuración de servidor.

Asignar patrón de configuración de servidor ✕

Seleccione un patrón para asignarlo a los servidores seleccionados. El patrón se asigna únicamente a los servidores aplicables.

Patrón a asignar:

Aplicar a grupos de recursos específicos:

Asignar patrón a:

- Todos los dispositivos aplicables (sobrescribir patrones asignados)
- Dispositivos aplicables sin asignación de patrón actual
- Solo los dispositivos aplicables seleccionados (sobrescribir patrones asignados)
- Solo los dispositivos aplicables seleccionados sin asignación de patrón

3. Seleccione el patrón que desee asignar.

Notas:

- En esta lista se muestran todos los patrones aplicables para los servidores específicos. Es posible que la lista esté incompleta si el servidor de organización aún está calculando los patrones aplicables. En este caso, cierre el cuadro de diálogo, espere un momento y vuelva a abrir el cuadro de diálogo.

- Seleccione el patrón **Sin asignación** para desasignar un patrón de la lista de dispositivos seleccionada.
4. Seleccione la regla de asignación. Puede presentar uno de los valores siguientes.
 - **Todos los dispositivos aplicables (sobrescribir patrones asignados)**
 - **Dispositivos aplicables sin asignación de patrón actual**
 - **Solo los dispositivos aplicables seleccionados (sobrescribir patrones asignados)**
 - **Solo los dispositivos aplicables seleccionados sin asignación de patrón**
 5. Haga clic en **Asignar**.

Paso 3. Despliegue el patrón asignado en servidores específicos.

1. Seleccione uno o más servidores.

Nota: Los modelos de dispositivo no admitidos se muestran en texto gris y no se pueden seleccionar.

2. Haga clic en el icono de **Desplegar** (☑) para mostrar el cuadro de diálogo Desplegar patrón de configuración de servidor.

3. Elija cuándo se activan las actualizaciones.
 - **Activación aplazada** activa todos los cambios de la configuración después del siguiente reinicio del servidor. El servidor de destino debe reiniciarse manualmente para continuar con el proceso de despliegue.

Importante: Utilice **Reiniciar normalmente** para reiniciar el servidor y continuar con el proceso de actualización. *No utilice **Reiniciar de inmediato**.*
4. Haga clic en **Desplegar**. Se crea un trabajo para llevar a cabo esta operación. Puede supervisar el progreso del trabajo desde la tarjeta **Supervisión** (📊) → **Trabajos**. Si el trabajo no finalizó correctamente, haga clic en el enlace del trabajo para mostrar los detalles correspondientes (consulte .)

Después de finalizar

Puede llevar a cabo las siguientes acciones desde la tarjeta Patrones.

- Ejecute manualmente una comprobación de cumplimiento de la configuración en los servidores seleccionados haciendo clic en **Todas las acciones** → **Comprobación del cumplimiento**.

- Desasigne un patrón de uno o más servidores de destino asignando el patrón **Sin asignación**.
- Reenvía los informes sobre cumplimiento de configuración de forma periódica a una o varias direcciones de correo electrónico haciendo clic en el icono **Crear despachador de informes** (+). El informe se envía utilizando los filtros de datos aplicados actualmente a la tabla. Todas las columnas de la tabla mostradas y ocultas se incluyen en el informe. Para obtener más información, consulte el apartado [Reenvío de informes](#).
- Añada un informe de cumplimiento de configuración a un despachador de informes específico utilizando los filtros de datos aplicados actualmente a la tabla haciendo clic en el icono de **Agregar a despachador de informes** (→). Si el despachador de informes ya incluye un informe de cumplimiento de configuración, este se actualiza para utilizar los filtros de datos actuales.

Mantener el cumplimiento de configuración del servidor

Los valores de un servidor pueden llegar a estar fuera de conformidad con el servidor si los valores se cambiaron sin utilizar patrones de configuración, si se produjo un problema al aplicar un patrón de configuración (por ejemplo, si el patrón se creó desde un nivel de firmware anterior al que está en el servidor) o al aplicar una actualización de firmware que cambia la configuración del servidor (por ejemplo, se pueden agregar o eliminar valores, los comportamientos de configuración pueden cambiar, se pueden agregar nuevas opciones o rangos de valor pueden cambiar).

Acerca de esta tarea

Puede determinar el estado de cumplimiento de cada servidor desde la columna **Estado de cumplimiento** en la página Configuración del servidor: Asignar y desplegar. Si un servidor no es conforme, sitúe el cursor encima del estado para determinar el motivo.

Procedimiento

Para corregir los problemas de conformidad con la configuración del servidor, siga uno de estos pasos.

- Obtenga un nuevo patrón de configuración basado en el nivel de firmware actual (consulte [Aprendizaje de un patrón de configuración de servidor a partir de un servidor existente](#)). A continuación, asigne y aplique ese patrón al servidor (consulte [Asignación y despliegue de un patrón de configuración de servidor](#)).
- Modifique el patrón de configuración aplicable para corregir valores no conformes haciendo clic en la fila del patrón para mostrar los detalles de patrones, haciendo los cambios necesarios y luego haciendo clic en **Guardar**. De forma predeterminada, todos los valores aprendidos están incluidos en el patrón. Puede excluir valores del patrón seleccionando los valores **Excluir/incluir valores en este patrón** y, a continuación, borrando los valores que no desea en el patrón. Los valores que se borran (marcados para la exclusión) se resaltan en amarillo. Al hacer clic en **Guardar**, solo se enumeran los valores incluidos en el patrón. Si ha excluido valores, puede volver a incluirlos haciendo clic en **Excluir/incluir valores en este patrón**, haciendo clic en **Mostrar los valores excluidos** y seleccionando los valores que desea incluir. Los valores que están seleccionados (marcados para la inclusión) se resaltan en verde.

Nota: La comprobación de conformidad se basa solo en los valores incluidos. Los valores excluidos no se marcan.

Cuando guarde el patrón modificado, XClarity Orchestrator ejecuta una comprobación de cumplimiento en los servidores asignados a ese patrón para determinar si la configuración del servidor coincide con el patrón. A continuación, puede desplegar el patrón cambiado en los servidores no conformes (consulte [Asignación y despliegue de un patrón de configuración de servidor](#)).

The screenshot displays the 'Configuración del patrón' (Pattern Configuration) interface. On the left, there is a sidebar with a vertical list of options: 'Configuración del patrón' (selected), 'BMC extendido', and 'UEFI extendido'. Below this, there are two toggle switches: 'Excluir/incluir valores en este patrón' (turned on) and 'Mostrar los valores excluidos' (turned on). A legend indicates that the 'Excluido' (Excluded) status is represented by a red box and 'Incluido' (Included) by a green box.

The main configuration area is titled 'Configuración del patrón' and contains two text input fields: 'Nombre*' (Name) with the value 'SD650_pattern' and 'Descripción' (Description) with the value '[Learned pattern from server: 10.240.211.221 on 2022-10-10]'. Below these fields, there is a list of configuration categories, each with a checked checkbox and a right-pointing arrow:

- Integrated Management Module**
 - > Login Profile
 - > General Settings
 - > Network Settings Interface
- UEFI**
 - System Recovery**
 - POST Watchdog Timer: Disable
 - POST Watchdog Timer Value: 5
 - Reboot System on NMI: Disable
 - Post Load Setup Default: Disable
 - <F1> Start Control: Auto
 - > Devices and I/O Ports
 - > Processors
 - > Physical Presence Policy Configuration

- Cree una copia modificada del patrón de configuración haciendo clic en la fila del patrón para mostrar los detalles de patrones, haciendo los cambios necesarios y luego haciendo clic en **Guardar como**. A continuación, asigne y aplique ese patrón al servidor no conforme (consulte [Asignación y despliegue de un patrón de configuración de servidor](#)).

Aprovisionamiento de sistemas operativos

Puede utilizar Lenovo XClarity Orchestrator para gestionar el repositorio de imágenes del SO y para desplegar imágenes del sistema operativo.

Antes de empezar

XClarity Orchestrator no despliega directamente sistemas operativos en los dispositivos. En su lugar, envía solicitudes al gestor de recursos correspondiente para realizar el despliegue. Asegúrese de que el gestor de recursos tenga las licencias necesarias para realizar funciones de despliegue del SO.

Revise las consideraciones de despliegue antes de intentar desplegar sistemas operativos en sus servidores gestionados (consulte [Consideraciones del despliegue del sistema operativo](#)).

Asegúrese de que todo el firmware del servidor gestionado tenga la versión más reciente (consulte [Aprovisionamiento de actualizaciones para los recursos gestionados](#)).

Asegúrese de que la configuración del servidor gestionado esté actualizada (consulte [Aprovisionamiento de configuraciones de servidor](#)).

Atención: Se recomienda *no* utilizar XClarity Orchestrator para realizar un despliegue del sistema operativo completo en dispositivos Converged y ThinkAgile.

Nota: Asegúrese de que los servidores se estén gestionando utilizando XClarity Administrator 4.0 o posterior.

Acerca de esta tarea

XClarity Orchestrator proporciona una forma sencilla de desplegar imágenes de sistema operativo en servidores sin sistema operativo. Si despliega un sistema operativo en un servidor que tiene un sistema operativo instalado, XClarity Orchestrator 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 se tarda en recopilar los datos de inventario. También afecta a la cantidad de tiempo que tarda en iniciarse el firmware del UEFI cuando se arranca el servidor. Durante el despliegue del sistema operativo, el servidor se reinicia varias veces.
- La cantidad de tráfico de red. La imagen del sistema operativo se descarga en el servidor sobre la red de datos o la red de despliegue del sistema operativo.
- La cantidad de RAM, procesadores y almacenamiento en la unidad de disco duro que está disponible para el servidor de organización y los gestores de recursos.

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.

Para desplegar un sistema operativo en un servidor, primero debe importar la imagen del sistema operativo al repositorio de imágenes de SO en el gestor de recursos de XClarity Orchestrator. Cuando se importa una imagen del SO:

- Se comprueba si hay espacio suficiente en el repositorio de imágenes de SO antes de importar el sistema operativo. En caso negativo, elimine una imagen existente del repositorio de imágenes de SO y vuelva a intentar importar la nueva.
- Se crea uno o más perfiles de esa imagen y se almacenan 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. También puede crear perfiles personalizados basados en los perfiles predefinidos en la imagen de SO base que se pueden desplegar para configuraciones específicas.

Para obtener una lista de sistemas operativos base y personalizados admitidos, consulte [Sistemas operativos compatibles](#).

Paso 2. **Personalizar y asignar el perfil del SO**

Los perfiles del sistema operativo se crean automáticamente al importar un sistema operativo. Los perfiles creados se basan en el tipo y la versión del sistema operativo. Puede modificar el perfil, incluidas las credenciales del SO, el nombre de host, los valores de red y almacenamiento, las claves de licencia y la ubicación de almacenamiento.

Paso 3. **Asignar y desplegar el perfil del SO**

Puede asignar un perfil de SO a uno o varios servidores de destino y, a continuación, desplegar el perfil en esos servidores. . Recuerde que para desplegar un sistema operativo, el servidor debe tener un estado de despliegue de **Preparado**.

XClarity Orchestrator no despliega directamente sistemas operativos en los dispositivos. En su lugar, envía una solicitud al gestor de recursos aplicable para realizar el despliegue y, a continuación, realiza un seguimiento del progreso de la solicitud. XClarity Orchestrator transfiere las imágenes aplicables al gestor de recursos y crea una solicitud para iniciar un trabajo en el gestor de recursos para realizar el despliegue.

Antes de intentar desplegar la imagen de un sistema operativo, revise [Consideraciones del despliegue del sistema operativo](#).

Para obtener más información acerca de cómo asignar y desplegar un perfil del SO, consulte [Despliegue de la imagen de un sistema operativo](#).

Consideraciones del despliegue del sistema operativo

Antes de intentar desplegar la imagen de un sistema operativo, revise las siguientes consideraciones.

Consideraciones del gestor de recursos

- Para los dispositivos que se gestionan con Lenovo XClarity Administrator, asegúrese de que la instancia de XClarity Administrator tenga las licencias o el período de prueba necesarios para realizar funciones de despliegue del SO.
- El despliegue del SO no se admite en los dispositivos gestionados por Lenovo XClarity Management Hub.

Consideraciones de dispositivo gestionado

- Asegúrese de que la función de despliegue del SO sea compatible con los dispositivos de destino..
- 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 todo el firmware del servidor gestionado tenga la versión más reciente (consulte [Aprovisionamiento de actualizaciones para los recursos gestionados](#)).
- Asegúrese de que la configuración del servidor gestionado esté actualizada (consulte [Aprovisionamiento de configuraciones de servidor](#)).Asegúrese también de que el dispositivo 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 del dispositivo](#)).

- Asegúrese de que esté definida la contraseña de la cuenta raíz que se va a utilizar para desplegar el sistema operativo. Para obtener más información sobre la configuración de la contraseña, consulte [Configuración de perfiles del sistema operativo](#).
- Asegúrese de que no haya ningún medio montado (como ISO) en el servidor de destino. Además, asegúrese de que no haya ninguna sesión de medio remoto activa abierta para el controlador de gestión.
- Asegúrese de que la marca de hora de BIOS con la fecha y hora actuales.
- Para servidores ThinkSystem
 - Asegúrese de que la opción BIOS heredada esté deshabilitada. Desde Setup Utility (F1) de BIOS/UEFI, haga clic en **Configuración de UEFI → Valores de sistema** y compruebe que la configuración de BIOS heredada esté establecida en Deshabilitada.
 - Para desplegar el sistema operativo se necesita la función de XClarity Controller empresarial.
- Para Servidores System x
 - Asegúrese de que la opción BIOS heredada esté deshabilitada. Desde Setup Utility (F1) de BIOS/UEFI, haga clic en **Configuración de UEFI → Valores de sistema** y compruebe que la configuración de BIOS heredada esté establecida en Deshabilitada.
 - Asegúrese de que se haya instalado una clave de característica bajo demanda (FoD) para la presencia remota. Puede determinar si la presencia remota está habilitada, deshabilitada o no instalada en un servidor desde la página Servidores (consulte [Visualización de los detalles del dispositivo](#)).
- Para los servidores de Flex System, asegúrese de que el chasis esté encendido.
- Para servidores NeXtScale, asegúrese de que se haya instalado una clave de característica bajo demanda (FoD) para la presencia remota. Puede determinar si la presencia remota está habilitada, deshabilitada o no instalada en un servidor desde la página Servidores (consulte [Visualización de los detalles del dispositivo](#)).
- Para los dispositivos Converged y ThinkAgile, se recomienda *no* utilizar XClarity Orchestrator para realizar un despliegue del sistema operativo completo.

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 imágenes de SO no se admitan solo en ciertas plataformas de hardware. Puede identificar si un sistema operativo es compatible con un servidor específico en [Sitio web de guía de interoperabilidad de SO de Lenovo](#).
- Siempre instale el sistema operativo más reciente para garantizar que cuente con los controladores de entrada de dispositivos de adaptador de E/S más recientes que necesita. 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 sobre cómo conseguir esa imagen, consulte [Soporte de VMware - página web de descargas](#).

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 el gestor de recursos esté configurado para utilizar tanto redes de gestión como de datos.
- Asegúrese de que el gestor de recursos se pueda comunicar con el servidor de destino (tanto el controlador de gestión de la placa base como la red de datos de los servidores) tanto a través de las interfaces de red gestión como de datos. Para especificar la interfaz que se va a utilizar para el despliegue del sistema operativo, consulte [Configuración del acceso de red](#) en la documentación en línea de XClarity Administrator.

Para obtener más información acerca de las redes e interfaces de despliegue de sistemas operativos, consulte [Consideraciones de red](#) en la documentación en línea de XClarity Administrator.

- Si la red es inestable o lenta, puede obtener resultados impredecibles al desplegar sistemas operativos.
- Debe utilizar direcciones IP asignadas dinámicamente mediante DHCP. No se admiten direcciones IP estáticas.

Para obtener más información acerca de las redes e interfaces de despliegue de sistemas operativos, consulte [Configuración del acceso de red](#) y [Consideraciones de red](#) en la documentación en línea de XClarity Administrator.

Consideraciones de almacenamiento y de opciones de arranque

- Puede instalar el sistema operativo solo en una unidad de disco local. No se admiten el hipervisor integrado, controladores M.2 ni el almacenamiento SAN.
- 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 varias unidades de disco. 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 varias unidades de disco en algunos casos. Para obtener más información, consulte [El instalador del SO no puede encontrar la unidad de disco en la que desea instalar](#) en la documentación en línea de XClarity Orchestrator.
- 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 varias unidades de disco. 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 varias unidades de disco en algunos casos.
- 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.

- Asegúrese de que el modo de arranque seguro esté deshabilitado para el servidor. Si está 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.
- 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.
 - 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 [Configuración de perfiles del sistema operativo](#).

Sistemas operativos compatibles

Lenovo XClarity Orchestrator admite el despliegue de varios sistemas operativos. Solo las versiones admitidas de sistemas operativos se pueden cargar en el repositorio de imágenes del SO de XClarity Orchestrator.

Importante:

- Para obtener más información sobre las limitaciones del despliegue de sistemas operativos para dispositivos específicos, consulte [Hardware y software admitidos](#) en la documentación en línea de XClarity Orchestrator.
- La característica de gestión criptográfica de XClarity Orchestrator 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 Orchestrator.
- Es posible que las imágenes de sistema operativo en el repositorio de imágenes de SO no se admitan solo en ciertas plataformas de hardware. 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 Orchestrator puede desplegar.

Sistema operativo	Versiones	Notas
Servidor Red Hat® Enterprise Linux (RHEL)	7.2 and later 8.x	Incluye KVM Notas: <ul style="list-style-type: none"> 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.
SUSE® Linux Enterprise Server (SLES)	12.3 and later 15.2 and later	Incluye hipervisores KVM y Xen Notas: <ul style="list-style-type: none"> 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.
VMware vSphere® Hypervisor (ESXi)	6.0.x 6.5.x 6.7.x 7.0.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: <ul style="list-style-type: none"> Se admiten todos los paquetes de actualizaciones existentes y futuros, 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). En algunas versiones de imágenes personalizadas de Lenovo VMware ESXi, puede haber imágenes separadas disponibles para ThinkSystem, System x 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.

Perfiles de las imágenes del sistema operativo

La importación de una imagen del SO genera perfiles del SO predefinidos. Cada perfil predefinido incluye la imagen del SO y las opciones de instalación de dicha imagen.

Puede modificar los perfiles para configurar las credenciales, la red y los valores de almacenamiento. También puede crear nuevos perfiles basados en las políticas del SO predefinido. Para obtener más información, consulte el apartado [Configuración de perfiles del sistema operativo](#).

En la tabla siguiente se muestra una lista de los perfiles de imagen del SO predefinidos que se crean al importar una imagen del sistema operativo. Esta tabla también enumera los paquetes que se incluyen en cada perfil.

Sistema operativo	Perfil de	Paquetes incluidos en el perfil
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
SUSE Linux Enterprise Server (SLES) 12.3 y posterior	Básico	<pattern>32bit</pattern> <pattern>Basis-Devel</pattern> <pattern>Minimal</pattern> <pattern>WBEM</pattern> <pattern>apparmor</pattern> <pattern>base</pattern> <pattern>documentation</pattern> <pattern>file_server</pattern> <pattern>fips</pattern> <pattern>gateway_server</pattern> <pattern>lamp_server</pattern> <pattern>mail_server</pattern> <pattern>ofed</pattern> <pattern>printing</pattern> <pattern>sap_server</pattern> <pattern>x11</pattern>
	Mínimo	<pattern>Minimal</pattern> <pattern>file_server</pattern> <pattern>sap_server</pattern>

Sistema operativo	Perfil de	Paquetes incluidos en el perfil
	KVM de virtualización	<pattern>32bit</pattern> <pattern>Minimal</pattern> <pattern>apparmor</pattern> <pattern>base</pattern> <pattern>documentation</pattern> <pattern>file_server</pattern> <pattern>fips</pattern> <pattern>kvm_server</pattern> <pattern>kvm_tools</pattern> <pattern>sap_server</pattern> <pattern>x11</pattern>
	Xen de virtualización	<pattern>32bit</pattern> <pattern>Minimal</pattern> <pattern>apparmor</pattern> <pattern>base</pattern> <pattern>documentation</pattern> <pattern>file_server</pattern> <pattern>fips</pattern> <pattern>sap_server</pattern> <pattern>x11</pattern> <pattern>xen_server</pattern> <pattern>xen_tools</pattern>
SUSE Linux Enterprise Server (SLES) 15.2 y posterior	Básico	<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	<pattern>base</pattern> <pattern>minimal_base</pattern> <pattern>yast2_basis</pattern> <package>wget</package>
	KVM de virtualización	<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
	Xen de virtualización	<pre> <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> </pre>
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 están abiertos (desbloqueados).

Asegúrese de que el hipervisor que está ejecutando el dispositivo de Lenovo XClarity Orchestrator permita el tráfico de red (TCP/UDP) en los puertos 139, 445, 3001, 3900, 8443, pues estos son necesarios para el despliegue del sistema operativo.

Perfil de virtualización RHEL

De forma predeterminada, el perfil de virtualización Red Hat Enterprise Linux (RHEL) bloquea todos los puertos excepto los que se indican en la tabla siguiente.

Tabla 1. Disponibilidad de puertos para los perfiles de virtualización de RHEL

Puerto	TCP o UDP	Dirección	Descripción de la comunicación
22	TCP	Entrada	Comunicación SSH
53	TCP, UDP	Salida/entrada	Comunicación con dispositivos de red KVM de RHEL
67	TCP, UDP	Salida/entrada	Comunicación con dispositivos de red KVM de RHEL
161	UDP	Salida	Comunicación con agentes SNMP
162	UDP	Entrada	Comunicación con agentes SNMP
427	TCP, UDP	Salida/entrada	Comunicación con agente de servicio SLP, agente de directorio SLP
3001	TCP	Salida/entrada	Comunicación con servicio de despliegue de imágenes de software de gestión
15988	TCP	Salida	Comunicación CIM-XML sobre HTTP
15989	TCP	Salida	Comunicación CIM-XML sobre HTTP
49152 - 49215	TCP	Salida/entrada	Comunicación de servidor virtual KVM

Perfiles básicos y mínimos de RHEL

De forma predeterminada, los perfiles básicos y mínimos de RHEL bloquean todos los puertos excepto los que se indican en la tabla siguiente.

Tabla 2. Disponibilidad de puertos para los perfiles básicos y mínimos de RHEL

Puerto	TCP o UDP	Dirección	Descripción de la comunicación
22	TCP	Entrada	Comunicación SSH
3001	TCP	Salida/entrada	Comunicación con servicio de despliegue de imágenes de software de gestión

Perfiles de virtualización, básicos y mínimos de SLES

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.

Perfil de virtualización VMware ESXi

Para ver una lista completa de los puertos abiertos para VMware vSphere Hypervisor (ESXi) con personalización de Lenovo, consulte la documentación de VMware para ESXi en la [Sitio web de la base de conocimiento de VMware](#).

