



Lenovo XClarity Integrator para VMware vCenter Guía del usuario y de instalación



Versión 8.6.0

Nota

Antes de usar esta información y el producto al que da soporte, lea la información contenida en [Apéndice D “Avisos” en la página 77](#).

Trigésima edición (Diciembre 2024)

© Copyright Lenovo 2014, 2024.

Portions © Copyright IBM Corporation 2012, 2024

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

Contenido

Contenido	i
Figurasiii
Tablas	v
Acerca de esta publicación	vii
Convenciones y terminologíavii
Recursos de la Webvii
Capítulo 1. Lenovo XClarity Integrator para VMware vCenter	1
Capítulo 2. Planificación e instalación de LXCI para VMware vCenter.	3
Requisitos del sistema	3
Versiones admitidas de VMware vCenter Server.	3
Versiones compatibles de Lenovo XClarity Administrator	4
Versión ESXi admitida	4
Modelos de servidor compatibles	4
Requisitos de hardware	7
Requisitos de la red	7
Instalación de Lenovo XClarity Integrator para VMware vCenter	10
Habilitar/deshabilitar vSphere Lifecycle Manager	11
Habilitación/deshabilitación de la gestión proactiva del hardware	11
Implementación de alta disponibilidad para Lenovo XClarity Integrator.	12
Actualización de Lenovo XClarity Integrator para VMware vCenter	12
Actualización de LXCI para VMware vCenter en entornos con base VMware ESXi	12
Desinstalación de Lenovo XClarity Integrator para VMware vCenter	14
Capítulo 3. Configuración de Lenovo XClarity Integrator	15
Detección y gestión de BMC.	15
Detección y gestión directa del BMC.	15
Detección y gestión de BMC mediante LXCA	17
Configuración de Lenovo XClarity Administrator	17
Configuración del control de acceso.	19
Importación del certificado de Lenovo XClarity Integrator al navegador web	19

Capítulo 4. Visualización de un resumen del entorno	21
Capítulo 5. Gestión de servidores.	23
Visualización de la información del sistema	23
Inicio de la función de recopilación de diagnóstico del sistema	24
Visualización de sucesos del servidor	24
Visualización del inventario del servidor	24
Visualización de utilización del servidor	25
Trabajo con la topología de hardware	26
Topología de hardware del host.	26
Topología de hardware del clúster.	30
Inicio de la interfaz web de BMC	31
Inicio de la consola remota	31
Uso de la función Actualizaciones de firmware.	32
Uso de la función Política de alimentación	32
Uso de la función Valores del sistema	33
Despliegue de un patrón de configuración en un servidor	33
Uso de la función Opciones de arranque	34
Visualización y exportación de los valores del sistema	35
Capítulo 6. Gestión de clústeres	37
Uso de la función vSphere Lifecycle Manager	37
Importación de los complementos básicos ESXi y Lenovo	37
Gestión de paquetes de firmware	37
Gestión del clúster a través de una imagen	39
Trabajar con la función Gestión proactiva del hardware	41
Visualización de información de salud	41
Uso de la función Rolling System Update (Actualización gradual del sistema)	41
Configuración de las preferencias de Actualización del sistema gradual	42
Gestión de las tareas de la función Rolling System Update (Actualización gradual del sistema)	43
Uso de la función Reinicio gradual del sistema.	47
Gestión de las tareas Reinicio gradual del sistema	47
Trabajo con alta disponibilidad proactiva	50
Habilitación de VMware vCenter HA preventiva con el proveedor de HA preventiva de Lenovo para un clúster	50

Agregar un host en un clúster con HA preventiva habilitada (con un proveedor de Lenovo)	51
Reutilizar el proveedor de HA preventiva de Lenovo	51
Pulsación de alta disponibilidad proactiva.	51
Gestión de sucesos del hardware.	51
Alarmas	51

Capítulo 7. Administración de Lenovo XClarity Integrator. 53

Configuración de conexiones de vCenter	53
Registro de Lenovo XClarity Integrator en un servidor vCenter.	53
Eliminar el registro de Lenovo XClarity Integrator de un servidor vCenter	55
Actualización del software de servidor de gestión	56
Configuración del acceso de red	57
Configuración del nombre de host, el nombre de dominio y DNS	57
Configuración de los valores IP de Eth0	57
Configuración de los valores IP de Eth1	58
Configuración de proxy	59
Configuración del enrutamiento avanzado.	59
Prueba de la conexión de red.	60
Establecimiento de la fecha y la hora	60
Gestión de la capacidad del disco	60
Recopilación de datos de servicio.	60
Gestión de autenticación y autorización	61
Configuración de un servidor de autenticación LDAP externo.	61
Trabajo con certificados de seguridad	64
Generación de un certificado de servidor firmado externamente y personalizado	64
Restauración del certificado de servidor generado por Lenovo XClarity Integrator	65
Regeneración del certificado raíz de la Entidad de certificación (CA)	66
Descarga e instalación de un certificado raíz de la entidad de certificación (CA)	66
Descarga del certificado de servidor	67

Gestión de certificados de confianza.	67
Apagado o reinicio de Lenovo XClarity Integrator	67

Apéndice A. Sucesos de gestión proactiva de hardware compatibles 69

LE-FQXSPSD0002G : Falla prevista en [StorageVolumeElementName] para la matriz [ComputerSystemElementName].	69
LE-FQXSPSD0003G : Se pronostica un error en la unidad [arg1] en el alojamiento/chasis (MTM-SN: [arg2]).	69

Apéndice B. Resolución de problemas 71

Los servidores no se pueden administrar automáticamente cuando se agrega LXCA a LXCI	71
Aparece el mensaje “No healthy upstream” (No hay flujo ascendente en buen estado) en la página de LXCI en vCenter	71
No se muestra la lista de firmware ni de complementos de controladores	71
Error en la función Exploración de BMC	72
No se muestra la página de mapa de chasis, actualización de firmware o patrón de configuración.	72
Lenovo XClarity Integrator no se muestra en el cliente de vSphere después de la instalación	72
Los datos que se muestran en Lenovo XClarity Integrator no están actualizados cuando Lenovo XClarity Integrator se abre en Internet Explorer 11 o versiones posteriores.	73
Los sucesos de hardware de un host se pierden cuando este host se gestiona mediante dos clientes de vCenter	74

Apéndice C. Funciones de accesibilidad 75

Apéndice D. Avisos 77

Marcas registradas	78
Avisos importantes	78

Figuras

1.	Detección y gestión de BMC	16	9.	Página de configuración de “Power Policy (Política de alimentación)”	32
2.	Página Asistente de registro.	18	10.	Página Patrón de configuración	33
3.	Página System Overview (Información general del sistema)	24	11.	Panel “Boot Options (Opciones de arranque)”	35
4.	Página “Inventory” (Inventario).	25	12.	Panel “System Settings” (Valores de sistema)	36
5.	Página “Utilization” (Utilización)	25	13.	Valores de Internet Explorer	74
6.	Topología de hardware.	27			
7.	Detalles del controlador	28			
8.	Estado de la PSU	28			

Tablas

1.	Términos y acrónimos usados con frecuencia.	vii
2.	Matriz de soporte de versiones de VMware vCenter.	3
3.	Matriz de versiones compatibles de Lenovo XClarity Administrator	4
4.	Servidores Lenovo compatibles	5
5.	Servidores IBM compatibles	7
6.	Requisitos de conexión a Internet	8
7.	Servidores y nodos de cálculo	9
8.	Requisitos de conexión a Internet	9
9.	Opciones de migración de datos de vSAN	29
10.	Opciones de migración de datos de vSAN	30
11.	Estados de la tarea Actualización gradual del sistema.	43
12.	Funciones de tareas de actualización continua del sistema.	44
13.	Funciones de tareas de reinicio gradual del sistema.	47
14.	Estado de la tarea Reinicio gradual del sistema.	49

Acerca de esta publicación

En este documento, se proporcionan instrucciones para instalar y utilizar Lenovo XClarity Integrator para VMware vCenter, *Versión 8.6.0*.

En estas instrucciones se incluye información sobre el uso de las funciones para obtener información del sistema, actualizar el firmware, controlar el consumo de energía, configurar los valores del sistema y crear reglas de migración para la máquina virtual en el entorno de gestión de VMware vCenter.