Importación de imágenes del sistema operativo

Antes de desplegar un sistema operativo con licencia para servidores gestionados, debe importar la imagen al repositorio de imágenes de SO.

Acerca de esta tarea

Para obtener información sobre las imágenes del sistema operativo que puede importar y desplegar, incluidos los sistemas operativos base y personalizados compatibles, consulte [Sistemas operativos compatibles](#).

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 Orchestrator:

- Se comprueba si hay espacio suficiente en el repositorio de imágenes de SO antes de importar el sistema operativo. En caso negativo, elimine una imagen existente del repositorio y vuelva a intentar importar la nueva.
- Se crea uno o más perfiles de esa imagen y se almacenan 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 está importando es mayor que 4 GB, considere el uso de un navegador web (como Chrome o Firefox).

Procedimiento

Para importar una imagen del sistema operativo en el repositorio de imágenes del SO, siga estos pasos.

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 Orchestrator, haga clic en **Aprovisionamiento** (🔑) → **Despliegue del SO** y, a continuación, haga clic en la pestaña **Gestión de SO** para mostrar la página Gestión de SO.

Paso 3. Haga clic en **Imágenes de SO** en el panel de navegación izquierdo para mostrar la tarjeta Imágenes de SO.

Gestión de SO

A continuación se muestra la lista de imágenes de SO gestionadas por y almacenadas en este servidor de gestión. Puede importar una nueva imagen del SO desde la estación de trabajo local o eliminar una imagen del SO de este repositorio.

Uso de almacenamiento del SO: 394.2 MB de 185.8 GB.

Imágenes del SO

🔄 📄 🗑️ 📁 Todas las acciones ▾ Filtros ▾ 🔍 Buscar ✕

<input type="checkbox"/>	Nombre de sistema operativo ~	Versión :	Estado :
<input type="checkbox"/>	esxi7.0_3-20036589.1	7.0	Preparado

0 Seleccionado / 1 Total Filas por página: 10 ▾

Paso 4. Haga clic en el icono de **Importar archivos** (📁) para mostrar el cuadro de diálogo Importar imágenes del SO.

Paso 5. Arrastre y suelte la imagen .iso que desee importar o haga clic en **Examinar** para buscar la imagen ISO que desee importar.

Paso 6. **Opcional:** seleccione un tipo de suma de comprobación y copie y pegue el valor de suma de comprobación en el campo de texto proporcionado.

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 los siguientes tipos de suma de comprobación: MD5, SHA1 y SHA256.

Paso 7. Haga clic en **Importar**.

XClarity Orchestrator carga la imagen del SO en el repositorio de imágenes del SO y añade los perfiles de SO predefinidos en la pestaña **Perfiles de SO**.

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.

Después de finalizar

Desde esta página puede llevar a cabo las siguientes acciones.

- Para eliminar una imagen del SO seleccionada, haga clic en el icono de **Eliminar** (🗑️).
- Para ver y editar perfiles del SO, haga clic en la barra de menús de XClarity Orchestrator, después en **Aprovisionamiento** (🔑) → **Despliegue del SO** y, a continuación, haga clic en la pestaña **Perfiles de SO**, seleccione el perfil y haga clic en el icono de **Editar** (✎) (consulte Configuración de perfiles del sistema operativo).
- Para eliminar perfiles de SO, haga clic en la barra de menús de XClarity Orchestrator, después en **Aprovisionamiento** (🔑) → **Despliegue del SO** y, a continuación, haga clic en la pestaña **Perfiles de SO**, seleccione los perfiles y haga clic en el icono de **Eliminar** (🗑️).

Nota: Si elimina el último perfil predefinido restante de un sistema operativo, este también se elimina.

Configuración de perfiles del sistema operativo

Los perfiles del sistema operativo se crean automáticamente al importar un sistema operativo. Los perfiles creados se basan en el tipo y la versión del sistema operativo. Puede modificar el perfil, incluidas las credenciales del SO, el nombre de host, los valores de red y almacenamiento, las claves de licencia y la ubicación de almacenamiento.

Antes de empezar

Revise las consideraciones antes de desplegar un sistema operativo en un dispositivo de servidor gestionado. Para obtener más información, consulte [Consideraciones del despliegue del sistema operativo](#).

Procedimiento

Para configurar un perfil de SO para su despliegue, siga estos pasos.

- Paso 1. En la barra de menús de XClarity Orchestrator, haga clic en **Aprovisionamiento** (🔑) → **Despliegue del SO** y, a continuación, haga clic en la pestaña **Perfiles de SO** para mostrar la página Perfiles de SO.
- Paso 2. Seleccione el perfil del SO.
- Paso 3. Haga clic en el icono de **Editar** (✎) para mostrar la tarjeta Detalles del perfil de SO.

Paso 4. Configure los atributos del perfil.

- **Nombre.** Al modificar el nombre del perfil se crea un nuevo perfil del SO.
- **Descripción.** Modifique la descripción de este perfil de SO.
- **Credencial de SO.** Introduzca las credenciales de SO de la cuenta de administrador que debe utilizarse para iniciar sesión en el sistema operativo.
- **Nombre de host.** Seleccione lo que debe usarse para el nombre de host. Puede elegir uno de los valores siguientes.
 - **Usar nombre de host predeterminado.** (predeterminado) El nombre de host es “nodo” seguido de los primeros 11 caracteres del Id. de dispositivo (por ejemplo, nodoABC31213310).
- **Configuración de red.** Seleccione los valores IP de este perfil. Puede elegir uno de los valores siguientes.
 - **DHCP.** (predeterminado) Utilice la infraestructura DHCP existente para asignar direcciones IPv4 a los servidores.
- **Valor de dirección MAC.** Seleccione la dirección MAC del puerto en el host donde se instalará el sistema operativo. Puede elegir uno de los valores siguientes.

Nota: No se admiten los puertos de red virtuales. No utilice un puerto de red físico para simular varios puertos de red virtual.

- **Usar AUTO.** (predeterminado) 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 servidor se reinicia automáticamente para utilizar la dirección MAC recién detectada para el despliegue. El gestor de recursos de XClarity Administrator puede detectar automáticamente puertos de red en las ranuras 1 a 16. Al menos un puerto de las ranuras 1 a 16 debe tener conexión con el gestor de recursos aplicable.

Si desea utilizar un puerto de red en la ranura 17 o superior para la dirección MAC, no puede utilizar AUTO.

- **Storage.** Seleccione la ubicación de almacenamiento donde desea desplegar la imagen del sistema operativo.
 - **Usar unidad de disco.** Instale la imagen del sistema operativo en la primera unidad de disco local RAID enumerada en el servidor gestionado. Solo se admiten unidades de disco conectadas a un controlador RAID o HBA SAS/SATA.

Si el RAID del servidor no está configurado correctamente o si está inactivo, puede que el disco local no esté visible en el servidor de organización. Para solucionar el problema, habilite la configuración del RAID mediante patrones de configuración (consulte [Aprendizaje de un patrón de configuración de servidor a partir de un servidor existente](#)) o mediante el software de gestión de RAID del servidor.

Notas:

- Si también hay una unidad M.2 presente, la unidad de disco debe configurarse para RAID de hardware.
- Si se habilita un adaptador SATA, el modo SATA *no debe* configurarse en **IDE**.
- Para servidores ThinkServer, la configuración está disponible solo a través del software de gestión de RAID en el servidor.

Paso 5. Haga clic en **Guardar**.

Después de finalizar

Puede realizar las acciones siguientes.

- Asignar un perfil de SO a uno o varios servidores en la pestaña **Asignar y desplegar** haciendo clic en seleccionar servidores y luego en el icono de **Asignar** (🔗) o haciendo clic en el icono de **Asignar** (🔗) y luego seleccionando un grupo de servidores. Una vez seleccionado el perfil de SO, puede optar por asignar el perfil de SO a:
 - **Todos los dispositivos aplicables (sobrescribir perfiles asignados)**
 - **Dispositivos aplicables sin asignación de perfil actual**
 - **Solo los dispositivos aplicables seleccionados (sobrescribir perfiles asignados)**
 - **Solo los dispositivos aplicables seleccionados sin asignación de perfil**
- Eliminar perfiles de SO seleccionados haciendo clic en el icono de **Eliminar** (🗑️).

Nota: Si elimina el último perfil predefinido restante de un sistema operativo, este también se elimina.

Despliegue de la imagen de un sistema operativo

Puede utilizar Lenovo XClarity Orchestrator para desplegar un sistema operativo en sus servidores gestionados.

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](#)).

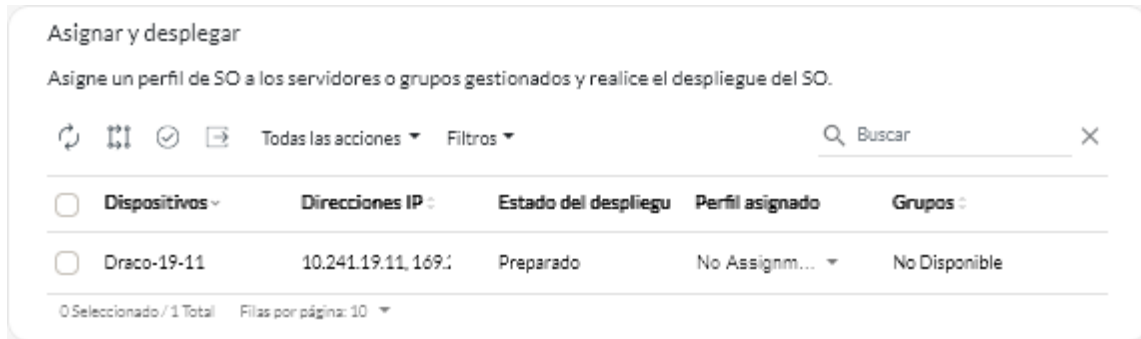
Atención: Si el servidor tiene instalado actualmente un sistema operativo, al desplegar la imagen se sobrescribirá el sistema operativo actual.

Procedimiento

Para desplegar la imagen de un sistema operativo en uno o varios servidores gestionados, realice uno de los procedimientos siguientes.

- **Para dispositivos específicos**

1. En la barra de menús de XClarity Orchestrator, haga clic en **Aprovisionamiento** (🔑) → **Despliegue del SO** y luego haga clic en la pestaña **Asignar y desplegar** para mostrar la tarjeta de Asignar y desplegar.



2. Seleccione uno o varios servidores en los que desee desplegar el sistema operativo.
3. Para cada servidor de destino, seleccione el perfil de SO que se desplegará de la lista desplegable en la columna **Perfiles de SO**. Asegúrese de seleccionar un perfil de SO compatible con el servidor de destino.
4. Compruebe que, para todos los servidores seleccionados, el estado de despliegue en la columna **Estado** sea Preparado.
5. Haga clic en el icono de **Desplegar** (☺) para mostrar el cuadro de diálogo Desplegar perfil.
6. Haga clic en el icono de **Desplegar** para iniciar el despliegue del sistema operativo. Se crea un trabajo para llevar a cabo esta operación. Puede supervisar el progreso del trabajo desde la tarjeta **Supervisión** (📧) → **Trabajos**. Si el trabajo no finalizó correctamente, haga clic en el enlace del trabajo para mostrar los detalles correspondientes (consulte .)

- **Para todos los dispositivos específicos de un grupo**

1. En la barra de menús de XClarity Orchestrator, haga clic en **Aprovisionamiento** (🔑) → **Despliegue del SO** y luego haga clic en la pestaña **Asignar y desplegar** para mostrar la tarjeta de Asignar y desplegar.
2. Asigne un perfil de SO al grupo de servidores.
 - a. Haga clic en el icono de **Asignar** (🔗) para mostrar el cuadro de diálogo Asignar perfil.

- b. Seleccione el perfil que se va a asignar.
 - c. Seleccione el grupo de dispositivos que se va a asignar.
 - d. Elija qué dispositivos del grupo se van a asignar.
 - **Todos los dispositivos aplicables (sobrescribir perfiles asignados)**
 - **Dispositivos aplicables sin asignación de perfil actual**
 - **Solo los dispositivos aplicables seleccionados (sobrescribir perfiles asignados)**
 - **Solo los dispositivos aplicables seleccionados sin asignación de perfil**
 - e. Haga clic en **Desplegar**.
3. Haga clic en el icono de **Desplegar** (☺) para mostrar el cuadro de diálogo Desplegar perfil.

4. Seleccione el grupo de dispositivos en el que desea desplegar el perfil de SO asignado.
5. Haga clic en el icono de **Desplegar** para iniciar el despliegue del sistema operativo. Se crea un trabajo para llevar a cabo esta operación. Puede supervisar el progreso del trabajo desde la tarjeta

Supervisión (📊) → **Trabajos**. Si el trabajo no finalizó correctamente, haga clic en el enlace del trabajo para mostrar los detalles correspondientes (consulte .)

Aprovisionamiento de actualizaciones para los recursos gestionados

Puede utilizar Lenovo XClarity Orchestrator para mantener los niveles actuales de software en los gestores de recursos y servidores gestionados de Lenovo XClarity Administrator. Puede utilizar el catálogo de actualizaciones para conocer los niveles de software que están disponibles, utilizar las políticas de conformidad de actualización para identificar los recursos que se deben actualizar basándose en criterios personalizados y, a continuación, desplegar las actualizaciones deseadas en esos recursos.

Procedimiento

En la siguiente figura se ilustra el flujo de trabajo para actualizar recursos gestionados.



Paso 1. Actualizar el catálogo

El *repositorio de actualizaciones* contiene un catálogo de los paquetes de actualización que se pueden aplicar a los recursos gestionados.

El *catálogo* contiene información acerca de las actualizaciones que están disponibles en la actualidad. El catálogo organiza las actualizaciones por tipos de recursos (plataformas) y componentes. Cuando actualiza el catálogo, XClarity Orchestrator recupera información acerca de las últimas actualizaciones disponibles desde el sitio web de soporte de Lenovo y almacena la información en el repositorio de actualizaciones.

Importante: XClarity Orchestrator debe estar conectado a Internet para actualizar el catálogo.

Cuando los nuevos paquetes de actualización estén disponibles, debe importar los paquetes de actualización aplicables antes de poder aplicar una actualización. Actualizar el catálogo no importa automáticamente los paquetes de actualizaciones.

Cuando XClarity Orchestrator se instala por primera vez, el repositorio de actualizaciones está vacío.

Paso 2. Descargar o importar paquetes de actualización en el repositorio

Si XClarity Orchestrator está conectado a Internet, puede descargar los paquetes de actualización que se enumeran en el catálogo de actualizaciones directamente desde el sitio web de soporte de Lenovo. Si XClarity Orchestrator no está conectado a Internet, puede importar manualmente los paquetes de actualización que descargó anteriormente desde el [Sitio web del Soporte del Centro de Datos de Lenovo](#) a una estación de trabajo que disponga de acceso de red para el host de XClarity Orchestrator.

Si elige descargar una versión menor, también se descargan los paquetes de actualización de requisitos previos.

Cuando importe manualmente los paquetes del repositorio, debe importar la carga útil (.tgz), los metadatos (.xml), el registro de cambios (.chg) y el archivo léame (.txt).

Cuando importe manualmente las actualizaciones, deberá importar los archivos requeridos en función del tipo de recurso.

- Para servidores ThinkSystem V3, importe el paquete de actualización único (*.zip). Este archivo zip contiene la carga útil, los archivos de metadatos (varios archivos *.json), el archivo de registro de cambios (*.chg) y el archivo Léame (*.txt).
- Para dispositivos del cliente ThinkEdge, importe la carga útil (Windows .exe). El archivo Léame (.txt) es opcional. Tenga en cuenta que, actualmente, solo se admite la actualización del **paquete de la utilidad flash BIOS para Windows**.
- Para XClarity Management Hub y XClarity Management Hub 2.0, importe el archivo de paquete de actualización único (.tgz). Este archivo contiene la carga útil, metadatos, historial de cambios y los archivos léame.
- Para el resto de recursos (incluido XClarity Administrator, servidores ThinkEdge, ThinkSystem V1 y V2, y dispositivos heredados), importe la carga útil (.zip, .uxz, .tar.gz, .tar, .bin), los metadatos (.xml), el registro de cambios (.chg) y el archivo Léame (.txt).

Para obtener más información sobre cómo importar actualizaciones, consulte [Descarga e importación de actualizaciones](#).

Paso 3. **Crear y asignar políticas de conformidad de actualización**

Las *políticas de cumplimiento de actualización* garantizan que el software o firmware de determinados recursos gestionados se encuentran en el nivel actual o especificado marcando los recursos que necesitan atención. Cada política de cumplimiento de actualización identifica qué recursos se supervisan y el nivel de software o firmware que debe instalarse a fin de mantener el cumplimiento de los recursos. XClarity Orchestrator utiliza estas políticas para comprobar el estado de los recursos gestionados e identificar los recursos que están fuera de cumplimiento.

Al crear una política de cumplimiento de actualización, puede elegir que XClarity Orchestrator marque un recurso cuando el software o firmware en el recurso sea de nivel inferior.

Una vez que se asigna una política de cumplimiento de actualización a un recurso, XClarity Orchestrator comprueba el estado de conformidad del recurso cuando cambia el repositorio de actualizaciones. Si el software o el firmware en el recurso no está en cumplimiento con la política de conformidad asignada, XClarity Orchestrator marca ese recurso como que no está en cumplimiento en la página Aplicar/Activar, según las reglas que ha especificado en la política de cumplimiento.

Por ejemplo, puede crear una política de conformidad de actualización que defina el nivel de línea base para el software para XClarity Administrator y, a continuación, asignar esa política de conformidad a todos los gestores de recursos de XClarity Administrator. Cuando se actualiza el catálogo de actualizaciones y cuando se descargan o importan nuevas actualizaciones, es posible que instancias de XClarity Administrator queden fuera de conformidad. Si esto ocurre, XClarity Orchestrator actualiza la página Aplicar/Activar para mostrar cuáles instancias de XClarity Administrator no son conformes y genera una alerta.

Para obtener más información acerca de la creación de políticas de conformidad de actualizaciones, consulte [Creación y asignación de políticas de conformidad de actualización](#).

Paso 4. **Aplicar y activar actualizaciones**

XClarity Orchestrator no aplica automáticamente las actualizaciones. Para actualizar los recursos de software, debe aplicar y activar manualmente la actualización en los recursos seleccionados que no cumplen con la política de cumplimiento de actualización asignada.

XClarity Orchestrator no actualiza los recursos directamente. En su lugar, envía una solicitud al gestor de recursos aplicable para realizar la actualización y, a continuación, realiza un seguimiento del progreso de la solicitud. XClarity Orchestrator identifica las dependencias que se requieren para realizar la actualización, garantiza que los recursos de destino se actualicen en el orden correcto, transfiere los paquetes de actualización aplicables al gestor de recursos y crea una solicitud para iniciar un trabajo en el gestor de recursos para realizar la actualización.

Para obtener más información acerca de cómo aplicar actualizaciones, consulte [Aplicar y activar actualizaciones a los gestores de recursos](#) y [Aplicar y activar actualizaciones a los servidores gestionados](#).

Consideraciones de actualización

Antes de implementar actualizaciones usando Lenovo XClarity Orchestrator, revise las siguientes consideraciones de importancia.

- Para obtener el mejor rendimiento, asegúrese de que los gestores de recursos de Lenovo XClarity Administrator ejecutan la versión 3.2.1 o posterior
- Asegúrese de que el repositorio de actualizaciones contiene los paquetes de actualización que desea aplicar. De lo contrario, actualice el catálogo de productos y descargue las actualizaciones adecuadas (consulte [Descarga e importación de actualizaciones](#)).
- Asegúrese de que no haya trabajos que se encuentren en ejecución en la actualidad en el recurso de destino. Si hay trabajos en ejecución, el trabajo de actualización queda en cola hasta que se completen todos los otros trabajos.
- Si el recurso tiene una política de cumplimiento de actualización asignada que presenta una no conformidad, debe corregir el no cumplimiento ajustando la política de cumplimiento o al asignar una política de alternativa.
- Si elige instalar un paquete de actualización que contiene actualizaciones para varios componentes, se actualizan todos los componentes a los que se aplica dicho paquete de actualización.

Consideraciones de recursos

- La función de actualizaciones solo admite la actualización de servidores y de gestores de recursos. Para ThinkSystem SR635 y SR655, solo son compatibles las actualizaciones de firmware BMC y UEFI.

Para los dispositivos ThinkSystem y ThinkAgile, las actualizaciones de firmware no son compatibles con el controlador gestionado de la placa base ni los bancos de copia de seguridad UEFI. En su lugar, actualice el banco principal y, a continuación, active la promoción automática.

- Antes de actualizar dispositivos gestionados, asegúrese de leer las consideraciones importantes de actualización (consulte [Consideraciones sobre la actualización de firmware](#) en la documentación en línea de XClarity Administrator).
- Antes de actualizar los gestores de recursos de XClarity Administrator, asegúrese de leer las consideraciones sobre la actualización para XClarity Administrator (consulte [Actualización del servidor de gestión de XClarity Administrator](#) en la documentación en línea de XClarity Administrator).
- Antes de actualizar los gestores de recursos de XClarity Administrator, realice una copia de seguridad del dispositivo virtual mediante la creación de una clonación (consulte [Creación de copias de seguridad de XClarity Administrator](#) en la documentación en línea de XClarity Administrator).
- Asegúrese de que los recursos que desee actualizar tengan una política de cumplimiento de actualización asignada.

- XClarity Orchestrator transfiere las actualizaciones aplicables al gestor de recursos durante el proceso de actualización. Asegúrese de que haya suficiente espacio en el servidor de gestión para contener las actualizaciones.
- Para dispositivos del cliente ThinkEdge, solo se admiten las actualizaciones de la BIOS en servidores que ejecuten Windows 10, versión 1809, o versiones posteriores de sistemas operativos de 64 bits. Actualmente no se admiten las ediciones especiales (como 10 S o 10x).
- No puede descargar actualizaciones de firmware para los siguientes servidores desde la interfaz web. En su lugar, descargue manualmente las actualizaciones desde ibm.com y, a continuación, importe las actualizaciones.
 - IBM System x iDataPlex dx360 M4
 - IBM System serie M4
 - IBM System x3100 M5 y x3250 M
 - IBM System x3850 X5 y x3950 X5
 - IBM System x3850 X6 y x3950 X6
 - IBM Flex System

Consideraciones del repositorio

- Asegúrese de que el repositorio de actualizaciones contiene los paquetes de actualización que desea aplicar. De lo contrario, actualice el catálogo de productos y descargue las actualizaciones adecuadas (consulte [Descarga e importación de actualizaciones](#)). Puede instalar las actualizaciones de requisito previo además de la actualización de destino. Debe descargar todos los requisitos previos de la actualización en el repositorio antes de se puedan aplicar.