Convenciones y terminología

Los párrafos que comienzan con las palabras **Nota**, **Importante** o **Atención** en negrita son avisos que sirven para resaltar información importante dentro del documento.

Nota: Estos avisos proporcionan consejos importantes, ayuda o consejos.

Importante: Estos avisos proporcionan información o consejos que pueden ayudarle a evitar situaciones incómodas o difíciles.

Atención: Estos avisos indican posibles daños a programas, dispositivos o datos. Un aviso de atención aparece delante de una instrucción o situación en la que puede producirse un daño.

La tabla siguiente describe algunos de los términos, acrónimos y abreviaturas que se utilizan en este documento.

Tabla 1. Términos y acrónimos usados con frecuencia

Término o acrónimo	Definición
BMC	Controlador de gestión de la placa base
LXCA	Lenovo XClarity Administrator
LXCI	Lenovo XClarity Integrator
PFA	Alerta predictiva de errores
UXSP	UpdateXpress System Packs

Recursos de la Web

En los siguientes sitios web se proporcionan recursos para entender, utilizar y resolver problemas en servidores System x, Flex System y BladeCenter, además, se incluyen herramientas de gestión de sistemas.

Sitio de Lenovo XClarity Integrator para VMware vCenter

Busque las descargas más recientes del Lenovo XClarity Integrator para VMware vCenter:

- [Sitio web de Lenovo XClarity Integrator para VMware](#)

Soluciones de Gestión de sistemas con Lenovo XClarity

En este sitio web se proporciona información general acerca de las soluciones de Lenovo XClarity que se integran en el hardware de System x y Flex System para ofrecer funciones de gestión del sistema:

- [Sitio Web de soluciones de gestión de sistemas con Lenovo XClarity](#)

Portal de soporte técnico de Lenovo

Este sitio web ayuda a los usuarios a obtener soporte técnico para el hardware y el software:

- [Sitio web del Portal de soporte de Lenovo](#)

Sitios web de ServerProven

Los siguientes sitios web proporcionan información general acerca de la compatibilidad con el hardware de los servidores BladeCenter, Flex System, System x y xSeries[®]:

- [Lenovo ServerProven: compatibilidad para productos BladeCenter](#)
- [Lenovo ServerProven: compatibilidad para el Chasis Flex System](#)
- [Lenovo ServerProven: compatibilidad para hardware, aplicaciones y middleware de System x](#)

Sitio web de VMware

Este sitio web puede ayudar a los usuarios a encontrar los productos de VMware:

- [Sitio web de VMware](#)

Capítulo 1. Lenovo XClarity Integrator para VMware vCenter

Lenovo XClarity Integrator para VMware vCenter es una extensión de LXCI para VMware vCenter que ofrece funciones de gestión ampliadas a los administradores del sistema en los servidores System x, BladeCenter y Flex System. Lenovo XClarity Integrator para VMware vCenter amplía las funciones de gestión de VMware vCenter integrando funciones de gestión del hardware de Lenovo.

Lenovo XClarity Integrator para VMware vCenter proporciona las siguientes funciones.

Panel de mandos

El panel proporciona:

- Información general de host seleccionados y estados de clúster, incluido el resumen de información del sistema y los mensajes de estado del sistema.
- Información de resumen relativa, entre otros, a la utilización general de recursos, mensajes de estado de host y al estado de la conexión.
- Información de BMC para cada host y permite a los usuarios iniciar la consola de BMC directamente.

Actualizaciones de firmware

Las actualizaciones de firmware adquieren y aplican Lenovo UpdateXpress System Packs (UXSP) y actualizaciones individuales a un sistema ESXi. La función Actualización gradual del sistema permite realizar actualizaciones no perturbadoras del sistema sin que se produzcan tiempos de inactividad en absoluto; además, automatiza el proceso de actualización de los hosts en un entorno de clústeres sin que haya interrupciones en la carga de trabajo y admite la actualización de varios hosts a la vez para ahorrar tiempo.

Medición de la alimentación

La función Power Metric (Medición de la alimentación) permite realizar operaciones de supervisión y ofrece un resumen del consumo de alimentación, del historial térmico y de la velocidad del ventilador; además, presenta un gráfico de tendencias del host gestionado. Los usuarios también pueden definir la limitación de alimentación para un host con capacidades para ello con el fin de restringir el consumo de alimentación del servidor.