En algunos casos, se pueden necesitar varias versiones para aplicar una actualización y todas las versiones se deberán descargar en el repositorio.

Consideraciones sobre el proceso de actualización

- Si elige instalar un paquete de actualización que contiene actualizaciones para varios componentes, se actualizan todos los componentes a los que se aplica dicho paquete de actualización.
- Cuando se realiza una solicitud para aplicar actualizaciones a un gestor de recursos y a uno o varios dispositivos gestionados por ese gestor de recursos, las actualizaciones se aplican primero al gestor de recursos.
- Mientras hay una actualización en progreso, el recurso de destino permanece bloqueado. No puede iniciar otras tareas de gestión en el recurso de destino hasta que se complete el proceso de actualización.
- Después de aplicar una actualización a un recurso, pueden ser necesarios uno o varios reinicios para activar completamente la actualización. Puede elegir si el recurso se reinicia inmediatamente o diferir la activación o priorizar la activación. Si elige reiniciar inmediatamente, XClarity Orchestrator reduce a un mínimo el número de reinicios necesarios. Si elige diferir la activación, las actualizaciones se activan la próxima vez que el recurso 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.
- Si elige reiniciar el recurso 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 recurso.
- Algunas actualizaciones de firmware requieren que un monitor esté conectado al dispositivo de destino. El proceso de actualización puede producir un error si un monitor no está conectado.

Descarga e importación de actualizaciones

Los paquetes de actualización deben estar disponibles en el repositorio de actualizaciones de antes de poder aplicar actualizaciones a los recursos gestionados.

Antes de empezar

Para recuperar la información más reciente acerca de los paquetes de actualización, seleccione el tipo de recurso y, a continuación, haga clic en **Buscar actualizaciones → Actualizar selección** para obtener información acerca de todos los paquetes de actualización disponibles o haga clic en **Buscar actualizaciones → Actualizar selección: solo más recientes** para obtener información sobre solo el paquete de actualización más reciente para ese recurso. A continuación, ordene la tabla utilizando la columna **Nombre** para ordenar las actualizaciones por versión.

XClarity Orchestrator utiliza una unidad independiente para el repositorio de actualizaciones. El requisito de tamaño mínimo para esta unidad es de 100 GB.

Acerca de esta tarea

Puede descargar o importar un único paquete de repositorio de XClarity Administrator o uno o más paquetes de actualización a la vez.







- **Paquetes de repositorio de XClarity Administrator** Los paquetes de repositorio de Lenovo XClarity Administrator contienen las actualizaciones de firmware más recientes disponibles en un punto específico en el tiempo para la mayoría de dispositivos admitidos y una política de cumplimiento de firmware actualizada predeterminada. Cuando se descarga un paquete de repositorio desde la [Página web de descarga de XClarity Administrator](#), cada paquete de actualización del paquete de repositorio se extrae e importa al repositorio de actualizaciones y, a continuación, se elimina el archivo de carga del repositorio. La política de cumplimiento de firmware predeterminada actualizada también se importa como una política predefinida. No puede modificar esta política predefinida.


Los siguientes paquetes de repositorio están disponibles.

- **Invgy_sw_lxca_cmmswitchrepo***x-x.x.x_anyos_noarch*. Contiene las actualizaciones de firmware para todos los CMM y conmutadores Flex System.
- **Invgy_sw_lxca_storagerackswitchrepo***x-x.x.x_anyos_noarch*. Contiene las actualizaciones de firmware para todos los conmutadores RackSwitch y dispositivos Lenovo Storage.
- **Invgy_sw_lxca_systemxrepo***x-x.x.x_anyos_noarch*. Contiene las actualizaciones de firmware para todos los servidores serie Converged HX, Flex System y System x.
- **Invgy_sw_thinksystemrepo***x-x.x.x_anyos_noarch*. Contiene actualizaciones de firmware para todos los servidores ThinkSystem.
- **Invgy_sw_lxca_thinksystemv2repo***x-x.x.x_anyos_noarch*. Contiene actualizaciones de firmware para todos los servidores ThinkSystem V2.
- **Invgy_sw_lxca_thinksystemv3repo***x-x.x.x_anyos_noarc*. Contiene actualizaciones de firmware para todos los servidores ThinkAgile y ThinkSystem V3.

Cuando importe manualmente los paquetes del repositorio, debe importar la carga útil (.tgz), los metadatos (.xml), el registro de cambios (.chg) y el archivo léame (.txt).

Puede determinar el estado de un paquete de repositorio en la columna **Estado** de la página Gestión de repositorios. Esta columna contiene los siguientes valores.

-  **No descargado**. El paquete de repositorio está disponible en la web, pero no se descarga ni se extrae al repositorio de actualizaciones.
-  **Descarga pendiente**. El paquete de repositorio está en cola para su descarga desde Internet.
-  **Descargando**. El paquete de repositorio se está descargando desde Internet.
-  **Aplicación pendiente**. El paquete de repositorio está en cola para extraer los paquetes de actualización del paquete de repositorio al repositorio de actualizaciones.
-  **Aplicando**. Los paquetes de actualización en el paquete de repositorio se extraen al repositorio de actualizaciones.
-  **x de y Descargado**. Algunos paquetes de repositorio, pero no todos, se descargan y se extraen al repositorio de actualizaciones. Los números entre paréntesis indican el número de actualizaciones descargadas y el número de actualizaciones disponibles.

-  **Descargado.** Todos los paquetes de actualización en el paquete de repositorio se almacenan en el repositorio de actualizaciones y el archivo de carga del paquete de repositorio se elimina.
- **Paquetes de actualización** Si XClarity Orchestrator está conectado a Internet, puede descargar los paquetes de actualización que se enumeran en el catálogo de actualizaciones directamente desde el sitio web de soporte de Lenovo. Si XClarity Orchestrator no está conectado a Internet, puede importar manualmente los paquetes de actualización que descargó anteriormente desde el [Sitio web del Soporte del Centro de Datos de Lenovo](#) a una estación de trabajo que disponga de acceso de red para el host de XClarity Orchestrator.






Si elige descargar una versión menor, también se descargan los paquetes de actualización de requisitos previos.

Cuando importe manualmente las actualizaciones, deberá importar los archivos requeridos en función del tipo de recurso.

- Para servidores ThinkSystem V3, importe el paquete de actualización único (*.zip). Este archivo zip contiene la carga útil, los archivos de metadatos (varios archivos *.json), el archivo de registro de cambios (*.chg) y el archivo Léame (*.txt).
- Para dispositivos del cliente ThinkEdge, importe la carga útil (Windows .exe). El archivo Léame (.txt) es opcional. Tenga en cuenta que, actualmente, solo se admite la actualización del **paquete de la utilidad flash BIOS para Windows**.
- Para XClarity Management Hub y XClarity Management Hub 2.0, importe el archivo de paquete de actualización único (.tgz). Este archivo contiene la carga útil, metadatos, historial de cambios y los archivos léame.
- Para el resto de recursos (incluido XClarity Administrator, servidores ThinkEdge, ThinkSystem V1 y V2, y dispositivos heredados), importe la carga útil (.zip, .uxz, .tar.gz, .tar, .bin), los metadatos (.xml), el registro de cambios (.chg) y el archivo Léame (.txt).

Importante: El tamaño máximo de todos los archivos que se deben importar al mismo tiempo es de 8 GB.

Puede utilizar la columna **Estado** de la página Gestión de repositorio para determinar si los archivos de actualización específicos deben almacenarse en el repositorio de actualizaciones. Esta columna contiene los siguientes valores.

-  **No descargado.** El paquete de actualización completo o la actualización individual están disponibles desde la web pero actualmente no se almacenan en el repositorio.
-  **Descarga pendiente.** El paquete de actualización está en cola para su descarga desde Internet.
-  **Descargando.** El paquete de actualización se está descargando desde Internet.
-  **x de y Descargado.** Algunas de las actualizaciones del paquete de actualización se almacenan en el repositorio, pero no todas. Los números entre paréntesis indican el número de actualizaciones almacenadas y el número de actualizaciones disponibles.
-  **Descargado.** El paquete de actualizaciones completo o cada actualización se almacenan en el repositorio.

Nota: Varias plataformas utilizan algunos paquetes de actualización. Si selecciona un paquete de actualización en la tabla, se selecciona en cada plataforma que lo usa.

Procedimiento

Para descargar o importar manualmente paquetes de actualización y paquetes de repositorio, lleve a cabo uno de los pasos siguientes.

- Si XClarity Orchestrator está conectado a Internet, descargue los paquetes de actualización que se enumeran en el catálogo.

1. En la barra de menús de XClarity Orchestrator, haga clic en **Aprovisionamiento** (🔒) → **Actualizaciones** y luego haga clic en **Gestión de repositorio** para mostrar la tarjeta Gestión de repositorio. La tarjeta Gestión del repositorio muestra información acerca de los paquetes de actualización en una estructura de árbol organizada por tipos de recursos, componentes y paquetes de actualización. De forma predeterminada, los tipos de recursos para solo los recursos *gestionados* se enumeran en la tabla. Haga clic en **Mostrar tipos de recursos disponibles** para ver todos los tipos de *recursos admitidos* que están disponibles en el catálogo.

Gestión de repositorio

Gestionar el repositorio de actualizaciones, incluyendo la importación de paquetes de actualización del sistema local y la descarga de la información del catálogo y la actualización de paquetes desde Internet. Actualice el catálogo para recuperar la información más reciente antes de descargar paquetes de actualización.

Uso de repositorio: 18.2 GB de 93.2 GB.

🔔 Si el paquete seleccionado es una versión menor, también se descargarán los paquetes de actualización de requisitos previos. ✕

Mostrar solo los tipos de recurso gestionados ▾ 🔍 Buscar ✕

🔄 ☰ ⬇️ 📄 🗑️ Actualizar catálogo ▾ ➡️ Todas las acciones ▾ Filtros ▾

<input type="checkbox"/>	Nombre	Tipo de	Versión	Fecha	Estado	Tamaño	Notas
<input type="checkbox"/>	› IBM Flex System x220 Compute Node		79...		📦...	77...	
<input type="checkbox"/>	› IBM Flex System x222 Compute Node		79...		📦...	65...	
<input type="checkbox"/>	› IBM Flex System x240 Compute Node		87...		📦...	1...	
<input type="checkbox"/>	› IBM Flex System x280/x480/x880 X6 Compute Node		79...		📦...	1...	
<input type="checkbox"/>	› IBM Flex System x440 Compute Node		79...		📦...	85...	
<input type="checkbox"/>	› Lenovo Converged HX5510/HX5510-C/HX3510-G/HX7		86...		📦...	5...	
<input type="checkbox"/>	› Lenovo Devices Repository Pack		Re...		📦...	27...	
<input type="checkbox"/>	› Lenovo Flex System x240 Compute Node		71...		📦...	6...	
<input type="checkbox"/>	› Lenovo Flex System x240 M5 Compute Node		95...		📦...	6...	
<input type="checkbox"/>	› Lenovo Flex System x280/x480/x880 X6 Compute Node		71...		📦...	6...	

0 Seleccionado / 14 Total Filas por página: 10 ▾

⏪ < 1 2 > ⏩

2. (Opcional) Seleccione uno o más tipos de recursos en la tabla, haga clic en **Buscar actualizaciones** y en una de las siguientes opciones para descargar información sobre las últimas actualizaciones disponibles para los tipos de recursos específicos.
 - **Actualizar selección.** Permite recuperar información acerca de todas las versiones de actualizaciones que están disponibles para el recurso seleccionado.
 - **Actualizar selección: Solo reciente.** Permite recuperar información acerca de la versión de actualización más actual que está disponible para el recurso seleccionado. Para dispositivos del cliente ThinkEdge, solo se admite **Actualizar selección: Solo reciente.**

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

3. Seleccione uno o más paquetes de repositorio, recursos, componentes y versiones de actualización que desee descargar. Puede expandir los tipos de recursos y los componentes para mostrar la lista de versiones de actualización que están disponibles en el catálogo para cada tipo de recurso y componente.
4. Haga clic en el icono **Descargar actualizaciones** (⬇️) para descargar las actualizaciones seleccionadas. Se crea un trabajo para llevar a cabo esta operación. Puede supervisar el progreso del trabajo desde la tarjeta **Supervisión** (📊) → **Trabajos**. Si el trabajo no finalizó correctamente, haga clic en el enlace del trabajo para mostrar los detalles correspondientes (consulte .)

Una vez completada la descarga, el área **Estado de descarga** para las actualizaciones seleccionadas cambia a “Descargado”.

- Si XClarity Orchestrator no está conectado a Internet, importe manualmente los paquetes de actualización y paquetes de repositorio.
 1. Descargue los archivos para cada paquete de repositorio y paquete de actualización en una estación de trabajo que tenga acceso al host de XClarity Orchestrator mediante un navegador web. Utilice estos vínculos para descargar las actualizaciones aplicables.
 - Para actualizaciones de Lenovo XClarity Administrator, vaya a [Página web de descarga de XClarity Administrator](#). También puede descargar actualizaciones de XClarity Administrator mediante los comandos Lenovo XClarity Essentials OneCLI. El siguiente ejemplo descarga la actualización más reciente (incluida la carga útil) en el directorio /lxca-updates y almacena los archivos de registro en el directorio /logs/lxca-updates. Para obtener más información sobre OneCLI, consulte [Comando acquire](#) en la documentación en línea de Lenovo XClarity Essentials OneCLI.

```
Onecli.exe update acquire --lxca --ostype none --mt lxca --scope latest --superseded --xml --dir ./lxca-updates --output ./logs/lxca-updates
```
 - Para paquetes del repositorio de actualizaciones de firmware, vaya a [Página web de descarga de XClarity Administrator](#).
 - Para actualizaciones de firmware, vaya a [Sitio web del Soporte del Centro de Datos de Lenovo](#).
 2. En la barra de menú de XClarity Orchestrator, haga clic en **Aprovisionamiento** (🔧) → **Actualizaciones** y luego haga clic en **Gestión de repositorio** para mostrar la tarjeta Gestión de repositorio.
 3. Haga clic en el icono **Importar** (📁) para mostrar el cuadro de diálogo Importar actualizaciones.
 4. Arrastre los archivos descargados y suéltelos en el cuadro de diálogo Importar, o bien haga clic en **Examinar** para ubicar los archivos.

Atención:

- Para dispositivos del cliente ThinkEdge, debe importar el archivo de carga útil para cada paquete de actualización. El archivo léame es opcional.
- Para todos los demás dispositivos, debe importar el archivo de metadatos así como el archivo de imágenes o de carga útil, el archivo de historial de cambios y el archivo léame para cada paquete de repositorio y paquete de 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.
- No importe otros archivos que puedan encontrarse en los sitios web de descarga de Lenovo.
- Si no incluye el archivo de metadatos (.xml o .json) para el paquete de repositorio o el paquete de actualización, no se importa el paquete de repositorio ni el paquete de actualización.

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

Cuando los archivos se importan y almacenan en el repositorio, la columna **Estado de descarga** cambia a “Descargado”.

Después de finalizar

Puede realizar las siguientes acciones desde la tarjeta Gestión de repositorio.

- Revise el archivo Léame, el archivo de historial de cambios y una lista de vulnerabilidades y exposiciones comunes (CVE) corregidas para una actualización específica haciendo clic en el icono de información (ℹ️) en la columna **Notas de la versión**. También puede encontrar una lista de CVE corregidas colocando el cursor por encima de la columna **CVE corregidas**. Haga clic en la ID de CVE para ver información detallada sobre la CVE desde el sitio web National Vulnerability Data.

Las columnas **Notas de la versión** y **CVE corregidas** están ocultas de manera predeterminada. Para mostrar estas columnas en la tabla, haga clic en **Todas las acciones** → **Alternar columnas**.

- Elimine solo el archivo de imagen (carga útil) para cada actualización seleccionada al hacer clic en el icono **Eliminar únicamente los archivos de carga útil** (🗑️). La información acerca de la actualización (el archivo de metadatos XML) permanece en el repositorio y el estado de descarga cambia a “No descargado”.

Importante:

- La carga útil de los paquetes de repositorio se elimina automáticamente después de extraer los paquetes de actualización durante el proceso de descarga o importación.
- No es posible eliminar los archivos de carga útil desde paquetes de actualización que se encuentren en uso en políticas de conformidad de actualización. En primer lugar, debe quitar el paquete de actualización de las políticas (consulte [Creación y asignación de políticas de conformidad de actualización](#)).
- Algunos paquetes de actualización son comunes para varias plataformas y componentes. La eliminación de un paquete de actualización común afecta a todas las plataformas y componentes que lo utilizan.

Creación y asignación de políticas de conformidad de actualización

Puede crear una política de cumplimiento de actualización basada en las actualizaciones adquiridas en el repositorio de actualizaciones. Luego puede asignar la política a uno o varios gestores de recursos o servidores gestionados.

Antes de empezar

Al crear una política de cumplimiento de actualización, debe seleccionar la versión de actualización de destino que se va a aplicar a los recursos que se van a asignar a la política. Asegúrese de que los archivos de actualización para la versión de destino estén en el repositorio de actualizaciones antes de crear la política.

Cuando descargue o importe un paquete de repositorio de actualización de firmware, las políticas de cumplimiento de firmware predefinidas en el paquete de repositorio se agregan al repositorio de actualización. Esto se considera una *política predefinida*, que no se puede modificar ni eliminar.

Acerca de esta tarea

Las *políticas de cumplimiento de actualización* garantizan que el software o firmware de determinados recursos gestionados se encuentran en el nivel actual o especificado marcando los recursos que necesitan atención. Cada política de cumplimiento de actualización identifica qué recursos se supervisan y el nivel de software o firmware que debe instalarse a fin de mantener el cumplimiento de los recursos. XClarity Orchestrator utiliza estas políticas para comprobar el estado de los recursos gestionados e identificar los recursos que están fuera de cumplimiento.

Al crear una política de cumplimiento de actualización, puede elegir que XClarity Orchestrator marque un recurso cuando el software o firmware en el recurso sea de nivel inferior.


Una vez que se asigna una política de cumplimiento de actualización a un recurso, XClarity Orchestrator comprueba el estado de conformidad del recurso cuando cambia el repositorio de actualizaciones. Si el software o el firmware en el recurso no está en cumplimiento con la política de conformidad asignada, XClarity Orchestrator marca ese recurso como que no está en cumplimiento en la página Aplicar/Activar, según las reglas que ha especificado en la política de cumplimiento.

Por ejemplo, puede crear una política de conformidad de actualización que defina el nivel de línea base para el software para XClarity Administrator y, a continuación, asignar esa política de conformidad a todos los gestores de recursos de XClarity Administrator. Cuando se actualiza el catálogo de actualizaciones y cuando se descargan o importan nuevas actualizaciones, es posible que instancias de XClarity Administrator queden fuera de conformidad. Si esto ocurre, XClarity Orchestrator actualiza la página Aplicar/Activar para mostrar cuáles instancias de XClarity Administrator no son conformes y genera una alerta.

Procedimiento

Para crear y asignar una política de cumplimiento de actualización, lleve a cabo los pasos siguientes.

Paso 1. Cree una política de cumplimiento de actualización.

1. En la barra de menús de XClarity Orchestrator, haga clic en **Aprovisionamiento**  → **Actualizaciones** y, a continuación, haga clic en **Gestión de políticas** para mostrar la tarjeta de Gestión de políticas.

Gestión de política

La gestión de política permite crear o modificar una política en función de las actualizaciones adquiridas en el repositorio de firmware.

ⓘ No puede editar o eliminar una política de cumplimiento que esté asignada. ✕

🔄 + 🗑️ ✎ 📄 📄 Todas las acciones ▾ Filtros ▾ 🔍 Buscar ✕

<input type="checkbox"/>	Nombre de la política	Estado de uso	Origen de la política	Última modificación	Descripción
<input type="checkbox"/>	ThinkAgile_VX_0...	← No asignado	👤 Definido por ...	4/10/22 17:08	ThinkAgile VX M...
<input type="checkbox"/>	v2.6.0-2020-01-...	→ Asignado	👤 Definido por ...	4/10/22 17:23	Production firmw...
<input type="checkbox"/>	v3.2.0-2021-07-...	← No asignado	👤 Definido por ...	4/10/22 17:34	Production firmw...
<input type="checkbox"/>	v3.6.0-2022-06-...	← No asignado	👤 Definido por ...	4/10/22 17:42	Production firmw...
<input type="checkbox"/>	ThinkAgile-VX-Se...	← No asignado	👤 Definido por ...	4/10/22 17:54	System and Com...
<input type="checkbox"/>	ThinkAgile-VX-Se...	← No asignado	👤 Definido por ...	4/10/22 18:07	System and Com...
<input type="checkbox"/>	v3.6.0-2022-06-...	← No asignado	👤 Definido por ...	4/10/22 18:25	Production firmw...
<input type="checkbox"/>	v3.6.0-2022-06-...	← No asignado	👤 Definido por ...	4/10/22 18:33	Production firmw...
<input type="checkbox"/>	v2.6.0-2019-12-...	← No asignado	👤 Definido por ...	4/10/22 18:41	Production firmw...

0 Seleccionado / 9 Total Filas por página: 10 ▾

2. Haga clic en el icono **Crear** (+) para abrir el cuadro de diálogo Crear política de cumplimiento.
3. Especifique el nombre y descripción opcional de la política.
4. Especifique el desencadenador de la política. Puede presentar uno de los valores siguientes.
 - **Marcar si no hay coincidencia exacta.** Si la versión de software o firmware que está instalada en el recurso es *anterior o posterior* a la versión de firmware de destino en la política de cumplimiento de actualizaciones, el recurso se etiqueta como no conforme. Por ejemplo, si sustituye un adaptador de red en un servidor y el firmware en dicho adaptador de red es distinto de la versión de firmware de destino en la política de cumplimiento de actualización, el servidor se marca como No conforme.
 - **No marcar.** Recursos que no se ajustan a la conformidad no se marcan.
5. Haga clic en la pestaña **Reglas** para añadir reglas de conformidad para esta política.
 - a. Seleccione el tipo de recurso para esta política.
 - b. Especifique el objetivo de cumplimiento para los recursos y componentes aplicables. Para los recursos con componentes, puede elegir uno de los siguientes valores.
 - **Personalizado.** El destino de conformidad de cada componente de recurso tiene la configuración predeterminada de la versión más reciente actual del repositorio para dicho componente.
 - **No actualizar.** El objetivo de cumplimiento para cada componente de recurso usa el valor predeterminado de **No actualizar**. Tenga en cuenta que si cambia el valor predeterminado para cualquier componente, el objetivo de conformidad para el recurso general cambia a **Personalizado**. Para los recursos sin componentes y para cada componente, puede elegir uno de los siguientes valores.

- *{firmware_level}*. Especifica que el firmware del componente debe encontrarse en la versión de firmware de línea base seleccionada.
- **No actualizar**. Especifica que el firmware del componente no se va a actualizar. Tenga en cuenta que el firmware en el controlador de gestión de respaldo (secundario) no se actualiza de forma predeterminada.

c. Haga clic en el icono **Añadir** (+) para añadir reglas adicionales y, a continuación, haga clic en el icono **Eliminar** (III) para eliminar las reglas.