Advanced Settings Utility

ASU gestiona los valores actuales del sistema en el host, incluidos los valores relativos a BMC, Unified Extensible Firmware Interface (UEFI) y al orden de arranque.

Gestión predictiva de errores

La función Predictive failure management (Gestión predictiva de errores) permite supervisar el estado del hardware del servidor y recibir alertas predictivas de errores. Los usuarios pueden establecer una política de gestión para un servidor sobre la base de alertas predictivas de errores para evacuar automáticamente las máquinas virtuales en respuesta a Alertas predictivas de errores para proteger sus cargas de trabajo o para notificarles tales alertas. La función Predictive failure management (Gestión predictiva de errores) se habilita o deshabilita manualmente en un host.

Función Actualización gradual del sistema

La función Actualización gradual del sistema (RSU) actualiza el firmware en un único paso mientras el sistema continúa ejecutándose sin interrupción en los servicios de aplicación de un host de servidor. La función RSU proporciona un enfoque de actualizaciones de firmware no disruptivas. Permite la gestión completa del firmware aprovechando el movimiento dinámico de la máquina virtual y el reinicio automático del host dentro de un clúster VMware definido sin que haya interrupciones en la carga de trabajo.

Reinicio gradual del sistema

La función Reinicio gradual del sistema (RSR) ofrece un mecanismo de reinicio automático continuo aprovechando el movimiento dinámico de la máquina virtual y el reinicio automático host dentro de un clúster VMware definido sin que haya interrupciones en la carga de trabajo.

Vista de topología de hardware para servidores de dispositivo ThinkAgile VX

La función de topología de hardware proporciona una vista gráfica integrada para los servidores de dispositivos ThinkAgile VX. Muestra el diseño del servidor, el inventario de hardware detallado y la información de estado, y proporciona un asistente guiado para gestionar los discos vSAN.

Integración de Lenovo XClarity Administrator

Lenovo XClarity Integrator se integra con Lenovo XClarity Administrator para proporcionar un método conveniente para automatizar la detección del servidor Lenovo, visualizar la vista de mapa de inventario de los servidores gestionados, la configuración de servidores con patrones de configuración y organizar el despliegue continuo de una política de firmware.

Integración de vSphere Lifecycle Manager (vLCM)

Lenovo XClarity Integrator se integra con vSphere Lifecycle Manager (vLCM), que se presentó en vSphere 7.0, para proporcionar un método útil para orquestar las actualizaciones de firmware a través de una imagen de ancho de clúster definida.

Capítulo 2. Planificación e instalación de LXCI para VMware vCenter

Utilice este procedimiento para planificar e instalar Lenovo XClarity Integrator para VMware vCenter.

Requisitos del sistema

Esta sección describe los requisitos del sistema para Lenovo XClarity Integrator para VMware vCenter.

Versiones admitidas de VMware vCenter Server

Lenovo XClarity Integrator para VMware vCenter es una extensión de VMware vCenter Server.

Desde la versión 6.0.0, Lenovo XClarity Integrator admite solo VMware vCenter 6.5 (U2) y versiones posteriores, solo puede tener acceso a través del cliente de vSphere HTML. El cliente de vSphere Flex ya no es compatible.

Dependiendo de la versión de VMware vCenter y del cliente de vSphere que se esté utilizando, seleccione la versión correcta de Lenovo XClarity Integrator según la siguiente matriz:

Tabla 2. Matriz de soporte de versiones de VMware vCenter

Versión de VMware vCenter	Versión de Lenovo XClarity Integrator		
	5.5.0 (Solo admite cliente Flex)	7.7.0 (Solo admite cliente HTML)	8.6.0
8.0 (U1, U2, U3)	X	X	√
8.0 GA	X	X	√
7.0 (U3)	X	√	√
7.0 (U1, U2)	X	√	X
7.0 GA	X	√	X
6.7 (U1, U2, U3)	√	√	X
6.5 (U2, U3)	√	√	X
6.5 (U1)	√	X	X
6.5	√	X	X
Versiones 6.0 y anteriores	√	X	X

Notas:

- Si la versión del VMware vCenter de destino es anterior a 6.5 (U2) o si los usuarios van a utilizar LXCI con el cliente vSphere Flex, no actualice LXCI a la versión 6.0.0.
- Si la versión de VMware vCenter de destino es anterior a la 7.0 (U1), no actualice LXCI a la versión 8.0.0.