6. Haga clic en **Crear**.

Paso 2. En la barra de menús de XClarity Orchestrator, haga clic en **Aprovisionamiento** (☰) → **Actualizaciones** y luego haga clic en **Aplicar y activar** para mostrar la tarjeta Aplicar y activar.

Paso 3. Asigne la política de conformidad de actualización a los recursos.

- **A un solo recurso** Para cada recurso, seleccione una política desde la lista desplegable en la columna **Política de cumplimiento asignada**.

Puede seleccionar de una lista de políticas de cumplimiento que sean aplicables al recurso. Si actualmente una política no está asignada al recurso, la política asignada se establece en **Sin asignación**. Si ninguna política es aplicable al recurso, la política asignada se establece en **No hay políticas aplicables**.

- **A varios recursos**

1. Seleccione uno o varios recursos a los que desee asignar la política.
2. Haga clic en el icono **Asignar política** (E+) para mostrar el cuadro de diálogo Asignar política.
3. Seleccione la política que desee asignar. Puede seleccionar de una lista de políticas de cumplimiento que sean aplicables a todos los recursos seleccionados. Si actualmente una política no está asignada al recurso, la política asignada se establece en **Sin asignación**. Si ninguna política es aplicable al recurso, la política asignada se establece en **No hay políticas aplicables**. Si no se seleccionaron recursos antes de abrir el cuadro de diálogo, se enumeran todas las políticas.

Nota: Seleccione **Sin asignación** para quitar la asignación de la política del recurso seleccionado.

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 política.
 - **Sin una política asignada**
 - **No conforme (sobrescriba la política asignada actual)**
 - **Conforme (sobrescriba la política asignada actual)**
6. Haga clic en **Aplicar**. 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.

- **Para grupos de recursos**

1. Haga clic en el icono **Asignar política** (E+) para mostrar el cuadro de diálogo Asignar política.
2. Seleccione la política que desee asignar. Puede seleccionar de una lista de políticas de cumplimiento que sean aplicables a todos los recursos del grupo. Si actualmente una política no está asignada al recurso, la política asignada se establece en **Sin asignación**. Si

ninguna política es aplicable al recurso, la política asignada se establece en **No hay políticas aplicables**.

Nota: Seleccione **Sin asignación** para quitar la asignación de la política de los recursos del grupo.

3. Seleccione uno o más grupos de recursos a los que desee asignar la política.
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 política.
 - **Sin una política asignada**
 - **No conforme (sobrescriba la política asignada actual)**
 - **Conforme (sobrescriba la política asignada actual)**
6. Haga clic en **Aplicar**. 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

Puede realizar las siguientes acciones desde la tarjeta Gestión de política.

- Vea los detalles de la política haciendo clic en la fila de la tabla.
- Modifique una política seleccionada haciendo clic en el icono **Editar** (✎).

Nota: No puede modificar una política que esté asignada a uno o varios recursos. Primero debe cancelar la asignación de la política.

- Para copiar y modificar una política seleccionada, haga clic en el ícono **Copiar** (📄).
- Elimine una política *definida por usuario* seleccionada haciendo clic en el icono **Eliminar** (🗑).

Nota: No puede eliminar una política que esté asignada a uno o varios recursos. Primero debe desasignar la política.

En la tarjeta Aplicar y activar, puede cancelar la asignación de una política para un recurso seleccionado al hacer clic en el icono de **Asignar** (📌), seleccionar la política **Sin asignación** y seleccionar si desea aplicar el cambio a todos los recursos con una asignación de política o solo a los recursos seleccionados.

Aplicar y activar actualizaciones a los gestores de recursos

XClarity Orchestrator no aplica automáticamente las actualizaciones. Para actualizar el software, debe aplicar y activar manualmente la actualización en los gestores de recursos Lenovo XClarity Administrator seleccionados que no cumplen con la política de conformidad de actualización asignada.

Antes de empezar

Antes de intentar aplicar y activar las actualizaciones en cualquier recurso, asegúrese de leer las consideraciones de la actualización (consulte [Consideraciones de actualización](#)).

Asegúrese de que se asigne una política de conformidad de actualización al recurso de destino (consulte [Creación y asignación de políticas de conformidad de actualización](#)).

No se puede aplicar una actualización del mismo nivel de software o de una versión anterior a la que está instalada en la actualidad.

Acerca de esta tarea

Puede aplicar actualizaciones de firmware a los gestores de recursos de XClarity Administrator que tienen asignada una política de cumplimiento de actualización y no la cumplen. Puede actualizar el software de las formas siguientes.

- Para gestores específicos que no están en cumplimiento
- Para todos los gestores que no están en cumplimiento en grupos específicos
- Para todos los gestores que no están en cumplimiento a los que se les asigna una política de cumplimiento de actualización específica
- Para todos los gestores que no están en cumplimiento en grupos específicos a los que se les asigna una política de cumplimiento de actualización específica
- Para todos los gestores que no están en cumplimiento y que están asignados a cualquier política pero lo cumplen

XClarity Orchestrator no actualiza los recursos directamente. En su lugar, envía una solicitud al gestor de recursos aplicable para realizar la actualización y, a continuación, realiza un seguimiento del progreso de la solicitud. XClarity Orchestrator identifica las dependencias que se requieren para realizar la actualización, garantiza que los recursos de destino se actualicen en el orden correcto, transfiere los paquetes de actualización aplicables al gestor de recursos y crea una solicitud para iniciar un trabajo en el gestor de recursos para realizar la actualización.

Durante el proceso de actualización, el recurso de destino 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 recurso de destino antes de continuar.

Si se produce un error al actualizar alguno de los componentes en un recurso de destino, el proceso de actualización del firmware no actualiza ese componente. En cambio, el proceso de actualización de otros componentes en el recurso y continúa actualizando el resto de recursos de destino en el trabajo de actualización actual.

Las actualizaciones de requisitos previos no se aplican automáticamente.

Consejo:

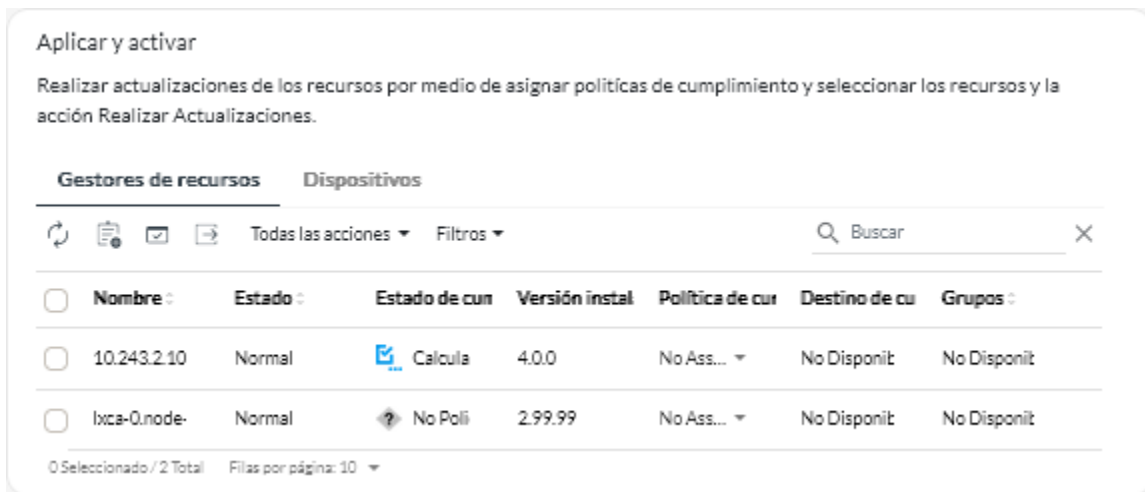
- La tabla enumera únicamente los gestores de recursos que se pueden actualizar.
- Las columnas **Número de Build** y **Número de Build de destino de conformidad** están ocultas en la vista de forma predeterminada. Puede mostrar estas columnas haciendo clic en **Todas las acciones** → **Alternar columnas**.

Procedimiento

Para aplicar actualizaciones a los gestores de recursos de XClarity Orchestrator, lleve a cabo uno de los siguientes procedimientos.

- **Para gestores de recursos específicos que no están en cumplimiento**

1. En la barra de menús de XClarity Orchestrator, haga clic en **Aprovisionamiento** (🔒) → **Actualizaciones** y, a continuación, haga clic en **Aplicar y activar** para mostrar la tarjeta de Aplicar y activar.



2. Haga clic en la pestaña **Gestores de recursos**.
 3. Seleccione uno o varios gestores de recursos a los que desee aplicar actualizaciones.
 4. Haga clic en el icono de **Aplicar actualizaciones** (📄) para mostrar el cuadro de diálogo Resumen de actualización.
 5. Haga clic en **Realizar actualizaciones** para aplicar las actualizaciones. Se crea un trabajo para llevar a cabo esta operación. Puede supervisar el progreso del trabajo desde la tarjeta **Supervisión** (📄) → **Trabajos**. Si el trabajo no finalizó correctamente, haga clic en el enlace del trabajo para mostrar los detalles correspondientes (consulte .)
- **Para todos los gestores de recursos que no están en cumplimiento en grupos específicos o que se les asigna una política de cumplimiento de actualización específica**
 1. En la barra de menús de XClarity Orchestrator, haga clic en **Aprovisionamiento** (🔑) → **Actualizaciones** y luego haga clic en **Aplicar y activar** para mostrar la tarjeta Aplicar y activar.
 2. Haga clic en la pestaña **Gestores de recursos**.
 3. Haga clic en el icono de **Aplicar actualizaciones** (📄) para mostrar el cuadro de diálogo Resumen de actualización.
 4. Seleccione los grupos y la política de cumplimiento de actualización.
 - Si no selecciona una política o un grupo, se actualizan todos los gestores que tienen una política asignada y que no están en cumplimiento con ella.
 - Si selecciona una política pero no un grupo, se actualizan todos los gestores que están asignados a esa política y que no están en cumplimiento con ella.
 - Si selecciona uno o más grupos y no una política, se actualizan todos los gestores en el grupo que no están en cumplimiento con la política asignada.
 - Si selecciona una política y uno o más grupos, se actualizan todos los gestores en el grupo que están asignados a esa política y que no están en cumplimiento con ella.
 5. Haga clic en **Realizar actualizaciones** para aplicar las actualizaciones. Se crea un trabajo para llevar a cabo esta operación. Puede supervisar el progreso del trabajo desde la tarjeta **Supervisión** (📄) → **Trabajos**. Si el trabajo no finalizó correctamente, haga clic en el enlace del trabajo para mostrar los detalles correspondientes (consulte .)

Aplicar y activar actualizaciones a los servidores gestionados

Lenovo XClarity Orchestrator no aplica automáticamente las actualizaciones. Para actualizar el firmware, debe aplicar y activar manualmente la actualización en los dispositivos seleccionados que no cumplen con la política de conformidad de actualización asignada.

Antes de empezar

Antes de intentar aplicar y activar las actualizaciones en cualquier dispositivo, asegúrese de leer las consideraciones de la actualización (consulte [Consideraciones de actualización](#)).

Asegúrese de que se asigne una política de conformidad de actualización al dispositivo de destino (consulte [Creación y asignación de políticas de conformidad de actualización](#)).

Puede aplicar actualizaciones de firmware solo a servidores gestionados.

Cuando actualice el firmware en muchos dispositivos a la vez, use XClarity Orchestrator versión 1.3.1 o posterior y Lenovo XClarity Administrator versión 3.2.1 o posterior para tener un mejor rendimiento.

Acerca de esta tarea

Puede aplicar actualizaciones de firmware a los dispositivos que tienen asignada una política de cumplimiento de actualización y no la cumplen. Puede actualizar el firmware de las formas siguientes.

- Para dispositivos específicos que no están en cumplimiento
- Para todos los dispositivos que no están en cumplimiento en grupos específicos
- Para todos los dispositivos que no están en cumplimiento a los que se les asigna una política de cumplimiento de actualización específica
- Para todos los dispositivos que no están en cumplimiento en grupos específicos a los que se les asigna una política de cumplimiento de actualización específica
- Para todos los dispositivos que no están en cumplimiento y que están asignados a cualquier política pero lo la cumplen

Un servidor se marca como No conforme cuando la versión de firmware instalada de uno o más componentes es *anterior o posterior* a la versión de firmware de destino en la política de cumplimiento de actualizaciones. Si la versión de firmware instalada es *posterior* a la versión de firmware de destino, debe seleccionar la opción **Forzar la actualización** cuando aplique la actualización para actualizar a una versión anterior del firmware en los componentes. Si la opción **Forzar la actualización** no está seleccionada, solo se aplican las versiones de firmware de destino posteriores a las versiones instaladas.

Nota: Solo ciertas opciones de dispositivos, adaptadores y unidades admiten la versión a la baja. Consulte la documentación del hardware para determinar si se admiten versiones anteriores.

XClarity Orchestrator no actualiza los recursos directamente. En su lugar, envía una solicitud al gestor de recursos aplicable para realizar la actualización y, a continuación, realiza un seguimiento del progreso de la solicitud. XClarity Orchestrator identifica las dependencias que se requieren para realizar la actualización, garantiza que los recursos de destino se actualicen en el orden correcto, transfiere los paquetes de actualización aplicables al gestor de recursos y crea una solicitud para iniciar un trabajo en el gestor de recursos para realizar la actualización.

Durante el proceso de actualización, el dispositivo de destino 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 de destino antes de continuar.

Si se produce un error al actualizar alguno de los componentes en un dispositivo de destino, el proceso de actualización del firmware no actualiza ese componente. En cambio, el proceso de actualización de otros componentes en el dispositivo y continúa actualizando el resto de dispositivos de destino en el trabajo de actualización actual.

Las actualizaciones de requisitos previos no se aplican automáticamente.

Sugerencias:

- La tabla enumera únicamente los dispositivos que se pueden actualizar.
- Las columnas **Número de Build**, **Número de Build de destino de conformidad** y **Nombre de producto** están ocultas en la vista de forma predeterminada. Puede mostrar estas columnas haciendo clic en **Todas las acciones** → **Alternar columnas**.
- Para servidores ThinkSystem SR635, SR645, SR655 y SR665, para aplicar firmware en banda y fuera de banda, aplique primero las actualizaciones a los controladores de gestión de la placa base y, a continuación, aplique las actualizaciones de firmware a las opciones restantes.

Procedimiento

Para aplicar actualizaciones a los dispositivos gestionados, lleve a cabo uno de los siguientes procedimientos.

• Para dispositivos específicos que no están en cumplimiento

1. En la barra de menú de XClarity Orchestrator, haga clic en **Aprovisionamiento** (🔗) → **Actualizaciones** y luego haga clic en **Aplicar y activar** para mostrar la tarjeta Aplicar y activar.
2. Haga clic en la pestaña **Dispositivos**.
3. Seleccione uno o varios dispositivos a los que desee aplicar actualizaciones.
4. Haga clic en el icono de **Aplicar actualizaciones** (☑) para mostrar el cuadro de diálogo Resumen de actualización.
5. Seleccione cuándo se activan las actualizaciones.
 - **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. Se produce un suceso cuando el estado cambia a modo de mantenimiento de firmware pendiente para notificarlo cuando se debe reiniciar el servidor.
 - **Activación con retardo.** Se realizan algunas de las operaciones de actualización, pero no todas ellas. Los dispositivos de destino se deben reiniciar manualmente para continuar con el proceso de actualización. Se realizan reinicios adicionales hasta que se completa la operación de actualización. Se produce un suceso cuando el estado cambia a modo de mantenimiento de firmware pendiente para notificarlo cuando se debe reiniciar el servidor.

Si un dispositivo de destino se reinicia por cualquier motivo, el proceso de actualización con retardo finaliza.

Importante:

- Utilice **Reiniciar normalmente** para reiniciar el servidor y continuar con el proceso de actualización. *No* utilice **Reiniciar de inmediato**.
- No elija Activación con retardo para más de 50 dispositivos al mismo tiempo. XClarity Orchestrator supervisa de forma activa los dispositivos con una activación con retardo, por lo que dicha activación se realiza cuando se reinicia un dispositivo. Si desea aplicar actualizaciones con activación con retardo para más de 50 dispositivos, divida la selección de actualizaciones en lotes de 50 dispositivos cada vez.
- **Activación inmediata.** Durante el proceso de actualización, el dispositivo de destino 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 de destino antes de continuar.

Notas:

- En el caso de servidores gestionados por XClarity Management Hub 2.0 y para dispositivos cliente ThinkEdge, solo se admite la activación inmediata, independientemente de la regla de activación que seleccione.
 - Cuando está habilitada, la opción de arranque de Wake on LAN puede interferir con las operaciones de Lenovo 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”.
6. **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.
 7. **Opcional:** seleccione **Programar actualización** para elegir la fecha y hora en la que desea que se ejecute la actualización de firmware. Si no se ha seleccionado, el firmware se actualiza de inmediato.
 8. Haga clic en **Realizar actualizaciones** para aplicar las actualizaciones. Se crea un trabajo para llevar a cabo esta operación. Puede supervisar el progreso del trabajo desde la tarjeta **Supervisión** (📊) → **Trabajos**. Si el trabajo no finalizó correctamente, haga clic en el enlace del trabajo para mostrar los detalles correspondientes (consulte .)
- **Para todos los dispositivos que no están en cumplimiento en grupos específicos a los que se les asigna una política de cumplimiento de actualización específica**
 1. En la barra de menús de XClarity Orchestrator, haga clic en **Aprovisionamiento** (🔒) → **Actualizaciones** y luego haga clic en **Aplicar y activar** para mostrar la tarjeta Aplicar y activar.
 2. Haga clic en la pestaña **Dispositivos**.
 3. Seleccione uno o más grupos de dispositivos a los que desee aplicar actualizaciones.
 4. Haga clic en el icono de **Aplicar actualizaciones** (☑️) para mostrar el cuadro de diálogo Resumen de actualización.
 5. Seleccione los grupos y la política de cumplimiento de actualización.
 - Si no selecciona una política o un grupo, se actualizan todos los dispositivos que tienen una política asignada y que no están en cumplimiento con ella.
 - Si selecciona una política pero no un grupo, se actualizan todos los dispositivos que están asignados a esa política y que no están en cumplimiento con ella.
 - Si selecciona uno o más grupos y no una política, se actualizan todos los dispositivos en el grupo que no están en cumplimiento con la política asignada.
 - Si selecciona una política y uno o más grupos, se actualizan todos los dispositivos en el grupo que están asignados a esa política y que no están en cumplimiento con ella.
 6. Seleccione cuándo se activan las actualizaciones.
 - **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. Se produce un suceso cuando el estado cambia a modo de mantenimiento de firmware pendiente para notificarlo cuando se debe reiniciar el servidor.
 - **Activación con retardo.** Se realizan algunas de las operaciones de actualización, pero no todas ellas. Los dispositivos de destino se deben reiniciar manualmente para continuar con el proceso de actualización. Se realizan reinicios adicionales hasta que se completa la operación de actualización. Se produce un suceso cuando el estado cambia a modo de mantenimiento de firmware pendiente para notificarlo cuando se debe reiniciar el servidor.

Si un dispositivo de destino se reinicia por cualquier motivo, el proceso de actualización con retardo finaliza.

Importante:

- Utilice **Reiniciar normalmente** para reiniciar el servidor y continuar con el proceso de actualización. *No utilice Reiniciar de inmediato.*
- No elija Activación con retardo para más de 50 dispositivos al mismo tiempo. XClarity Orchestrator supervisa de forma activa los dispositivos con una activación con retardo, por lo que dicha activación se realiza cuando se reinicia un dispositivo. Si desea aplicar actualizaciones con activación con retardo para más de 50 dispositivos, divida la selección de actualizaciones en lotes de 50 dispositivos cada vez.
- **Activación inmediata.** Durante el proceso de actualización, el dispositivo de destino 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 de destino antes de continuar.

Notas:

- En el caso de servidores gestionados por XClarity Management Hub 2.0 y para dispositivos cliente ThinkEdge, solo se admite la activación inmediata, independientemente de la regla de activación que seleccione.
 - Cuando está habilitada, la opción de arranque de Wake on LAN puede interferir con las operaciones de Lenovo 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”.
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.
 8. **Opcional:** seleccione **Programar actualización** para elegir la fecha y hora en la que desea que se ejecute la actualización de firmware. Si no se ha seleccionado, el firmware se actualiza de inmediato.
 9. Haga clic en **Realizar actualizaciones** para aplicar las actualizaciones. Se crea un trabajo para llevar a cabo esta operación. Puede supervisar el progreso del trabajo desde la tarjeta **Supervisión** (📧) → **Trabajos**. Si el trabajo no finalizó correctamente, haga clic en el enlace del trabajo para mostrar los detalles correspondientes (consulte .)

Después de finalizar

Puede llevar a cabo las siguientes acciones desde la tarjeta Patrones.

- Reenvía los informes sobre la conformidad del firmware de forma periódica a una o varias direcciones de correo electrónico haciendo clic en el icono **Crear despachador de informes** (⊕). El informe se envía utilizando los filtros de datos aplicados actualmente a la tabla. Todas las columnas de la tabla mostradas y ocultas se incluyen en el informe. Para obtener más información, consulte el apartado [Reenvío de informes](#).
- Añada un informe de cumplimiento de firmware a un despachador de informes específico utilizando los filtros de datos aplicados actualmente a la tabla haciendo clic en el icono de **Agregar a despachador de informes** (➔). Si el despachador de informes ya incluye un informe de cumplimiento de firmware, este se actualiza para utilizar los filtros de datos actuales.

Puede cancelar un trabajo de actualización de firmware programado que aún no se ha ejecutado haciendo clic en **Supervisión** (📧) → **Trabajos** en la barra de menús de XClarity Orchestrator y haga clic en la pestaña **Programas** para mostrar la tarjeta Trabajos programados. Seleccione el trabajo programado y, a continuación, haga clic en el icono de **Cancelado** (⏏).

Capítulo 6. Análisis de tendencias y predicción de problemas

Lenovo XClarity Orchestrator genera alertas de análisis basadas en problemas de hardware y firmware conocidos, supervisa las tendencias para detectar anomalías que se producen en sus recursos gestionados y genera heurística que puede calcular la probabilidad de problemas inminentes o de errores. Las tendencias se visualizan como consultas, gráficos y tablas que muestran el estado de cumplimiento, el historial de problemas y el detalle de los recursos que tienen más problemas. A continuación, puede analizar estas tendencias para obtener información sobre la causa de los problemas y resolverlos rápidamente.

Importante:

- Las funciones de análisis son compatibles con servidores ThinkAgile, ThinkSystem y ThinkEdge que ejecutan el firmware XCC v1.4 o posterior.
- Para utilizar las funciones de análisis, se necesita una licencia de análisis de Lenovo XClarity Orchestrator para cada dispositivo que admita las funciones de análisis. Una licencia *no está* vinculada a dispositivos específicos. Para obtener más información, consulte [Aplicación de licencias de XClarity Orchestrator](#) en la documentación en línea de XClarity Orchestrator.