Versiones compatibles de Lenovo XClarity Administrator

Tabla 3. Matriz de versiones compatibles de Lenovo XClarity Administrator

LXCA	Versión de LXCI										
	7.4.0	7.5.0	7.6.0	7.7.0	8.0.0	8.1.0	8.2.0	8.3.0	8.4.0	8.5.0	8.6.0
4.2	X	X	X	X	X	X	X	X	X	X	√
4.1	X	X	X	X	X	X	X	X	X	√	X
4.0	X	X	X	X	X	√	√	√	√	√	X
3.6	X	X	√	√	√	√	√	√	√	X	X
3.5	X	√	√	√	√	√	√	√	√	X	X

Versión ESXi admitida

Lenovo XClarity Integrator para VMware vCenter admite tanto Lenovo imágenes personalizadas VMware vSphere Hypervisor (ESXi) como imágenes estándar de VMware ESXi. Se admiten las siguientes versiones.

- 8.0
- 7.0
- 6.7
- 6.5
- 6.0

Los usuarios pueden descargar imágenes de ESXi personalizadas de Lenovo desde el sitio web de descargas de productos de VMware: <https://my.vmware.com/web/vmware/downloads>. Localice VMware vSphere y haga clic en el enlace **Download Product** (Descargar producto). A continuación haga clic en la pestaña **Custom ISOs** (ISO personalizadas) para ubicar la imagen de Lenovo para ESXi.

Modelos de servidor compatibles

Este tema proporciona información acerca de los modelos de servidor admitidos para Lenovo XClarity Integrator para VMware vCenter.

El complemento de XClarity Integrator no tiene limitaciones de modelos de servidor. No obstante, el hardware que gestiona el plug-in está limitado a los modelos de servidor de Lenovo que se incluyen en la siguiente tabla.

Tabla 4. Servidores Lenovo compatibles

Serie	Modelos de servidor	
ThinkSystem	<ul style="list-style-type: none"> • SD530 (7X20, 7X21, 7X22) • SD530 V3 (7DD3, 7DDA) • SD535 V3 (7DD1, 7DD8) • SD550 V3 (7DD2, 7DD9) • SD630 V2 (7D1K) • SE350 (7Z46, 7D1X, 7D27) • SN550 (7X16) • SN550 V2 (7Z69) • SN850 (7X15) • SR150 (7Y54) (solo China) • SR158 (7Y55) • SR250 (7Y51, 7Y52) (en todo el mundo, excepto en la India) • SR250 (7Y72, 7Y73) (solo en la India) • SR250 V2 (7D7Q, 7D7R, 7D7S) • SR258 (7Y53) • SR530 (7X07, 7X08) • SR550 (7X03, 7X04) • SR570 (7Y02, 7X03) • SR590 (7X98, 7X99) • SR250 V3 (7DCM, 7DCL) • SR630 (7X01, 7X02) • SR630 V2 (7Z70, 7Z71) • SR630 V3 (7D72, 7D73, 7D74) • SR635 (7Y98, 7Y99) • SR635 V3 (7D9G, 7D9H) • SR645 (7D2X, 7D2Y) • SR645 V3 (7D9C, 7D9D) 	<ul style="list-style-type: none"> • SR650 (7X05, 7X06) • SR650 V2 (7Z72, 7Z73) • SR650 V3 (7D75, 7D76, 7D77) • SR655 (7Y00, 7Z01) • SR655 V3 (7D9E, 7D9F) • SR665 (7D2V, 7D2W) • SR665 V3 (7D9A, 7D9B) • SR670 (7Y36, 7Y37, 7Y38) • SR670 V2 (7Z22, 7Z23) • SR675 V3 (7D9Q, 7D9R) • SR850 (7X18, 7X19) • SR850 V2 (7D31, 7D32, 7D33) • SR850 V3 (7D96, 7D97, 7D98) • SR850P (7D2F, 7D2G, 7D2H) • SR860 (7X69, 7X70) • SR860 V2 (7Z59, 7Z60, 7D42) • SR860 V3 (7D93, 7D94, 7D95) • SR950 (7X11, 7X12, 7X13) • SR950 V3 (7DC4, 7DC5, 7DC6) • ST250 (7Y45, 7Y46) • ST250 V2 (7D8F, 7D8G) • ST250 V3 (7DCF, 7DCE) • ST258(7Y47) • ST258 V2 (7D8H) • ST550 (7X09, 7X10) • ST558 (7Y15, 7Y16) (Solo China) • ST650 V2 (7Z74, 7Z75) • ST650 V3 (7D7A, 7D7B) • ST658 V2 (7Z76)
ThinkServer	<ul style="list-style-type: none"> • SR588 V2 (7D53) • SR590 V2 (7D53) 	<ul style="list-style-type: none"> • SR660 V2 (7D6L) • SR668 V2 (7D6L)
ThinkEdge	<ul style="list-style-type: none"> • SE350 V2 (7DA9) • SE360 V2 (7DAM) 	<ul style="list-style-type: none"> • SE450 (7D8T) • SE455 V3 (7DBY)
Soluciones	<ul style="list-style-type: none"> • Servidor de dispositivo ThinkAgile Serie HX (7D20, 7D2T, 7D1Z, 7X82, 7X83, 7X84, 7Y95, 7Z08, 7Z29, 7Z44, 8689, 8693, 8695, 5462) • Nodo certificado de ThinkAgile Serie HX (7D20, 7D29, 7Y88, 7Y89, 7Y90, 7Y96, 7Z03, 7Z04, 7Z05, 7Z09, 7Z45) • Sistema integrado ThinkAgile VX (7D43, 7D6X, 7D6W, 7D82, 7D9K, 7D9L, 7D9V, 7D9W) 	<ul style="list-style-type: none"> • Dispositivo de ThinkAgile Serie VX (7Y11, 7Y12, 7Y13, 7Y14, 7Y91, 7Y92, 7Y93, 7Y94, 7Z13, 7Z58, 7Z62, 7Z63) • Nodo certificado de ThinkAgile VX Serie (7D6W, 7D6X, 7D9L, 7D9K, 7D9V, 7D9W, 7Y92, 7Y93, 7Y94, 7Z12, 7Z58, 7Z63, 7DDK)
System x	<ul style="list-style-type: none"> • nx360 M5 (5465) • nx360 M5 DWC (5467, 5468, 5469) • Nodo de cálculo x240 (7162, 2588) • Nodo de cálculo x240 M5 (2591, 9532) • Nodo de cálculo x280,x480,x880 X6 (7196, 4258) • Nodo de cálculo x440 (7167, 2590) • x3250 M6 (3633) 	<ul style="list-style-type: none"> • x3500 M5 (5464) • x3550 M4 (7914) • x3550 M5 (5463) • x3630 M4 (7158) • x3650 M4 (7915) • x3650 M5 (5462, 8871) • x3750 M4 (8753) • x3850 X6 / x3950 X6 (6241)

Tabla 4. Servidores Lenovo compatibles (continuación)