Creación de informes de análisis personalizados

Los informes de análisis se ejecutan de forma continua en segundo plano a la hora de dar a conocer el grado de funcionamiento de su centro de datos en tiempo real.

Acerca de esta tarea

Lenovo XClarity Orchestrator proporciona varios informes de análisis predefinidos que se basan en los datos de sucesos, inventario o mediciones que se recopilan de los recursos gestionados. A continuación, estos se muestran como estadísticas (en forma de tabla) o gráficamente como gráficos de barras o gráficos circulares. Puede ver ejemplos de estos informes en las páginas [Análisis \(🔍\) → Análisis predefinido](#).

También puede crear sus propios informes personalizados para representar los datos que le interesan más.

Procedimiento

Para crear un informe de análisis personalizado, complete los pasos siguientes.

Paso 1. Crear alertas personalizadas.

XClarity Orchestrator genera alertas de análisis basadas en problemas de hardware y firmware conocidos. También puede crear alertas personalizadas para utilizarlas en sus informes personalizados.

Paso 2. Crear informes personalizados (consultas).

Puede añadir informes gráficos personalizados a XClarity Orchestrator definiendo consultas sobre la base de los datos que más le interesen.

Creación de reglas para alertas de análisis personalizadas

Lenovo XClarity Orchestrator genera alertas basadas en problemas de hardware y firmware conocidos. Puede definir *reglas de alertas* personalizadas para generar alertas de análisis cuando se produce un suceso específico o cuando se produce una infracción de una medición específica. A continuación, puede utilizar dichas alertas para generar informes personalizados de información (consultas).

Acerca de esta tarea

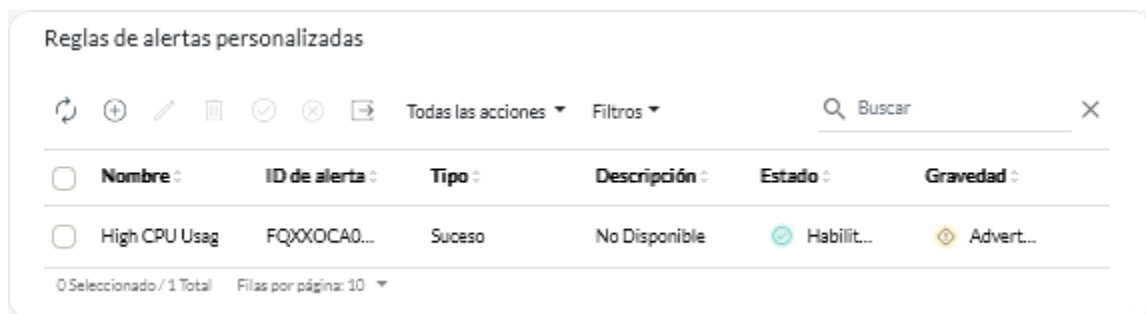
Los sucesos se elevan para todas las alertas, incluidas las alertas de correo electrónico personalizadas. Se usa el mismo código de suceso para la alerta activa y para el suceso con el formato FQXX0CAxxxxc, donde xxxx es el identificador único y c es la gravedad.

Las alertas personalizadas se incluyen en la lista de alertas activas de estado. Todas las alertas activas, incluidas las alertas personalizadas, se muestran en una única vista unificada (consulte [Supervisión de alertas activas](#)).

Procedimiento

Para crear una regla de alertas personalizadas, lleve a cabo los siguientes pasos.

Paso 1. Desde la barra de menú de XClarity Orchestrator, haga clic en **Análisis** (🔍) → **Alertas personalizadas**, para mostrar la tarjeta Reglas de alertas personalizadas.



Paso 2. Haga clic en el icono de **Crear** (+) para mostrar el cuadro de diálogo Crear regla de alertas personalizadas.

Paso 3. Especifique un nombre único y una descripción opcional para la regla de alertas personalizadas.

Paso 4. Seleccione el tipo de origen para esta regla.

- **Suceso.** Genera una alerta cuando ocurre un suceso específico, según los criterios de la regla.
- **Métrica.** Genera una alerta cuando se infringe una métrica específica, según los criterios de la regla.

Paso 5. Haga clic en **Detalles del activador de la regla** y especifique los criterios de esta regla. Los criterios varían según el tipo de origen.

- **Reglas de alertas basadas en sucesos**

- Especifique el tipo de destino de esta alerta.
 - **Dispositivo.** Genera una alerta cuando el suceso ocurre en cualquier dispositivo. El nombre del dispositivo se incluye en esta alerta.
 - **Grupo de dispositivos.** Genera una alerta cuando el suceso ocurre en un dispositivo en cualquier grupo de dispositivos. El nombre del grupo se incluye en la alerta.
- Especifique el Id. del suceso que activa una alerta. Para obtener una lista de los Id. de sucesos, consulte [Mensajes de sucesos y alertas](#) en la documentación en línea de XClarity Orchestrator.
- Especifique el número de veces (recuento) que el suceso debe ocurrir en el intervalo especificado antes de que se produzca una alerta.
- Seleccione el período de tiempo (intervalo), en minutos, en el que el suceso tiene lugar antes de que se produzca una alerta.

- **Reglas de alertas basadas en métricas**

- Seleccionar modo de criterios.

- **promedio**. Genera una alerta cuando el valor promedio de la métrica supera el umbral (basado en el comparador) durante un intervalo específico.

Por ejemplo, puede crear una regla para generar una alerta cuando la temperatura media de la CPU (**metric**) en un periodo de 24 horas (**interval**) sea superior a (**operator**) 40 grados C (**threshold**).

- **conteo**. Genera una alerta cuando la métrica supera el umbral (basado en el comparador) una cantidad determinada de veces durante un intervalo específico.

Por ejemplo, puede crear una regla para generar una alerta cuando la temperatura de la CPU (**metric**) sea superior a (**operator**) 40 grados C (**threshold**) 5 veces (**count**) en un periodo de 24 horas (**interval**).

- **simple**. Genera una alerta cuando la métrica supera el umbral (según el comparador).

Por ejemplo, puede crear una regla para generar una alerta cuando la temperatura de la CPU (**metric**) sea superior a (**operator**) 40 grados C (**threshold**).

- Seleccione la medición (métrica) para esta alerta de una lista de mediciones admitidas por los recursos gestionados.
- Si el modo de criterios es “recuento”, especifique el número de veces que se infracción el valor en el intervalo especificado antes de que se levante una alerta.
- Seleccione la función de comparación.
 - >=. Mayor o igual que
 - <=. Menor o igual que
 - >. Mayor que
 - <. Menor que
 - =. Igual a
 - !=. No es igual a
- Especifique el valor de umbral que se va a comparar con el valor de métrica.
- Si el modo de criterios es “promedio” o “cuenta”, seleccione el período de tiempo (intervalo), en minutos, en el que se evalúa la medición.


Paso 6. Haga clic en **Alerta y detalles del suceso** y especifique la información que se mostrará para la alerta y el suceso.

1. Especifique el mensaje, la descripción y la acción del usuario para mostrar la alerta y el suceso asociados. Puede incluir variables entre corchetes, por ejemplo `[[DeviceName]]`, para incluir el nombre del campo (variable). En la tabla a la derecha de los campos de entrada se muestra una lista de los campos disponibles (sobre la base de la medición seleccionada).
2. Seleccione la gravedad de esta regla de alerta.
 - **Advertencia**. El usuario puede decidir si es preciso realizar alguna acción.
 - **Crítico**. Es preciso realizar una acción inmediatamente y el espectro de resultados es amplio (por ejemplo, un corte eléctrico inminente o la afectación de un recurso crítico).
3. Especifique un número de 4 dígitos para utilizarlo como código de suceso para esta alerta. Puede especificar un número entre 0001 y 9999 que no se esté utilizando todavía.

Paso 7. Opcionalmente, cambie el estado a **Habilitado** para permitir que XClarity Orchestrator produzca una alerta de análisis cuando se cumplan los criterios de las alertas personalizadas.

Paso 8. Haga clic en **Crear**.

Después de finalizar

Puede ver la lista de las alertas de análisis que se han producido en función de las reglas de alertas personalizadas habilitadas haciendo clic en **Supervisión**  → **Alertas**.

Puede realizar las siguientes acciones desde la tarjeta de Reglas de alertas personalizadas.

- Modifique las propiedades de una regla de alertas personalizadas haciendo clic en el icono de **Editar** (✎).
- Elimine una regla de alertas personalizadas seleccionada haciendo clic en el icono de **Eliminar** (🗑).
- Habilitado o deshabilitar una o varias reglas de alertas personalizadas seleccionadas, haga clic en el icono **Habilitar** (☑) o el icono **Deshabilitar** (☒).

Creación de informes personalizados (consultas)

Puede añadir informes gráficos y tabulares personalizados a Lenovo XClarity Orchestrator definiendo las consultas basándose en los datos recopilados, como alertas, sucesos, inventarios, métricas de dispositivos o sus métricas personalizadas (agregaciones).

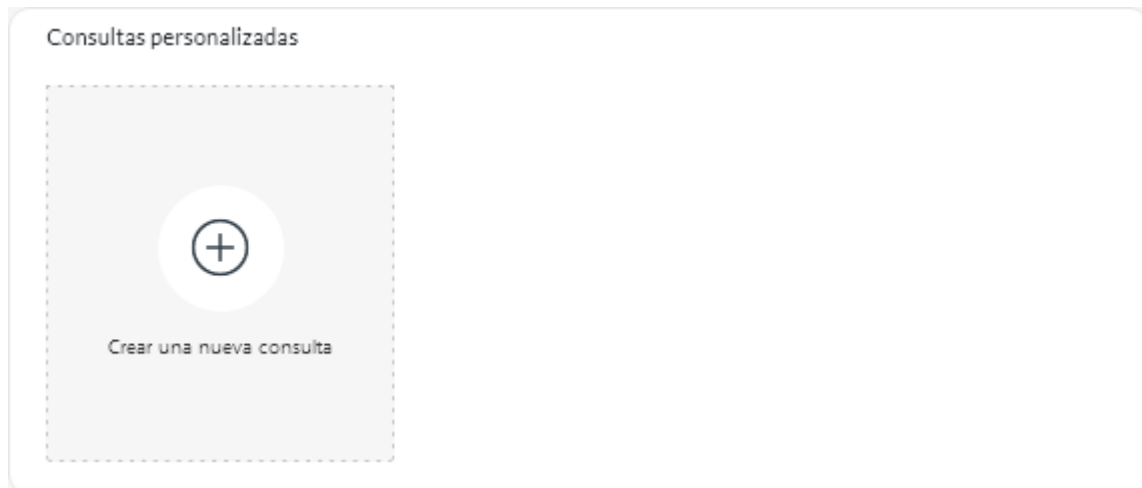
Antes de empezar

Importante: La creación de informes personalizados y de análisis en XClarity Orchestrator requiere una base de datos de descripción básica y consultas de base de datos.

Acerca de esta tarea

Para crear un informe personalizado, complete los pasos siguientes.

- Paso 1. En la barra de menús de XClarity Orchestrator, haga clic en **Análisis** (🔍) → **Consultas personalizadas** para mostrar la tarjeta Consultas personalizadas.



- Paso 2. Haga clic en el icono **Crear** (+) para mostrar el cuadro de diálogo Crear consulta personalizada.
- Paso 3. Especifique un nombre único para la consulta personalizada.
- Paso 4. Seleccione el tipo de datos que desea utilizar como la fuente para esta consulta.

Puede elegir uno de los siguientes tipos de fuentes de datos.

- **Alerts.** Condiciones de hardware o de gestión que es necesario investigar y necesitan la acción del usuario
- **Events.** Sucesos de recursos y auditorías
- **Events-Resource.** Condición de hardware o de Orchestrator que se produjo en un dispositivo gestionado, un gestor de recursos o XClarity Orchestrator
- **Events-Audit.** Actividades del usuario que se realizaron desde un gestor de recursos o XClarity Orchestrator
- **Inventories-Manager.** Datos de inventario para gestores de recursos
- **Inventories-Device.** Datos de inventario para dispositivos gestionados de todos los tipos
- **Inventories-Device-Server.** Datos de inventario para servidores gestionados

- **Inventories-Device-Switch.** Datos de inventario para conmutadores gestionados
- **Inventories-Device-Storage.** Datos de inventario para dispositivos de almacenamiento gestionados
- **Inventories-Device-Chassis.** Datos de inventario para chasis gestionados
- **CPUTemp.** Datos de métricas para la temperatura, en Celsius, de cada procesador en un dispositivo gestionado. La métrica se captura cada minuto.
- **CPUUtilizationStats.** Datos de métricas para el uso del procesador, como porcentaje, para un dispositivo gestionado. La métrica se captura cada minuto.
- **InletAirTemp.** Datos de métricas para la temperatura de aire de entrada, en Celsius, en un dispositivo gestionado. La temperatura se captura cada minuto.
- **MemoryUtilizationStats.** Datos de métricas para la memoria utilizada, como porcentaje, por un dispositivo gestionado. La métrica se captura cada minuto.
- **PowerMetrics.** Datos de estadísticas para el consumo de alimentación, en vatios, por todos los procesadores, módulos de memoria o todo el sistema para un dispositivo gestionado. Estos indicadores se capturan cada 30 segundos.
- **PowerSupplyStats.** Datos de métrica de la entrada y salida de la fuente de alimentación, en vatios, para un dispositivo gestionado. Estos indicadores se capturan cada 30 segundos.

Los tipos de orígenes de datos (alertas, sucesos, inventarios y métricas) que se enumeran en la lista varían según los datos que están disponibles en XClarity Orchestrator. Por ejemplo, si hay datos de alertas disponibles, se indica el tipo **Alerts**. Si hay datos de sucesos disponibles, se indican los tipos **Events-***.

El origen seleccionado para los datos afecta a los datos que están disponibles en la pestaña **Condiciones de consulta**. Si selecciona un tipo genérico, como **Inventories-Devices**, solo se enumeran los atributos comunes a todos los dispositivos. Si selecciona **Inventories-Device-Server**, se muestran los atributos que son comunes a todos los servidores.

Paso 5. Haga clic en **Condiciones de consulta** para definir las condiciones de consulta del informe.

1. Restrinja los datos que desee utilizar para esta consulta.
 - a. Selección de uno o varios campos de la lista desplegable **Campos filtrados**. Los campos que se enumeran según el tipo de origen de datos seleccionado en el [paso 4](#).
 - b. Si seleccionó varios campos de filtro, elija el operador que se va a utilizar para crear la consulta. Puede presentar uno de los valores siguientes.
 - **AND.** Todos los valores deben coincidir.
 - **OR.** Uno o más valores deben coincidir.
 - **Y (negado).** Ninguno de los valores debe coincidir.
 - **O (negado).** Uno o más valores debe no coincidir.
 - c. Para cada campo filtrado que haya seleccionado, seleccione el operador de comparación en la lista desplegable **Comparación** y el valor de campo. Los operadores de comparación disponibles varían en función del tipo de datos para el atributo.
 - **>=.** Coincide con valores que son *mayores o iguales que* un valor especificado
 - **<=.** Coincide con valores que son *menores o iguales que* un valor especificado
 - **>.** Coincide con valores que son *mayores que* un valor especificado
 - **<.** Coincide con valores que son *menores que* un valor especificado
 - **=.** Coincide con valores que son *iguales que* un valor especificado
 - **!=.** Coincide con todos los valores que son *no iguales que* un valor especificado
 - **Contains.** (Solo consultas de sucesos y de inventario) Coincide con todos los valores parciales especificados en una matriz
 - **In.** (Solo consultas de sucesos y de inventario) Coincide con todos los valores especificados en una matriz
 - **NotIn.** (Solo consultas de sucesos y de inventario) No coincide con ninguno de los valores parciales especificados en una matriz

Consejo: Para buscar los valores actuales de cualquier campo, cree una nueva consulta con el mismo tipo de origen de datos, seleccione el nombre del campo en la lista desplegable **Campos agrupados**, especifique 0 para el **Límite** y, a continuación, haga clic en **Guardar**. La pestaña **Opciones de gráfico** se muestra con una lista de todos los valores actuales.

2. Opcionalmente, elija una función de agregación en la sección **Agregación de resultados** para crear un nuevo campo basado en los datos filtrados y especifique un nombre (alias) para el nuevo campo. Para algunas funciones de agregación como promedio y máximo, también debe especificar el campo en el que desea aplicar la función.

Para consultas de sucesos y de inventario, puede elegir una de las siguientes funciones.

- **Promedio.** Media estadística de todos los valores
- **Suma.** Suma de todos los valores
- **Conteo.** Número de valores
- **Máximo.** Valor más alto
- **Mínimo.** Valor más bajo
- **First.** Valor con la marca de tiempo más antigua
- **Last.** Valor con la marca de tiempo más reciente

Para las consultas de métricas, puede elegir una de las siguientes funciones.

- **Conteo.** Número de valores no nulos
- **Distinct.** Lista de valores únicos
- **Integral.** Valor de campo promedio
- **Mean.** Media aritmética (promedio) de valores
- **Median.** Valor medio
- **Mode.** Valor más frecuente
- **Spread.** Diferencia entre los valores mínimo y máximo
- **StdDev.** Desviación estándar
- **Suma.** Suma de todos los valores

3. Si lo desea, elija los campos que desee utilizar para agrupar los resultados de la consulta en la lista desplegable **Campos agrupados**. Cuando elige un campo agrupado, XClarity Orchestrator desenreda (desconstruye) los datos para que haya un punto de datos para cada valor de los campos seleccionados.
4. Opcionalmente, elija cómo ordenar los resultados de la consulta seleccionando un campo en la lista desplegable **Ordenar por campo** y el criterio de orden en la lista desplegable **Criterio de orden**. Para consultas de métricas, solo puede ordenar por hora.
5. Opcionalmente, especifique el número de puntos de datos a arrojar en los resultados de la consulta en el campo **Límite**. El límite predeterminado es 10. Si especifica 0 o lo deja vacío, se arrojan todos los puntos de datos.

Opcionalmente, también puede especificar el número de puntos de datos que desea omitir en los resultados de la consulta en el campo **Desplazamiento**.

6. (Solo consultas de métricas) Si elige campos agrupados, especifique opcionalmente el número de conjuntos de datos que deben arrojarse en los resultados de la consulta en el campo **Límite de la serie**. El límite predeterminado es vacío (0). Si especifica 0 o lo deja vacío, se arrojan todos los conjuntos de datos.

Opcionalmente, también puede especificar el número de conjuntos de datos que desea omitir en los resultados de la consulta en el campo **Desplazamiento de serie**.

7. Haga clic en **Guardar** para guardar la consulta y generar el informe.

Paso 6. Haga clic en **Opciones de gráfico** para elegir el aspecto y la apariencia del informe. Los siguientes tipos de gráficos están disponibles.

- **Tabla.** Muestra los datos en forma de tabla.

- **Barra.** Muestra los datos como un gráfico de barras. Elija los campos que desee utilizar para los ejes x e y.
- **Circular.** Muestra los datos como un gráfico circular. Elija los campos que desee utilizar para los ejes x e y. Puede optar por utilizar un gráfico circular solo cuando los datos no están agrupados.

Paso 7. Haga clic en **Crear** para añadir una tarjeta nueva que contenga un informe con los resultados de la consulta actual.

Después de finalizar

Puede realizar las siguientes acciones desde la tarjeta Consultas personalizadas.

- Para ampliar un informe personalizado, haga clic en el icono **Agrandar** (🔍) en la tarjeta del informe personalizado. Para los informes tabulares, el icono de informe de la tarjeta Consultas personalizadas muestra solo las cuatro primeras columnas de la tabla. Puede agrandar el informe para ver todas las columnas de la tabla.

El enlace **Ver detalles** en una columna de la tabla indica que la columna contiene varios campos de datos. Haga clic en el enlace **Ver detalles** para mostrar una tabla emergente que enumera los datos adicionales.

- Para modificar las propiedades de un informe personalizado, haga clic en el icono **Editar** (✎) de la tarjeta.
- Para eliminar el informe personalizado, haga clic en el icono **Eliminar** (🗑️) de la tarjeta.

Análisis de tiempos de arranque de un dispositivo

El panel Análisis contiene tarjetas de informe que resumen los tiempos de arranque para dispositivos gestionados. El *tiempo de arranque* es la cantidad de tiempo, en segundos, que tardó en completarse el arranque del sistema, antes de pasarlo al sistema operativo.

Para mostrar los informes de tiempo de arranque, haga clic en **Análisis** (🔍) → **Análisis predefinido** y luego haga clic en **Tiempos de arranque** para mostrar las tarjetas de análisis relacionadas.

Nota: Las estadísticas de arranque solo están disponibles para los dispositivos ThinkSystem y ThinkAgile que ejecutan XCC firmware v1.40 o posterior.

Tiempos de arranque

Esta tarjeta de informe incluye un gráfico de barras que muestra la cantidad de tiempo que tardó en completarse el proceso para dispositivos con más tiempo de arranque más reciente.

Análisis de problemas de conectividad

El panel Análisis contiene tarjetas de informe que muestran estadísticas sobre los problemas de conectividad.

Se notifica la pérdida de conectividad utilizando el suceso siguiente.

- **FQXHMDM0163J.** La conexión entre el gestor de recursos y el controlador de gestión de la placa base en el dispositivo está fuera de línea.

Para mostrar los informes de conectividad perdida, haga clic en **Análisis** (🔍) → **Análisis predefinidos** y luego haga clic en **Problemas de conectividad** para mostrar las tarjetas de análisis relacionadas.

Problemas de conectividad por tiempo

Esta tarjeta de informe incluye un gráfico de barras que muestra el número de problemas de conectividad que ocurrieron durante el día o mes actual por cada recurso.

También puede mostrar datos para un rango de tiempo específico seleccionando el icono **Valores** (⚙️) que se encuentran en la esquina superior derecha de la tarjeta.

10 dispositivos principales por número problemas de conectividad

Esta tarjeta de informe incluye un gráfico de barras que muestra los 10 dispositivos principales que están notificando la mayor cantidad de problemas de conectividad en general. Puede hacer clic en un elemento de la leyenda para obtener más información sobre un recurso específico.

Análisis de correcciones de seguridad

El panel Análisis contiene tarjetas de informe que muestran análisis sobre correcciones de seguridad para vulnerabilidades y exposiciones comunes (CVE) conocidas.

Para mostrar los informes de CVE, haga clic en **Análisis** (🔍) → **Análisis predefinidos** y luego haga clic en **Correcciones de seguridad** para mostrar las tarjetas de análisis relacionadas.

Correcciones de seguridad

Esta tarjeta de informe incluye las siguientes estadísticas y gráficos.