Serie	Modelos de servidor	
ThinkServer heredado	<ul style="list-style-type: none"> • RD350 • RD450 • RD550 • RD650 	<ul style="list-style-type: none"> • RS160 • SD350 (5493) • TD350 • TS460
<p>Notas:</p> <ul style="list-style-type: none"> • vSphere Lifecycle Manager solo admite los siguientes servidores: <ul style="list-style-type: none"> – Dispositivo Lenovo ThinkAgile Serie VX – Nodo certificado de Lenovo ThinkAgile Serie VX – Sistema integrado Lenovo ThinkAgile VX – Lenovo ThinkSystem SD630 V2, SE350, SE350 V2, SE450, SR630, SR630 V2, SR630 V3, SR645, SR645 V3, SR650, SR650 V2, SR650 V3, SR665, SR665 V3, SR850P, SR850 V2, SR850 V3 y SR950, SR950 V3. • La topología de hardware solo admite los siguientes servidores: <ul style="list-style-type: none"> – Dispositivo ThinkAgile VX: <ul style="list-style-type: none"> – 7Y93: Dispositivo ThinkAgile VX2320/VX3320/VX7320N – 7Y94: Dispositivo ThinkAgile VX5520/VX7520/VX3520G – 7Z62: dispositivo ThinkAgile VX2330/VX3330/VX7330-N – 7Z63: dispositivo ThinkAgile VX3530-G/VX5530/VX7530 – Nodo certificado ThinkAgile VX: <ul style="list-style-type: none"> – 7DDK: ThinkAgile VX850 V3/VX850 V3-DPU CN – 7D43: Nodo ThinkAgile VX7576 – 7D6X: ThinkAgile VX630 V3 CN – 7D6W: ThinkAgile VX650 V3/VX650 V3-DPU CN – 7D82: Nodo ThinkAgile VX3376 – 7D9L: ThinkAgile VX665 V3 CN – 7D9K: ThinkAgile VX645 V3 CN – 7D9V: ThinkAgile VX635 V3 CN – 7D9W: ThinkAgile VX655 V3 CN – 7Z62: Nodo ThinkAgile VX3331 – 7Z63: Nodo certificado ThinkAgile VX7531 – 7Y94: Nodo certificado ThinkAgile VX 2U/Nodo certificado VX 2U (para SAP HANA) – Sistema integrado ThinkAgile VX: <ul style="list-style-type: none"> – 7D43: ThinkAgile VX3575-G/VX5575/VX7575 IS – 7D6X: ThinkAgile VX630 V3 IS – 7D6W: ThinkAgile VX650 V3/VX650 V3-DPU IS – 7D82: ThinkAgile VX2375/VX3375/VX7375-N IS – 7D9K: ThinkAgile VX645 V3 IS – 7D9L: ThinkAgile VX665 V3 IS – 7D9V: ThinkAgile VX635 V3 IS – 7D9W: ThinkAgile VX655 V3 IS • Los servidores ThinkServer admiten solo inventario, supervisión y reinicio gradual, y parte de la información del inventario se mostrará como "NA". • Para ThinkServer SR588 V2/SR590 V2 (7D53), la versión de BMC debe ser la 5.30 o posterior. • Para ThinkServer SR660 V2/SR668 V2 (7D6L), la versión de BMC debe ser la 5.33 o posterior. 		

Tabla 5. Servidores IBM compatibles

Serie	Modelos de servidor	
System x	<ul style="list-style-type: none"> • dx360 M2 (7321, 7323) • dx360 M3 (6391) • dx360 M4 (7912, 7913, 7918, 7919) • HS22 (7870, 7809, 1911, 1936) • HS22V (7871, 1949) • HS23 (7875, 1882, 1929) • HS23E (8038, 8039) • HX5 (7872, 7873, 1909, 1910) • nx360 M4 (5455) • Smart Analytics System (7949) • Nodo de cálculo x220 (7906, 2585) • Nodo de cálculo x222 (7916) • Nodo de cálculo x240 (8956, 8737, 8738, 7863) • Nodo de cálculo x280 X6/Nodo de cálculo x480 X6/Nodo de cálculo x880 X6 (4259, 7903) • Nodo de cálculo x440 (7917) • x3100 M4 (2582, 2586) • x3100 M5 (5457) • x3200 M2 (4367, 4368) • x3200 M3 (7327, 7328) • x3250 M2 (7657, 4190, 4191, 4194) • x3250 M3 (4251, 4252, 4261) • x3250 M4 (2583) 	<ul style="list-style-type: none"> • x3250 M5 (5458) • x3300 M4 (7382) • x3400 M2 (7836, 7837) • x3400 M3 (7378, 7379) • x3500 M2 (7839) • x3500 M3 (7380) • x3500 M4 (7383) • x3530 M4 (7160) • x3550 M2 (7946, 4198) • x3550 M3 (7944, 4254) • x3550 M4 (7914) • x3620 M3 (7376) • x3630 M3 (7377) • x3630 M4 (7158, 7518, 7519) • x3650 M2 (7947, 4199) • x3650 M3 (7944, 7945, 4254, 4255, 5454) • x3650 M4 (7915) • x3650 M4 HD (5460) • x3650 M4 BD (5466) • x3750 M4 (8722, 8733) • x3755 M4 (7164) • x3690 X5 (7148, 7149, 7147, 7192) • x3850 X5/X3950 X5 (7145, 7146, 7143, 7191) • x3850 X6/x3950 X6 (3837, 3839)
<p>Notas:</p> <ul style="list-style-type: none"> • No se admiten actualizaciones de firmware en servidores IBM. • ESXi 6.5 o posterior personalizado por Lenovo no se admite en servidores IBM. • System x3250 M4 (2583) solo admite funciones parciales en el panel y Lenovo Dynamic System Analysis. Las funciones de actualización, alimentación y configuración del sistema no son compatibles. 		