- Un gráfico circular que muestra el número de dispositivos gestionados que tienen vulnerabilidades y exposiciones comunes (CVE) para las cuales hay disponible una corrección de seguridad, según la máxima gravedad de CVE
 - **Crítico**. Número de dispositivos con al menos una CVE crítica
 - **No crítica**. Número de dispositivos que tienen al menos una CVE alta, media o baja, pero que no tienen CVE críticas
 - **Protegido**. Número de dispositivos sin CVE conocidas y que están protegidos
- Un gráfico circular que muestra el número de CVE únicos para los cuales hay disponibles correcciones de seguridad, por gravedad (crítica, alta, media o baja)

Puede pasar el cursor sobre cada barra de color en los gráficos circulares para obtener más información sobre el estado. También puede hacer clic en el número junto a cada estado para ver una lista de todos los dispositivos que se ajustan a los criterios.

Página Dispositivos

La tarjeta Dispositivos indica el número total de CVE para las cuales hay disponible una corrección de seguridad y la gravedad más alta de CVE para cada dispositivo. Puede expandir el dispositivo para ver una lista de componentes en dicho dispositivo que tienen correcciones de seguridad, así como el número de correcciones de seguridad disponibles de actualizaciones de firmware que se descargan en el repositorio de actualizaciones.

Puede hacer clic en el número de correcciones de seguridad para abrir un cuadro de diálogo con una lista filtrada de CVE aplicables para ese componente. En ese cuadro de diálogo, puede hacer clic en el enlace de CVE para obtener información detallada sobre esa CVE en la web.

Puede mostrar u ocultar la tarjeta Dispositivos haciendo clic en el alternador **Mostrar u ocultar dispositivos**. El icono de alternación cambia automáticamente a **Mostrar dispositivos** cuando hace clic en un número en los gráficos.

Análisis de estado de la unidad

El panel Análisis contiene tarjetas de informe que muestran la información sobre el estado y la falla predictiva de unidades de disco duro y unidades de estado sólido en servidores ThinkAgile y ThinkSystem gestionados.

Para mostrar los informes de firmware, haga clic en **Análisis (🔍)** → **Análisis predefinidos** y luego haga clic en **Análisis predictivo de la unidad** para mostrar las tarjetas de análisis relacionadas.

Los análisis se admiten para los siguientes tipos de modelo de unidad.

Unidad de disco duro

- ST2000NX0253
- ST8000NM0055
- ST10000NM0086
- ST12000NM0008

Unidades de estado sólido

- Intel SSDSC2BB800G4

Importante: Las unidades con firmware más antiguo no son aptas para el análisis. Actualice las unidades en el nivel de firmware más reciente para permitir un análisis predictivo.

Unidades en riesgo

Esta tarjeta de informe contiene un gráfico circular que muestra el número de unidades en cada estado (normal o en riesgo).

Historial de unidades en riesgo

Esta tarjeta de informe contiene un gráfico de barras que muestra el número de unidades con error durante la última semana o el año pasado. Sitúe el cursor por encima de cada barra del gráfico para mostrar una lista filtrada de unidades con error, por dispositivo, ese día.

Unidades con falla predictiva

La tarjeta de informes contiene una tabla que enumera los dispositivos con unidades con errores. Puede hacer clic en un dispositivo para enumerar los detalles de cada unidad en riesgo de ese dispositivo.

Análisis de firmware

El panel Análisis contiene tarjetas de informe que muestran análisis sobre el firmware.

Para mostrar los informes de firmware, haga clic en **Análisis (🔍)** → **Análisis predefinidos** y luego haga clic en **Análisis de firmware** para mostrar las tarjetas de análisis relacionadas.

Análisis de firmware

Esta tarjeta de informe incluye un gráfico de barras que muestra el número de firmware que está instalado en los dispositivos gestionados según la categoría y antigüedad del firmware.

El firmware se agrupa en las siguientes categorías.

- Controlador de gestión
- Herramientas del sistema
- UEFI

Las antigüedades de firmware se agrupan en los siguientes intervalos

- **Menos de 6 meses**
- **6 a 12 meses**
- **1 a 2 años**
- **Más de 2 años**

Puede filtrar los dispositivos que están incluidos en el informe utilizando los campos de entrada de **Filtros**. También puede guardar las consultas filtradas que desee utilizar habitualmente.

Puede mostrar u ocultar la tarjeta Dispositivos haciendo clic en el alternador **Mostrar u ocultar dispositivos**. La tarjeta Dispositivos enumera los tipos de firmware y las antigüedades de todos los dispositivos que se incluyen en el gráfico.

Análisis de sucesos perdidos

El panel Análisis contiene tarjetas de informe que muestran estadísticas sobre los sucesos perdidos. Los sucesos perdidos se determinan por una brecha en los números de secuencia

Los sucesos tienen un número de secuencia que indica el orden en el que se ha producido cada suceso en un dispositivo específico. Los números de secuencia de sucesos deben ser consecutivos para un dispositivo específico. Si hay números de secuencia que no son consecutivos, el espacio puede indicar que se han perdido uno o más sucesos.

Para mostrar los informes de sucesos perdidos, haga clic en **Análisis avanzados** (⚙️) → **Análisis predefinidos** y luego haga clic en **Sucesos perdidos** para mostrar las tarjetas de análisis relacionadas.

Sucesos perdidos por tiempo

Esta tarjeta de informe incluye un gráfico de barras que muestra el número de sucesos perdidos durante el día o mes actual por cada recurso.

También puede mostrar datos para un rango de tiempo específico seleccionando el icono **Valores** (⚙️) que se encuentran en la esquina superior derecha de la tarjeta.

10 dispositivos principales por número de sucesos perdidos

Esta tarjeta de informe incluye un gráfico de barras que muestra los 10 dispositivos principales que están notificando la mayor cantidad de sucesos perdidos en general.

Análisis y predicción de la capacidad del gestor de recursos

El panel Análisis contiene tarjetas de informe que se predicen cuando los administradores de recursos van a superar el número máximo de dispositivos gestionados. Para los administradores de recursos de Lenovo XClarity Administrator, se admiten hasta 1.000 dispositivos gestionados.

Para mostrar los informes de capacidad de gestor de recursos, haga clic en **Análisis avanzados** (⚙️) → **Análisis predefinidos** y luego haga clic en **Pronóstico de capacidad de gestor** para mostrar las tarjetas de análisis relacionadas.

Capacidad de gestor

Este informe enumera la capacidad del dispositivo para cada gestor de recursos, incluido el número de dispositivos gestionados y el estado de capacidad, que indica si la capacidad está sobrecargada. Se utilizan las siguientes capacidades.

- (✅) **Normal**. El número de dispositivos gestionados es menor que el número máximo de dispositivos compatibles.
- (⚠️) **Advertencia**. El número de dispositivos gestionados es cercano al número máximo de dispositivos compatibles.
- (❌) **Crítico**. El número de dispositivos gestionados es mayor que el número máximo de dispositivos compatibles.

Gestionar tendencia de capacidad

Esta tarjeta de informe incluye un gráfico de líneas que muestra el número de dispositivos gestionados, a lo largo del tiempo, para un gestor de recursos específico y la tendencia prevista cuando el número de dispositivos gestionados alcanzará la capacidad máxima admitida para ese gestor de recursos.

Haga clic en una fila de la tabla capacidad de gestión para mostrar las tendencias de capacidad de ese gestor de recursos.

Puede cambiar el periodo de tiempo que se muestra haciendo clic en el menú desplegable. Puede elegir visualizar datos por año, trimestre, mes o día. También puede cambiar el número de periodos que se muestran en el gráfico utilizando el cuadro zoom situado debajo del gráfico.

Análisis y predicción de las tendencias de utilización

El panel Análisis contiene tarjetas de informe que muestran el uso histórico y previsto del procesador, el almacenamiento y la memoria en los dispositivos y recursos virtuales (como hosts, clústeres y máquinas virtuales).

Importante: Esta función requiere una conexión con el gestor de recursos de VMware vRealize Operations Manager (consulte [Conexión de gestores de recursos](#)).

Para mostrar los informes de tendencias de utilización, haga clic en **Análisis avanzados** (🔍) → **Análisis predefinidos** y luego haga clic en **Tendencia de utilización de carga de trabajo** para mostrar las tarjetas de análisis relacionadas.

Selección de recurso

Este informe enumera los dispositivos y recursos virtuales gestionados por el servidor de organización.

Haga clic en una fila de la tabla para mostrar las tendencias de utilización para ese recurso.

Tendencia de utilización de CPU

Esta tarjeta de informe incluye un gráfico de líneas que muestra la utilización del procesador, a lo largo del tiempo, para un recurso virtual específico y la tendencia prevista cuando la utilización del procesador alcanzará la capacidad máxima admitida para ese recurso virtual.

Puede cambiar el periodo de tiempo que se muestra para los datos históricos y los datos desaprobados de los menús desplegables **Historial** y **Proyección**, respectivamente. También puede cambiar el número de periodos que se muestran en el gráfico utilizando el cuadro zoom situado debajo del gráfico.

Tendencia de utilización de la memoria

Esta tarjeta de informe incluye un gráfico de líneas que muestra la utilización de la memoria, a lo largo del tiempo, para un recurso virtual específico y la tendencia prevista cuando la utilización de la memoria alcanzará la capacidad máxima admitida para ese recurso virtual.

Puede cambiar el periodo de tiempo que se muestra para los datos históricos y los datos desaprobados de los menús desplegables **Historial** y **Proyección**, respectivamente. También puede cambiar el número de periodos que se muestran en el gráfico utilizando el cuadro zoom situado debajo del gráfico.

Tendencia de utilización de almacenamiento

Esta tarjeta de informe incluye un gráfico de líneas que muestra la utilización del almacenamiento, a lo largo del tiempo, para un recurso virtual específico y la tendencia prevista cuando la utilización del almacenamiento alcanzará la capacidad máxima admitida para ese recurso virtual.

Puede cambiar el periodo de tiempo que se muestra para los datos históricos y los datos desaprobados de los menús desplegables **Historial** y **Proyección**, respectivamente. También puede cambiar el número de períodos que se muestran en el gráfico utilizando el cuadro zoom situado debajo del gráfico.

Análisis de rendimiento y métricas de uso

El panel Análisis contiene tarjetas de informe que muestran mapas de puntos problemáticos que se basan en métricas y recursos específicos durante las últimas 24 horas.

Para mostrar el mapa de puntos problemáticos de rendimiento, haga clic en **Análisis avanzados** (🔍) → **Análisis predefinidos** y luego haga clic en **Mapa de puntos problemáticos de rendimiento** para mostrar las tarjetas de análisis relacionadas.

Mapa de puntos problemáticos de rendimiento

Esta tarjeta de informe incluye un mapa de puntos problemáticos que muestra el número de dispositivos que tienen los valores de métricas dentro de una serie de rangos específicos durante un período de tiempo determinado.

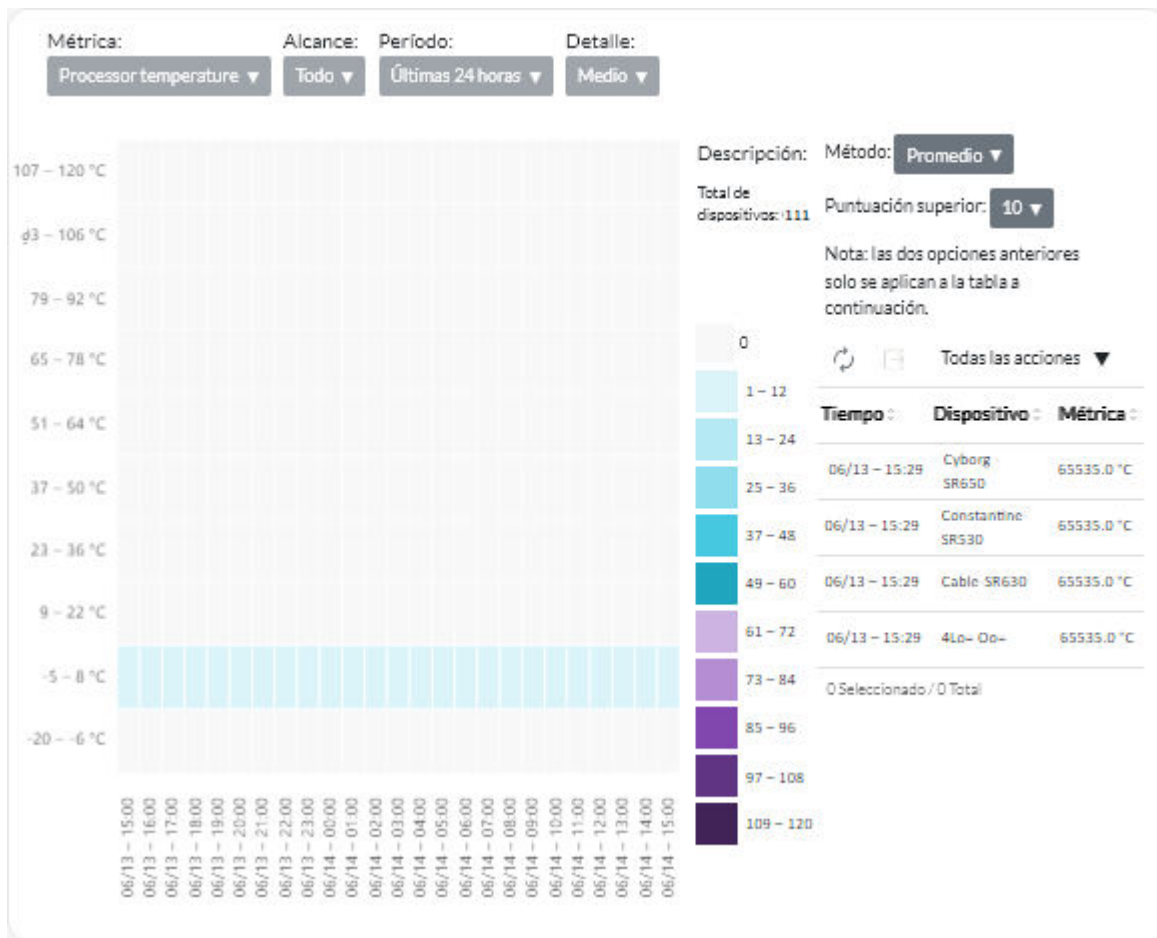
Puede hacer clic en cualquier celda del mapa de puntos problemáticos para mostrar una lista emergente de los dispositivos representados por esa celda, con información el valor real de la métrica para cada dispositivo y una marca de tiempo de cuándo se recopiló la métrica.

Puede configurar el mapa de puntos problemáticos para mostrar solo la información que le interesa.

- Puede elegir mostrar datos para una de las siguientes métricas.
 - Temperatura del procesador
 - Utilización del procesador
 - Utilización de la memoria
- Puede optar por agregar los datos de la métrica a partir de la media o el valor máximo (más alto).
- Puede filtrar los mapas de puntos problemáticos para incluir solo los datos de métrica de los dispositivos de un grupo de dispositivos específico.

Nota: Si define el alcance de la interfaz de usuario a un gestor de recursos específico, solo se incluirán en el mapa de puntos problemáticos los datos de los dispositivos de los grupos seleccionados que también se gestionan mediante el gestor de recursos.

- También puede elegir los rangos de valores numéricos que se van a mostrar en el eje x del mapa de puntos problemáticos. El número de valores entre el máximo y el mínimo se dividen en partes iguales según el número que elija. Puede optar por 10, 15 o 20.
- También puede optar por listar los 10, 15 o 20 dispositivos principales con los valores más altos y marcas de tiempo de cuándo se recopiló la métrica.



Análisis de sucesos repetidos

El panel Análisis contiene tarjetas de informe que resumen los sucesos repetidos para cada dispositivo.

Los *sucesos repetidos* se generan cuando se producen las siguientes condiciones:

- **FQXXOIS0002J**. Se generó un suceso crítico o de advertencia con la misma ID una o más veces para el mismo dispositivo en al menos tres periodos consecutivos de 5 minutos.
- **FQXXOIS0003J**. Se generaron más de cinco sucesos críticos o de advertencia para el mismo dispositivo cada hora durante dos o más horas consecutivas.

Para mostrar los informes de sucesos repetidos, haga clic en **Análisis avanzados** (🔍) → **Análisis predefinidos** y luego haga clic en **Sucesos repetidos** para mostrar las tarjetas de análisis relacionadas.

Sucesos repetidos

Esta tarjeta de informe incluye un gráfico de barras que muestra el número de sucesos repetidos en general por cada dispositivo.

Sucesos repetidos por hora

Esta tarjeta de informe incluye un gráfico de barras que muestra el número de sucesos repetidos generados en el día actual, por cada dispositivo.

Análisis de intentos de acceso no autorizado

El panel Análisis contiene tarjetas de informe que resumen los intentos de acceso no autorizado (error de inicio de sesión).

Para mostrar los informes de acceso no autorizado, haga clic en **Análisis** (🔍) → **Análisis predefinidos** y luego haga clic en **Intentos de acceso no autorizado** para mostrar las tarjetas de análisis de acceso no autorizado.

Cantidad de intentos de inicio de sesión fallidos por usuario

Esta tarjeta de informe incluye un gráfico que muestra el número de intentos de acceso no autorizado en general para cada usuario (por nombre de usuario). Puede mostrar los datos como un gráfico de barras (📊) o un gráfico circular (📈) haciendo clic en el icono adecuado en la esquina superior izquierda de la tarjeta.

Puede desplazarse sobre cada una de las barras o piezas del gráfico para obtener más información, como la última aparición.

Cantidad de intentos de inicio de sesión fallidos por usuario, en cada período

Esta tarjeta de informe incluye un gráfico de barra que muestra el número de intentos de acceso no autorizado producidos en el día actual para cada usuario (por nombre de usuario).

Cantidad de intentos de inicio de sesión fallidos por dirección IP de usuario

Esta tarjeta de informe incluye un gráfico de barra que muestra el número total de todos los intentos de acceso no autorizado en general para cada usuario (por dirección IP). Puede mostrar los datos como un gráfico de barras (📊) o un gráfico circular (📈) haciendo clic en el icono adecuado en la esquina superior izquierda de la tarjeta.

Puede desplazarse sobre cada una de las barras o piezas del gráfico para obtener más información, como la última aparición.

Cantidad de intentos de inicio de sesión fallidos por dirección IP de usuario, en cada período

Esta tarjeta de informe incluye un gráfico de barra que muestra el número de intentos de acceso no autorizado producidos en el día actual para cada usuario (por dirección IP).

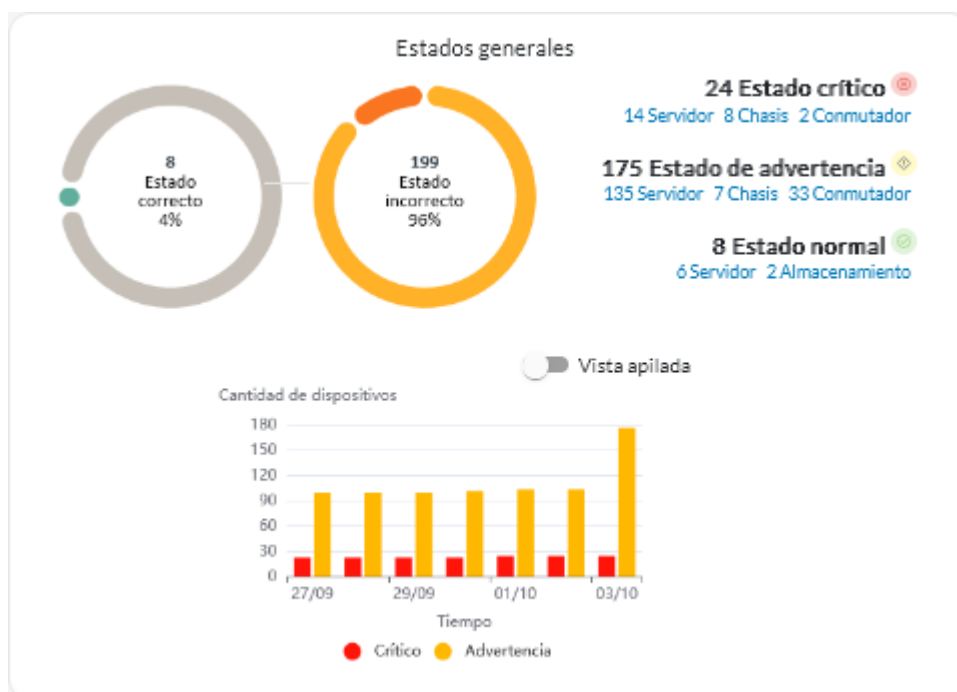
Análisis de estado del dispositivo

La tarjeta de Estado general en el panel y la tarjeta Análisis de dispositivos en cada página de dispositivos resumen el estado general de los dispositivos gestionados.

Resumen de estado de todos los dispositivos

Desde la barra de menú de XClarity Orchestrator, haga clic en **Panel** (📄) para mostrar las tarjetas del panel con una descripción general y el estado de todos los dispositivos gestionados y otros recursos (consulte [Visualización de un resumen del estado de su entorno](#)).

Puede cambiar el ámbito del resumen a solo los dispositivos gestionados por un gestor de recursos específico o en un grupo de recursos específico mediante el uso del menú desplegable **Seleccionar gestor**.



Cada barra coloreada en el gráfico circular y de barras indica el número de dispositivos en un estado específico. Puede pasar el cursor sobre cada barra coloreada para obtener más información sobre el estado. También puede hacer clic en el número de dispositivos en cada estado para ver una lista de todos los dispositivos que se ajustan a los criterios.

Resumen del estado de todos los dispositivos de un tipo específico

Para ver los resúmenes de alertas globales activas, haga clic en **Recursos** (⚙️) en la barra de menú de XClarity Orchestrator y luego haga clic en el tipo de dispositivo para mostrar una tarjeta con una vista de tabla de todos los dispositivos de ese tipo. Por ejemplo, si selecciona **Servidores**, se muestra una lista de todos los bastidores, torres y servidores compactos, además de todos los servidores Flex System y ThinkSystem en un chasis.

Puede cambiar el alcance del resumen basado en la propiedad del dispositivo desde la lista desplegable **Analizar por**.

- **Modelo de tipo de equipo.** (Predeterminado) Este informe resume el estado del dispositivo por modelo de tipo de equipo (MTM).
- **Tipo de máquina.** Este informe resume el estado del dispositivo por tipo de equipo.
- **Nombre del producto.** Este informe resume el estado del dispositivo por producto.



XClarity Orchestrator resume el estado del dispositivo basándose en criterios específicos. Cada resumen incluye la siguiente información.

- Un gráfico circular que muestra el número total de dispositivos que están en mal estado y porcentaje de dispositivos en cada estado incorrecto (crítico, advertencia o desconocido).

Cada barra coloreada en el gráfico circular indica el número de dispositivos en un estado específico. Puede pasar el cursor sobre cada barra coloreada para obtener más información sobre el estado.

- Un gráfico de líneas que muestra el número de dispositivos para cada tipo de estado de condición por día sobre el número especificado de días.

Cada barra coloreada en el gráfico de líneas indica el número de dispositivos en un estado específico. Puede pasar el cursor sobre cada barra coloreada para obtener más información sobre el estado.

- El número de dispositivos de cada tipo que no están en un estado correcto en un día específico. El día actual se muestra de manera predeterminada. Puede cambiar el día pasando el cursor sobre cada día en el gráfico de líneas.

Análisis del estado de los recursos de infraestructura

Puede determinar el estado general y las tendencias del sensor de los recursos de infraestructura.

Estado de los recursos de infraestructura

En la barra de menú de Lenovo XClarity Orchestrator, haga clic en **Recursos** (🔧) → **Infraestructura** para mostrar la tarjeta Infraestructura. Puede determinar el estado de cada recurso en la columna **Estado**.

Tendencias del sensor

En la barra de menú de XClarity Orchestrator, haga clic en **Recursos** (🔧) → **Infraestructura** para mostrar la tarjeta de infraestructura, y luego haga clic en un recurso de infraestructura de la tabla para ver una lista de sensores para ese recurso y la medición más reciente de cada uno.

Seleccione uno o más sensores, y luego haga clic en el icono de **Gráfico** (📊) para ver los gráficos de línea que muestran las mediciones, a lo largo del tiempo, para cada sensor seleccionado. De forma predeterminada, los sensores con la misma unidad (como vatios o amperios) se generan en el mismo gráfico.

Nota: Schneider Electric EcoStruxure IT Expert recopila datos del sensor cada 5 minutos y XClarity Orchestrator sincroniza estos datos cada hora. Actualmente, XClarity Orchestrator solo guarda los últimos 60 minutos de datos.

Análisis de alertas activas

La tarjeta de Análisis de alertas resume las alertas activas.

Lenovo XClarity Orchestrator resume las alertas activas basándose en criterios específicos. Cada resumen incluye la siguiente información.

- Un gráfico circular que muestra el número total de alertas activas y el porcentaje de alertas asociadas con cada tipo de resumen
- El número de alertas activas para cada tipo de resumen
- Antigüedad de la alerta activa más antigua
- Un gráfico de líneas que muestra el número de alertas para cada tipo de resumen por día sobre el número especificado de días
- El número de alertas activas para cada tipo de resumen en un día específico. El día actual se muestra de manera predeterminada. Puede cambiar el día pasando el cursor sobre cada día en el gráfico de líneas.

Alertas activas generales

Para ver los resúmenes de alertas activas generales, lleve a cabo los pasos siguientes.

1. En la barra de menú de XClarity Orchestrator, haga clic en **Supervisión** (📊) → **Alertas** para mostrar la tarjeta Análisis de alertas.
2. Seleccione el periodo de tiempo en la lista desplegable encima del gráfico de líneas. El valor predeterminado es los últimos siete días.
3. Seleccione el tipo de resumen en la lista desplegable **Analizar por**.
 - **Gravedad.** (predeterminado) En este informe se resumen las alertas activas por gravedad: crítica, advertencia e informativa.
 - **Tipo de origen** En este informe se resumen las alertas activas generadas por cada tipo de origen, como dispositivo, gestión y análisis.
 - **Tipo de recurso** En este informe se resumen las alertas activas para cada tipo de recurso, como dispositivos, gestores de recursos y XClarity Orchestrator.
 - **Capacidad de servicio.** En este informe se resumen las alertas activas asociadas con cada tipo de capacidad de servicio: **ninguna** (no se requiere servicio), **usuario** (el usuario brinda el servicio), **con capacidad de servicio** (Lenovo brinda el servicio).

Alertas activas para un dispositivo específico

Para ver la alerta activa para un dispositivo específico, lleve a cabo los pasos siguientes.

1. Desde la barra de menú de XClarity Orchestrator, haga clic en **Recursos** (🔍) y luego haga clic en el tipo de dispositivo para mostrar una tarjeta con una vista de tabla de todos los dispositivos gestionados de ese tipo.
2. Haga clic en la fila del dispositivo para mostrar las tarjetas de resumen del dispositivo para dicho dispositivo.

3. Haga clic en **Registro de alertas** para mostrar la lista de alertas activas para el dispositivo y la tarjeta de análisis de alertas.
4. En la tarjeta Análisis de alertas, seleccione el periodo de la lista desplegable sobre el gráfico de líneas. El valor predeterminado es los últimos siete días.
5. Seleccione el tipo de resumen en la lista desplegable **Analizar por**.
 - **Tipo de origen** En este informe se resumen las alertas activas generadas por cada tipo de origen, como dispositivo, gestión y análisis.
 - **Tipo de capacidad de servicio** En este informe se resumen las alertas activas asociadas con cada tipo de capacidad de servicio: ninguna (no se requiere servicio), usuario (el usuario brinda el servicio), con capacidad de servicio (Lenovo brinda el servicio).
 - **Gravedad**. En este informe se resumen las alertas activas por gravedad: crítica, advertencia e informativa.

Capítulo 7. Trabajo con servicio y soporte

Lenovo XClarity Orchestrator proporciona un conjunto de herramientas que puede utilizar para recopilar los archivos de servicio y enviarlos a 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. Puede contactar con Soporte de Lenovo para obtener ayuda y asistencia técnica cuando se producen problemas.

Envío de datos periódicos a Lenovo

Opcionalmente, puede permitir que Lenovo XClarity Orchestrator recopile información acerca de su entorno de hardware y envíe esos datos a Lenovo periódicamente. Lenovo utiliza estos datos para mejorar su experiencia con los productos de Lenovo y con el soporte de Lenovo.

Antes de empezar

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

Atención: Debe aceptar el [Declaración de privacidad de Lenovo](#) antes de poder transferir datos al soporte de Lenovo.

Acerca de esta tarea

Al analizar los datos de hardware de varios usuarios, Lenovo puede aprender los cambios de hardware que se producen con frecuencia. Estos datos se pueden utilizar para mejorar los análisis predictivos y para mejorar su experiencia de servicio y soporte por la existencia de piezas en las regiones geográficas adecuadas.

Al aceptar enviar datos de hardware a Lenovo, se recopilan los siguientes datos y se envían de forma periódica.

- **Datos de hardware diarios.** Solo cambios en los datos de inventario y en los datos de análisis de la unidad (si está habilitada la recopilación de datos) para cada dispositivo gestionado
- **Datos de hardware semanales.** Todos los datos de inventario para los dispositivos gestionados y la información acerca de los gestores de recursos conectados

Atención: Estos datos *no son anónimos*.

- Los datos recopilados *incluyen* UUID, WWN, Id. de dispositivo y números de serie. XClarity Orchestrator modifica el inventario al aplicar un algoritmo hash a los UUID, WWN e Id. de dispositivo utilizando SHA512.
- Los datos recopilados *no incluyen* información de red (direcciones IP, nombres de dominio o nombres de hosts) ni información de usuario.

Cuando se envían datos a Lenovo, se transmiten desde la instancia de XClarity Orchestrator a la herramienta de carga de Lenovo mediante HTTPS. Las API REST se llaman a través de esta conexión HTTPS para enviar los datos. Un certificado que se carga previamente en XClarity Orchestrator se utiliza para la autenticación. Si una instancia de XClarity Orchestrator no tiene acceso directo a Internet y hay un proxy configurado en XClarity Orchestrator, los datos se transmiten a través de dicho proxy.

A continuación, los datos se trasladan al repositorio de Atención al cliente de Lenovo, donde se almacenan hasta por 5 años. Este repositorio es una ubicación segura que también se utiliza cuando los datos de

depuración se envían a Lenovo para resolver problemas. Se utiliza en la mayoría de los productos de servidores, almacenamiento y conmutadores de Lenovo.

Desde el repositorio de Atención al cliente de Lenovo, se ejecutan consultas en todos los datos proporcionados y de uso y los gráficos se ponen a disposición del equipo de productos de Lenovo para su análisis.

Procedimiento

Para permitir a XClarity Orchestrator recopilar y enviar datos de los clientes a Lenovo, lleve a cabo los siguientes pasos.

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

Carga de datos periódica

Le queremos pedir un favor. Para mejorar este producto y su experiencia de uso, ¿nos permitiría recopilar información sobre cómo utiliza este producto?

[Declaración de privacidad de Lenovo](#)

Acepto enviar datos de hardware a Lenovo de forma periódica ?

Los datos de inventario de hardware y de unidad-análisis se envían de forma periódica a Lenovo. Lenovo puede usar estos datos para mejorar su futura experiencia de soporte (por ejemplo, almacenar y mover las piezas correctas más a su alcance).

Nunca se recopila información personal. Si en algún momento decide que preferiría que dejemos de recopilar esta información, puede deshabilitar la carga de datos periódica mediante el botón de alternación que se encuentra arriba.

Puede guardar el último archivo enviado o un archivo de muestra en función de la información que le hemos recopilado.

?

Archivos disponibles ▼ Guardar archivo

Paso 2. Opcionalmente, acepte enviar datos de hardware a Lenovo.

Paso 3. Acepte el [Declaración de privacidad de Lenovo](#).

Después de finalizar

Puede realizar las acciones siguientes desde esta página si aceptó enviar datos.

- Puede guardar los archivos de datos diarios y semanales más reciente que se enviaron a Lenovo al sistema local seleccionando el archivo que desea descargar y haciendo clic en **Guardar archivo**.

Recopilación de datos de servicio para XClarity Orchestrator

Puede recopilar manualmente los datos de servicio para Lenovo XClarity Orchestrator y luego guardar la información como un archivo en formato tar.gz en el sistema local. Puede luego enviar los archivos de servicio a su proveedor de servicio de preferencia para obtener ayuda para resolver problemas a medida que surjan.

Antes de empezar

Más información:  [Cómo recopilar datos de servicio](#)

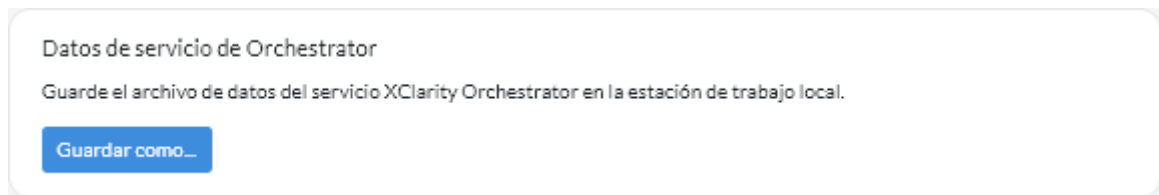
Debe ser miembro de un grupo de usuarios al que esté asignado el rol de **Supervisor** predefinido.

Asegúrese de que el navegador web no bloquee los elementos emergentes del sitio web de XClarity Orchestrator cuando descargue datos del servicio

Procedimiento

Para recopilar los datos de servicio para XClarity Orchestrator, lleve a cabo los siguientes pasos.

Paso 1. En la barra de menú de XClarity Orchestrator, haga clic en **Administración** (⚙️) → **Servicio y soporte** y luego haga clic en **Datos de servicio** en el panel de navegación izquierdo para mostrar la tarjeta Datos del servicio de gestión.



Paso 2. Haga clic en **Guardar como** para recopilar datos del servicio y guardar el archivo en el sistema local.

Se crea un trabajo para recopilar datos del servicio. Puede supervisar el progreso del trabajo desde la tarjeta **Supervisión** (📊) → **Trabajos**. Si el trabajo no finalizó correctamente, haga clic en el enlace del trabajo para mostrar los detalles correspondientes (consulte .)

Después de finalizar

También puede llevar a cabo estas acciones relacionadas.

- Abra manualmente un informe de servicio para un dispositivo específico en la tarjeta Informes de servicio de la página Servicio específico de dispositivo, haciendo clic en el icono **Abrir informe de servicio** (📄) (consulte [Abrir manualmente un informe de servicio en el Centro de Soporte de Lenovo](#)).
- Adjunte un archivo de datos de servicio a un informe de servicio activo seleccionado en la tarjeta Informes de servicio de la página Servicio específico de dispositivo, haciendo clic en el icono **Adjuntar archivo de servicio** (+). Puede adjuntar un archivo desde XClarity Orchestrator o desde el sistema local.

Notas:

- Puede adjuntar un archivo único que no sea superior a 2 GB. El nombre de archivo no debe superar los 200 caracteres. Para obtener información sobre cómo crear archivos de datos de servicio, consulte [Recopilar datos del servicio de dispositivos](#).
- El informe de servicio debe estar en estado Abierto, En curso o En espera. No puede adjuntar un archivo a un informe de servicio que esté en el estado Cerrado u Otro.
- No puede adjuntar un archivo a un Informe de servicio de *software* abierto para el gestor de recursos.
- Guarde uno o más archivos de almacenamiento de datos de servicio seleccionados en el sistema local desde la tarjeta de Datos del servicio de gestión haciendo clic en el icono **Guardar** (↓). Si se seleccionan varios archivos, estos se comprimen en un solo archivo .tar.gz antes de descargarlos.
- Elimine uno o más archivos de datos de servicio seleccionados que ya no necesite de la tarjeta Datos del servicio de gestión haciendo clic en el icono de **Eliminar** (🗑️) o elimine todos los archivos haciendo clic en el icono de **Eliminar todo** (⊖).

Recopilar datos del servicio de dispositivos

Cuando existe un problema con un dispositivo que requiere la ayuda de un proveedor de servicio como Soporte de Lenovo para su resolución, puede recopilar manualmente los datos de servicio (incluida la información del servicio, el inventario y los registros) correspondientes a ese dispositivo como un archivo en formato tar.gz con el fin de identificar mejor la causa del problema. Puede guardar el archivo de almacenamiento en su sistema local y luego enviar el archivo a su proveedor de servicio de preferencia.

Antes de empezar

Debe aceptar el [Declaración de privacidad de Lenovo](#) antes de poder recopilar datos del servicio. Puede aceptar la declaración de privacidad haciendo clic en **Administración** (⚙️) → **Servicio y soporte** y haciendo clic en **Configuración de Llamar a casa** en el panel de navegación izquierdo y, a continuación, seleccionando **Acepto la declaración de privacidad de Lenovo**.

Para obtener información acerca de cómo guardar los datos del servicio para XClarity Orchestrator en su sistema local, consulte [“Recopilación de datos de servicio para XClarity Orchestrator”](#) en la [página 204](#).

Para obtener información acerca de abrir manualmente un informe de servicio y enviar datos de servicio al Centro de soporte de Lenovo, consulte [“Abrir manualmente un informe de servicio en el Centro de Soporte de Lenovo”](#) en la [página 214](#).

Para obtener información acerca de la configuración de Llamar a casa para abrir automáticamente un informe de servicio en el Centro de Soporte de Lenovo y enviar el archivo de datos de servicio cuando ocurre un suceso en un dispositivo, consulte [“Apertura automática de informes de servicio mediante la función Llamar a casa”](#) en la [página 210](#).

Acerca de esta tarea

Cuando se recopilan datos de servicio a través de Lenovo XClarity Orchestrator, el servidor de organización envía la solicitud al gestor de recursos (como Lenovo XClarity Administrator). El gestor de recursos recopila y guarda los datos como archivo en su repositorio local y, a continuación, o transfiere a XClarity Orchestrator.

Puede recopilar datos del servicio para un máximo de **50** dispositivos por vez.

Procedimiento

Para recopilar los datos de servicio para un dispositivo específico, lleve a cabo los pasos siguientes.

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

Acciones de dispositivo

Todas las acciones ▼ Filtros ▼ Q Buscar X

<input type="checkbox"/>	Dispositiv	Estado	Tipo	Conectiv	Alimentac	Direccion	Grupos	Nombre d	Tipo de di
<input type="checkbox"/>	IO M...	...	Switch	10.243:	No Disp	IBM F...	Conm...
<input type="checkbox"/>	Newp...	...	Server	10.243)	No Disp	Lenov...	Servi...
<input type="checkbox"/>	IO M...	...	Switch	192.168	No Disp	IBM F...	Conm...
<input type="checkbox"/>	IO M...	...	Switch	10.243:	No Disp	IBM F...	Conm...
<input type="checkbox"/>	IO M...	...	Switch	10.243:	No Disp	IBM F...	Conm...
<input type="checkbox"/>	IO M...	...	Switch	10.243:	No Disp	IBM F...	Conm...
<input type="checkbox"/>	ite-bt...	...	Server	10.243:	No Disp	Lenov...	Servi...
<input type="checkbox"/>	IO M...	...	Switch	10.243:	No Disp	IBM F...	Conm...
<input type="checkbox"/>	IO M...	...	Switch	10.243:	No Disp	IBM F...	Conm...
<input type="checkbox"/>	IO M...	...	Switch	0.0.0.0,	No Disp	IBM F...	Conm...

0 Seleccionado / 84 Total Filas por página: 10

1 2 3 4 5

Paso 2. Seleccione el dispositivo para el que desea recopilar datos del servicio y luego haga clic en el icono **Recopilar datos del servicio** (↓).

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

Paso 3. Haga clic en **Datos de servicio de dispositivo** en el panel de navegación izquierdo para mostrar la tarjeta Datos de servicio. El archivo de datos de servicio se muestra en la tabla.

Datos de servicio de dispositivo

Use esta página para descargar archivos de diagnóstico recopilados de los dispositivos.

Todas las acciones ▼ Filtros ▼ Q Buscar X

<input type="checkbox"/>	Archivo	Dispositivo	Fecha y hora	Grupos
<input type="checkbox"/>	7916AC1_SLOT0...	*node03_1	4/10/22 14:26	No Disponible

0 Seleccionado / 1 Total Filas por página: 15

Paso 4. Opcionalmente, guarde el archivo de servicio en el sistema local seleccionando el archivo haciendo clic en el icono **Guardar** (↓).

Después de finalizar

También puede llevar a cabo estas acciones relacionadas.

- Abra manualmente un informe de servicio para un dispositivo específico en la tarjeta Informes de servicio de la página Servicio específico de dispositivo, haciendo clic en el icono **Abrir informe de servicio** (📄) (consulte [Abrir manualmente un informe de servicio en el Centro de Soporte de Lenovo](#)).
- Adjunte un archivo de datos de servicio a un informe de servicio activo seleccionado en la tarjeta Informes de servicio de la página Servicio específico de dispositivo, haciendo clic en el icono **Adjuntar archivo de servicio** (📎). Puede adjuntar un archivo desde XClarity Orchestrator o desde el sistema local.

Notas:

- Puede adjuntar un archivo único que no sea superior a 2 GB. El nombre de archivo no debe superar los 200 caracteres. Para obtener información sobre cómo crear archivos de datos de servicio, consulte [Recopilar datos del servicio de dispositivos](#).
- El informe de servicio debe estar en estado Abierto, En curso o En espera. No puede adjuntar un archivo a un informe de servicio que esté en el estado Cerrado u Otro.
- No puede adjuntar un archivo a un Informe de servicio de *software* abierto para el gestor de recursos.
- Guarde uno o más archivos de almacenamiento de datos de servicio seleccionados en el sistema local desde la tarjeta de Datos de servicio haciendo clic en el icono **Guardar** (↓). Si se seleccionan varios archivos, estos se guardan como un solo archivo .tar.gz.

Nota: Puede guardar un máximo de **50** archivos de datos del servicio en el sistema local al mismo tiempo.

- Elimine uno o más archivos de datos de servicio seleccionados que ya no necesite de la tarjeta Datos de servicio haciendo clic en el icono de **Eliminar** (🗑️) o elimine todos los archivos haciendo clic en el icono de **Eliminar todo** (⊖).

Nota: Debe ser miembro del grupo **SupervisorGroup** para eliminar todos los archivos.

Importación de datos del servicio para dispositivos

Puede importar un archivo de datos del servicio para un dispositivo específico. El archivo se puede recuperar desde un gestor de recursos de Lenovo XClarity Administrator o directamente desde el controlador de gestión de la placa base.

Acerca de esta tarea

Puede importar hasta 10 archivos a la vez con un total combinado de 2 GB o menos.

Si importa datos de servicio para el dispositivo de almacenamiento varias veces, los datos de servicio que se importan último sobrescriben los datos de inventario.

Procedimiento

Para importar un archivo de datos de servicio, lleve a cabo los siguientes pasos.

- Paso 1. En la barra de menú de XClarity Orchestrator, haga clic en **Administración** (⚙️) → **Servicio y soporte** y luego haga clic en **Datos de servicio** en el panel de navegación izquierdo para mostrar la tarjeta Datos del servicio de dispositivo.
- Paso 2. Haga clic en el icono **Importar** (📁) para importar archivos de datos de servicio.
- Paso 3. Arrastre uno o varios archivos de datos de servicio (en formato .tar.gz, tzz o tgz) al cuadro de diálogo Importar o haga clic en **Examinar** para ubicar el archivo.
- Paso 4. Seleccione **Añadir el servidor en los datos de servicio al inventario solo para revisión** si el archivo es para un dispositivo que no está gestionado en la actualidad mediante XClarity Orchestrator.

Paso 5. Haga clic en **Importar** para importar y analizar el archivo y, opcionalmente, gestionar el dispositivo fuera de línea.

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

Creación y asignación de contactos para el servicio y el soporte

Cuando los recursos requieren la asistencia del Soporte de Lenovo, Lenovo necesita saber con quién ponerse en contacto. Puede definir la información de contacto en un solo lugar y asignar esos contactos como contactos principales y secundarios predeterminados para recursos específicos.

Antes de empezar

Asegúrese de que se acepta [Declaración de privacidad de Lenovo](#). Puede revisar y aceptar la declaración de privacidad desde la página **Administración** → **Servicio y soporte** → **Configuración de Llamar a casa**.

Acerca de esta tarea

Puede asignar contactos principales y secundarios a grupos de recursos. Cuando asigne contactos a un grupo de recursos, los contactos se asignan a todos los recursos de ese grupo.

La asignación de contactos principales y secundarios es opcional; sin embargo, si desea asignar un contacto secundario, también debe asignar un contacto principal.

Si un dispositivo pertenece a varios grupos, es posible que a cada grupo se le asigne un contacto principal diferente. Puede elegir usar la asignación de contacto principal para el primer grupo o el último grupo al que se asignó el dispositivo (consulte [Abrir manualmente un informe de servicio en el Centro de Soporte de Lenovo](#)).

Si un dispositivo no pertenece a un grupo con un contacto principal asignado, el contacto de Llamar a casa se asigna de forma predeterminada. El contacto de Llamar a casa se usa cuando los informes de servicio se abren automáticamente mediante Llamar a casa (consulte [Apertura automática de informes de servicio mediante la función Llamar a casa](#)). Los contactos asignados a recursos y grupos tienen prioridad sobre el contacto de Llamar a casa predeterminado.

Cuando abra manualmente un informe de servicio, puede elegir usar los contactos asignados al recurso del problema o puede elegir otro contacto (consulte [Abrir manualmente un informe de servicio en el Centro de Soporte de Lenovo](#)).

Procedimiento

• Definir un contacto

1. En la barra de menú de Lenovo XClarity Orchestrator, haga clic en **Administración** (⚙️) → **Servicio y soporte** y luego haga clic en **Información de contacto** en el panel de navegación izquierdo para mostrar la tarjeta Información de contacto.
2. Haga clic en el icono **Crear** (+) para mostrar el cuadro de diálogo Agregar contacto.
3. Rellene el nombre del contacto, el correo electrónico, el número de teléfono y la ubicación.
4. Seleccione el método de contacto preferido.
5. Haga clic en **Guardar** para crear el contacto.

• Asignar contactos a grupos de recursos

1. En la barra de menú de Lenovo XClarity Orchestrator, haga clic en **Recursos** (⚙️) → **Grupos** para mostrar la tarjeta Grupos.
2. Seleccione el grupo y haga clic en el icono **Editar** (✎) para mostrar el cuadro de diálogo Editar.
3. Seleccione el grupo de recursos.
4. Haga clic en la pestaña **información de contacto**.
5. Seleccione el contacto de soporte principal y uno o más contactos de soporte secundarios para asignarlos a todos los dispositivos del grupo.
6. Haga clic en **Guardar**.

Después de finalizar

Puede realizar las siguientes acciones desde la tarjeta de información de contacto.

- Haga clic en el icono **Editar** (✎) para modificar un contacto seleccionado.
- Haga clic en el icono **Eliminar** (🗑️) para eliminar un contacto seleccionado.

Apertura automática de informes de servicio mediante la función Llamar a casa

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

Antes de empezar

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

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

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

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

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

Cuando los contactos están en los siguientes países, Llamar a casa requiere un contrato de soporte técnico de Lenovo. Para obtener más información, póngase en contacto con su representante de Lenovo o un business partner autorizado.

- Catar
- Arabia Saudita
- Emiratos Árabes Unidos

Acerca de esta tarea

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

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

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

Para obtener información sobre cómo ver los informes de servicio que se han abierto automáticamente mediante la función Llamar a casa, consulte .

Procedimiento

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

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

Configuración de Llamar a casa

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

[Declaración de privacidad de Lenovo](#)

Acepto la declaración de privacidad de Lenovo

Detalles del cliente

Número de cliente

Contacto principal para uso de varias asignaciones de grupos ?

Primera asignación de grupo

Última asignación de grupo

Contacto predeterminado

Estado de Llamar a casa: Habilitado Deshabilitado

Nombre de contacto	Calle
<input type="text"/>	<input type="text"/>
Correo electrónico	Ciudad
<input type="text"/>	<input type="text"/>
Número de teléfono	Estado/provincia
<input type="text"/>	<input type="text"/>
Nombre de la empresa	País/región
<input type="text"/>	<input type="text"/>
Método para contacto	Código zip/código postal
<input type="text"/>	<input type="text"/>

Ubicación del sistema ?

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

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

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

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

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

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

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

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



Paso 7. Rellene la información de ubicación del sistema.

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


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

Después de finalizar

Puede realizar las acciones siguientes que están relacionadas con los datos de servicio.

- Restablezca la configuración de Llamar a casa a los valores predeterminados haciendo clic en **Restablecer configuración**.
- Ver información sobre *todos* los informes de servicio enviados al Centro de soporte de Lenovo, ya sea de manera automática o manual, utilizando Llamar a casa, haciendo clic en **Informes de servicio** en el panel de navegación izquierdo. Para obtener más información, consulte el apartado [Visualización de estados e informes de servicio](#).
- Recopile los datos del servicio de un dispositivo seleccionado de la tarjeta Acciones de dispositivo, seleccione el dispositivo y, a continuación, haga clic en el icono **Recopilar datos del servicio** (). Para obtener más información, consulte el apartado [Recopilar datos del servicio de dispositivos](#).
- Adjunte un archivo de datos de servicio a un informe de servicio activo seleccionado en la tarjeta Informes de servicio de la página Servicio específico de dispositivo, haciendo clic en el icono **Adjuntar archivo de servicio** (). Puede adjuntar un archivo desde XClarity Orchestrator o desde el sistema local.

Notas:

- Puede adjuntar un archivo único que no sea superior a 2 GB. El nombre de archivo no debe superar los 200 caracteres. Para obtener información sobre cómo crear archivos de datos de servicio, consulte [Recopilar datos del servicio de dispositivos](#).
- El informe de servicio debe estar en estado Abierto, En curso o En espera. No puede adjuntar un archivo a un informe de servicio que esté en el estado Cerrado u Otro.
- No puede adjuntar un archivo a un Informe de servicio de *software* abierto para el gestor de recursos.
- Abra manualmente un informe de servicio en el Centro de soporte de Lenovo, recopile los datos de servicio de un dispositivo específico y envíelos al Centro de soporte de Lenovo desde la tarjeta Acciones de dispositivo, seleccionando el dispositivo y haciendo clic en el icono **Abrir informe de servicio** (). Para obtener más información, consulte el apartado [Abrir manualmente un informe de servicio en el Centro de Soporte de Lenovo](#). Si el Centro de soporte de Lenovo requiere datos adicionales, el soporte de Lenovo podría pedirle que vuelva a recopilar los datos de servicio de ese mismo u otro dispositivo.

Abrir manualmente un informe de servicio en el Centro de Soporte de Lenovo

Si Llamar a casa se habilita mediante un despachador de servicio y se produce un suceso en un dispositivo gestionado, Lenovo XClarity Orchestrator abre automáticamente un informe de servicio, recopila los archivos de servicio para el dispositivo gestionado y envía los archivos automáticamente al Centro de Soporte de Lenovo. También puede recopilar los archivos de servicio para un dispositivo gestionado de forma manual como un archivo, guardar el archivo al sistema local y enviarlos al Centro de Soporte de Lenovo en cualquier momento. Al abrir un informe de servicio se inicia el proceso para determinar una resolución a sus problemas de hardware poniendo la información relevante a disposición de soporte de Lenovo de forma rápida y eficiente. Los técnicos de servicio de Lenovo podrán empezar a trabajar en la búsqueda de una resolución en cuanto haya abierto un informe de servicio.

Antes de empezar

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

- Asegúrese de que la información de contacto de Llamar a casa esté configurada y habilitada ([Apertura automática de informes de servicio mediante la función Llamar a casa](#)).
- Asegúrese de que XClarity Orchestrator pueda comunicarse con el Centro de Soporte de Lenovo haciendo clic en **Administración** (🔧) → **Servicio y soporte** en la barra de menú de XClarity Orchestrator y haciendo clic en **Configuración de Llamar a casa** en el panel de navegación izquierdo para mostrar la página Configuración de Llamar a casa. Luego, haga clic en **Prueba de configuración de Llamar a casa** para generar un suceso de prueba y verificar que XClarity Orchestrator pueda comunicarse con el Centro de Soporte de Lenovo.
- Asegúrese de que todos los puertos requeridos por XClarity Orchestrator (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 Orchestrator.
- Asegúrese de que exista una conexión a las direcciones de Internet requeridas por la opción Llamar a casa. Para obtener más información acerca de los firewall, consulte [Firewall y servidores proxy](#) en la documentación en línea de XClarity Orchestrator.
- Si XClarity Orchestrator accede a Internet mediante un proxy HTTP, asegúrese de que el servidor proxy esté configurado para usar la autenticación básica y que no esté configurado como un proxy de terminación. Para obtener más información acerca de la configuración de proxy, consulte [Configurar valores de red](#).

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

Acerca de esta tarea

Cuando abra manualmente un informe de servicio, puede elegir usar los contactos asignados al recurso del problema o puede elegir otro contacto.



Cuando se asignan los contactos principales y secundarios a un grupo, esos contactos se asignan a cada dispositivo de ese grupo. A cada dispositivo se le puede asignar un contacto principal y uno o varios contactos secundarios. Si un dispositivo pertenece a varios grupos, todos los contactos secundarios

asignados a todos los grupos de los que el dispositivo pertenece se asignan al dispositivo. Si un dispositivo pertenece a varios grupos, es posible que a cada grupo se le asigne un contacto principal diferente. Puede elegir usar la asignación de contacto principal para el primer grupo o el último grupo al que se asignó el dispositivo (consulte [Apertura automática de informes de servicio mediante la función Llamar a casa](#)).

Si un dispositivo no pertenece a un grupo con un contacto principal asignado, el contacto de Llamar a casa se asigna de forma predeterminada. El contacto de Llamar a casa se usa cuando los informes de servicio se abren automáticamente mediante Llamar a casa (consulte [Apertura automática de informes de servicio mediante la función Llamar a casa](#)). Los contactos asignados a recursos y grupos tienen prioridad sobre el contacto de Llamar a casa predeterminado.


Procedimiento

Para abrir manualmente un informe de servicio, lleve a cabo los pasos siguientes.

- Si Llamar a casa está configurado y habilitado, lleve a cabo los pasos siguientes para abrir un informe de servicio, recopilar los datos de servicio y envíe los archivos al Centro de soporte de Lenovo.
 1. Desde la barra de menú de XClarity Orchestrator, haga clic en **Recursos**  y luego haga clic en el tipo de dispositivo para mostrar una tarjeta con una vista de tabla de todos los dispositivos gestionados de ese tipo.
 2. Haga clic en la fila del dispositivo para mostrar las tarjetas de resumen del dispositivo para dicho dispositivo.
 3. Haga clic en **Servicio** en el panel de navegación izquierdo para mostrar la tarjeta Informe de servicio.
 4. Haga clic en el icono **Abrir informe de servicio**  para mostrar el cuadro de diálogo Agregar nuevo informe.
 5. Proporcione una descripción del problema informado e incluya cualquier código de suceso pertinente.
 6. Opcionalmente, elija la gravedad del problema. Puede presentar uno de los valores siguientes.
 - **Urgente**
 - **Alto**
 - **Medio** (predeterminado)
 - **Bajo**
 7. Haga clic en **Enviar**.
- Cuando Llamar a casa está configurado y habilitado, y se produce un suceso de mantenimiento en un dispositivo específico, XClarity Orchestrator abre *automáticamente* un informe de servicio y transfiere los datos de servicio de ese dispositivo al Centro de Soporte de Lenovo.

Después de finalizar

Puede realizar las siguientes acciones desde la página de Servicio específico de dispositivo.

- Ver información acerca de *todos* los informes de servicio abiertos haciendo clic en **Servicio y soporte** → **Informes de servicio** en la barra de menús de XClarity Orchestrator.
- Agregue una nota a un informe de servicio seleccionado haciendo clic en el icono **Añadir nota de informe de servicio** .

Notas:

- El informe de servicio debe estar en estado Abierto, En curso o En espera. No puede agregar una nota a un informe de servicio que está en el estado Cerrado u Otro.
- Puede agregar una nota solo a los informes de servicio de Lenovo. No puede agregar una nota a los informes de servicio de IBM, Service Now o Cherwill.

- No puede agregar una nota a un informe de servicio de *software* abierto para un gestor de recursos.
- Adjunte un archivo de datos de servicio a un informe de servicio activo seleccionado en la tarjeta Informes de servicio de la página Servicio específico de dispositivo, haciendo clic en el icono **Adjuntar archivo de servicio** (+). Puede adjuntar un archivo desde XClarity Orchestrator o desde el sistema local.

Notas:

- Puede adjuntar un archivo único que no sea superior a 2 GB. El nombre de archivo no debe superar los 200 caracteres. Para obtener información sobre cómo crear archivos de datos de servicio, consulte [Recopilar datos del servicio de dispositivos](#).
- El informe de servicio debe estar en estado Abierto, En curso o En espera. No puede adjuntar un archivo a un informe de servicio que esté en el estado Cerrado u Otro.
- No puede adjuntar un archivo a un Informe de servicio de *software* abierto para el gestor de recursos.

Visualización de estados e informes de servicio

Puede ver la información sobre los informes de servicio que se crearon de forma manual o se enviaron de forma automática al Centro de Soporte de Lenovo a través de Llamar a casa y de los informes de servicio que se generaron mediante servicios de soporte distintos de Llamar a casa.

Acerca de esta tarea

El estado del informe de servicio se sincroniza con el Centro de Soporte de Lenovo cada 24 horas.

La columna **Estado** identifica el estado del informe de servicio. Un informe de servicio puede estar en uno de los siguientes estados.

- **Activo**
- **Respondido**
- **Cancelado**
- **Cancelado**
- **Creado**
- **Ciente cancelado**
- **Cerrado**
- **Parte rechazada**
- **Duplicado**
- **Error**
- **Estado de error**
- **En progreso**
- **Inicializado**
- **Combinado**
- **Supervisión: solución desplegada**
- **Nuevo**
- **En espera**
- **Pendiente**
- **Iniciación del problema**
- **Problema resuelto**
- **Procesando**
- **Rechazado**
- **Investigando**
- **Resuelto**
- **Solución proporcionada**
- **Enviado**
- **Desconocido**
- **Esperando**

- Esperando detalles
- Esperando el soporte interno de Lenovo
- Esperando soporte externo
- Esperando los comentarios de los clientes sobre la solución
- Esperando el despliegue de la solución
- Transferido a servicios gestionados
- Transferencia en activo
- Trabajo en progreso

La columna **Tipo** identifica el tipo de informe de servicio que se enumera en la columna Número de informe de servicio. El tipo service-ticket puede ser uno de los valores siguientes.

- Informe de Cherwill
- Informe de Llamar a casa de IBM
- Lenovo Call Home Ticket
- Informe de paso de Llamar a casa de Lenovo
- Informe de Llamar a casa de software de Lenovo
- ServiceNow

Procedimiento

- **Ver los estados de todos los informes de servicio** Haga clic en **Administración** (⚙️) → **Servicio y soporte** y luego haga clic en **Informes de servicio** en el panel de navegación izquierdo para mostrar la tarjeta de Informes de servicio.

Consejo: Haga clic en el ID del suceso para mostrar un resumen del suceso que ha generado el informe de servicio, incluida la acción del usuario en caso de que la hubiera.







<input type="checkbox"/>	Número de i	Estado	ID de suces	Descripción	Nombre del	Número de:	Fecha de cre
<input type="checkbox"/>	100103...	En pr...	FQXXOSSl	test_ticket	Abyss-S...	ABYSSR...	11/9/23 ...
<input type="checkbox"/>	100103...	En pr...	806F010C	Uncorre...	Abyss-S...	ABYSSR...	11/9/23 ...

0 Seleccionado / 2 Total Filas por página: 15

- **Ver el estado de los informes de servicio para un dispositivo específico**
 1. Desde la barra de menú de XClarity Orchestrator, haga clic en **Recursos** (⚙️) y luego haga clic en el tipo de dispositivo para mostrar una tarjeta con una vista de tabla de todos los dispositivos gestionados de ese tipo.
 2. Haga clic en la fila del dispositivo para mostrar las tarjetas de resumen del dispositivo para dicho dispositivo.
 3. Haga clic en **Servicio** en el menú de navegación izquierdo para mostrar la tarjeta de Informes de servicio con una lista de todos los informes de servicio para el dispositivo.

Consejo: Haga clic en el ID del suceso para mostrar un resumen del suceso que ha generado el informe de servicio, incluida la acción del usuario en caso de que la hubiera.

Informes de servicio










 Todas las acciones ▾ Filtros ▾

<input type="checkbox"/>	Número de infor	Estado	ID de suceso	Descripción	Número de serie	Fecha de creació
<input type="checkbox"/>	1001032647	En pr...	FQXXOSS00	test_ticket	ABYSSR093	11/9/23 5:...
<input type="checkbox"/>	1001032643	En pr...	806F010C2C	Uncorrecta...	ABYSSR093	11/9/23 4:...


0 Seleccionado / 2 Total Filas por página: 15 ▾

Después de finalizar


Puede realizar las acciones siguientes que están relacionadas con los informes de servicio.

- Configure XClarity Orchestrator para que automáticamente se abra un informe de servicio cuando se produzca un suceso que se puede reparar (consulte [“Apertura automática de informes de servicio mediante la función Llamar a casa” en la página 210](#)).
- Sincronizar los datos con el centro de soporte de Lenovo y actualizar el estado de todos los informes de servicio activos haciendo clic en el icono **Actualizar estado de informe de servicio** .
- Abra manualmente un informe de servicio para un dispositivo específico en la tarjeta Informes de servicio de la página Servicio específico de dispositivo, haciendo clic en el icono **Abrir informe de servicio** .
- Agregue una nota a un informe de servicio seleccionado haciendo clic en el icono **Añadir nota de informe de servicio** .

Notas:

- El informe de servicio debe estar en estado Abierto, En curso o En espera. No puede agregar una nota a un informe de servicio que está en el estado Cerrado u Otro.
- Puede agregar una nota solo a los informes de servicio de Lenovo. No puede agregar una nota a los informes de servicio de IBM, Service Now o Cherwill.
- No puede agregar una nota a un informe de servicio de *software* abierto para un gestor de recursos.
- Adjunte un archivo de datos de servicio a un informe de servicio activo seleccionado en la tarjeta Informes de servicio de la página Servicio específico de dispositivo, haciendo clic en el icono **Adjuntar archivo de servicio** . Puede adjuntar un archivo desde XClarity Orchestrator o desde el sistema local.

Notas:

- Puede adjuntar un archivo único que no sea superior a 2 GB. El nombre de archivo no debe superar los 200 caracteres. Para obtener información sobre cómo crear archivos de datos de servicio, consulte [Recopilar datos del servicio de dispositivos](#).
- El informe de servicio debe estar en estado Abierto, En curso o En espera. No puede adjuntar un archivo a un informe de servicio que esté en el estado Cerrado u Otro.
- No puede adjuntar un archivo a un Informe de servicio de *software* abierto para el gestor de recursos.
- Reenvía los informes sobre los informes de servicio activos de forma periódica a una o varias direcciones de correo electrónico haciendo clic en el icono **Crear despachador de informes** . El informe se envía utilizando los filtros de datos aplicados actualmente a la tabla. Todas las columnas de la tabla mostradas y ocultas se incluyen en el informe. Para obtener más información, consulte .

- Añada un informe de informes de servicio activos a un despachador de informes específico utilizando los filtros de datos aplicados actualmente a la tabla haciendo clic en el icono de **Agregar a despachador de informes** (↗). Si el despachador de informes ya incluye un informe de informes de servicio activos, este se actualiza para utilizar los filtros de datos actuales.

Ver información de garantía

Puede determinar el estado de la garantía (incluidas las garantías extendidas) de los dispositivos gestionados.

Antes de empezar

Lenovo XClarity Orchestrator debe acceder a las URL siguientes para recopilar información de garantía para los dispositivos gestionados. Asegúrese de que no haya firewall que bloqueen el acceso a estas URL. Para obtener más información, consulte [Firewall y servidores proxy](#) en la documentación en línea de XClarity Orchestrator.

- Base de datos de Lenovo Warranty (mundial) - <https://ibase.lenovo.com/POIRequest.aspx>
- Servicio web de Lenovo Warranty - <http://supportapi.lenovo.com/warranty/> o <https://supportapi.lenovo.com/warranty/>

Notas:

- Actualmente no se admite el soporte de garantía para usuarios en China.
- Las garantías se enumeran para el chasis, pero no los correspondientes Chassis Management Module (CMM).





Acerca de esta tarea



La información de garantía se recupera semanalmente para los dispositivos que tienen garantía y diariamente para aquellos dispositivos que no la tienen.

Procedimiento

Para ver la información de garantía, haga clic en **Administración** (⚙️) → **Servicio y soporte** y luego en **Garantía** en el panel de navegación izquierdo para mostrar la tarjeta Garantía.





Garantía





 Todas las acciones ▾ Filtros ▾

 Buscar 




Dispositivo	Estado	Nombre del	Tipo-Modelo	Número de	Número de	Fecha de in	Fecha de ca	Grupos
*node02_	No Dis...	IBM Flex	7916/...	No Dispc	SLOT002	No Dispc	No Dispo	No Dispc
*node02_	No Dis...	IBM Flex	7916/...	No Dispc	SLOT002	No Dispc	No Dispo	No Dispc
*node03_	No Dis...	IBM Flex	7916/...	No Dispc	SLOT003	No Dispc	No Dispo	No Dispc
*node03_	No Dis...	IBM Flex	7916/...	No Dispc	SLOT003	No Dispc	No Dispo	No Dispc
*node06_	No Dis...	IBM Flex	7916/...	No Dispc	SLOT006	No Dispc	No Dispo	No Dispc
*node06_	No Dis...	IBM Flex	7916/...	No Dispc	SLOT006	No Dispc	No Dispo	No Dispc
*node09_	No Dis...	IBM Flex	7916/...	No Dispc	SLOT009	No Dispc	No Dispo	No Dispc
*node09_	No Dis...	IBM Flex	7916/...	No Dispc	SLOT009	No Dispc	No Dispo	No Dispc
*node11_	No Dis...	IBM Flex	7916/...	No Dispc	SLOT011	No Dispc	No Dispo	No Dispc
*node11_	No Dis...	IBM Flex	7916/...	No Dispc	SLOT011	No Dispc	No Dispo	No Dispc
10.243.1	No Dis...	Lenovo F	9532/...	No Dispc	06DGCV	No Dispc	No Dispo	No Dispc
10.243.1	No Dis...	IBM Flex	8731/...	No Dispc	23LAR6E	No Dispc	No Dispo	No Dispc
10.243.1	No Dis...	IBM Flex	7916/...	No Dispc	CAR206:	No Dispc	No Dispo	No Dispc
10.243.1	No Dis...	IBM Flex	7917/...	No Dispc	06EKZB:	No Dispc	No Dispo	No Dispc
10.243.2	No Dis...	IBM Flex	8737/...	No Dispc	06PGVA:	No Dispc	No Dispo	No Dispc

211 Total Filas por página: 15 ▾



1



Después de finalizar

Puede realizar las siguientes acciones desde la tarjeta Garantía.

- Puede configurar cuando desee que se le notifique la caducidad de la garantía para los dispositivos gestionados haciendo clic en el icono de **Configurar valores de garantía** (). Puede configurar los valores siguientes.
 - Habilite la generación de alertas cuando la garantía del dispositivo esté a punto de caducar.
 - Establezca el número de días antes de que caduque la garantía que desea generar una alerta.
- Busque la información de la garantía (si está disponible) para un dispositivo específico en el sitio web de Soporte de Lenovo haciendo clic en el enlace en la columna **Estado**.
- Reenvíe los informes sobre las garantías de forma periódica a una o varias direcciones de correo electrónico haciendo clic en **Todas las acciones** →  **Añadir despachador de informes**. El informe se envía utilizando los filtros de datos aplicados actualmente a la tabla. Todas las columnas de la tabla mostradas y ocultas se incluyen en el informe.
- Añada un informe de garantías a un despachador de informes específico utilizando los filtros de datos aplicados actualmente a la tabla haciendo clic en el icono de **Agregar a despachador de informes** (.

Si el despachador de informes ya incluye un informe de garantías, este se actualiza para utilizar los filtros de datos actuales.

Lenovo