Requisitos de hardware

Esta sección describe los requisitos de hardware para Lenovo XClarity Integrator para VMware vCenter. De forma predeterminada, el dispositivo virtual Lenovo XClarity Integrator para VMware vCenter está preconfigurado con la siguiente configuración de hardware.

- Memoria: 16 GB RAM
- Espacio de disco: 128 GB de espacio libre de disco
- Procesador: 4 procesadores

Requisitos de la red

En esta sección se proporcionan los requisitos de red, incluidos los requisitos de puerto, firewall y proxy.

Disponibilidad de puertos

Debe haber varios puertos disponibles, dependiendo de cómo estén implementados los firewalls en el entorno. Si puertos necesarios están bloqueados o se utilizan en otro proceso, es posible que algunas funciones de Lenovo XClarity Integrator no funcionen.

Consulte las secciones siguientes para determinar los puertos que deben estar abiertos en función del entorno. Las tablas de estas secciones incluyen información acerca de cómo se utiliza cada puerto en XClarity Integrator, vCenter, el dispositivo gestionado afectado, el protocolo (TCP o UDP) y la dirección del flujo de tráfico.

El tráfico *entrante* identifica los flujos desde el dispositivo gestionado o los sistemas externos a XClarity Integrator, por lo que los puertos deben estar abiertos en el dispositivo XClarity Integrator. El tráfico *saliente* identifica el flujo desde XClarity Integrator hasta el dispositivo gestionado o los sistemas externos.

- “Acceso a los servidores de XClarity Integrator” en la página 8
- “Acceso entre XClarity Integrator y dispositivos gestionados” en la página 8

Acceso a los servidores de XClarity Integrator

Si el servidor de XClarity Integrator y todos los dispositivos gestionados se rigen por un firewall y los usuarios tienen pensado acceder a estos dispositivos a través de un navegador que está fuera del firewall, deben asegurarse de que los puertos de XClarity Integrator estén abiertos.

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

Nota: XClarity Integrator es una aplicación RESTful que se comunica de forma segura a través de TCP en el puerto 443.

Tabla 6. Requisitos de conexión a Internet

Comunicación	Dispositivo XClarity Integrator	vCenter	XClarity Administrator ¹	Servicios de Lenovo ²
Salida (puertos abiertos en sistemas externos)	DNS – TCP/UDP en el puerto 53	HTTPS – TCP en el puerto 443	HTTPS – TCP en el puerto 443	HTTPS – TCP en el puerto 443
Entrada (puertos abiertos en el dispositivo XClarity Integrator)	HTTPS – TCP en el puerto 443	HTTPS – TCP en el puerto 443	N/A	N/A

1. Para registrar XClarity Administrator en XClarity Integrator, consulte https://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/plan_openports.html.
2. Para acceder a los sitios web de servicio específicos de Lenovo, consulte “Firewall” en la página 9.

Acceso entre XClarity Integrator y dispositivos gestionados

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

Nota: También se debe permitir el protocolo ICMP entre XClarity Integrator y el BMC del servidor. Lenovo XClarity Integrator utiliza ICMP (ping) para comprobar la conectividad del BMC durante las actualizaciones de firmware.

Tabla 7. Servidores y nodos de cálculo

Comunicación	ThinkSystem y ThinkAgile	System x
Salida (puertos abiertos en sistemas externos)	<ul style="list-style-type: none"> • SLP – UDP en el puerto 427 • HTTPS – TCP en el puerto 443 • CIM HTTPS – TCP en el puerto 5989² • Actualizaciones de firmware - TCP en el puerto 6990⁴ • SLP – UDP en el puerto 427 	<ul style="list-style-type: none"> • HTTPS – TCP en el puerto 443 • IPMI – TCP en el puerto 623¹ • CIM HTTP – TCP en el puerto 5988³ • CIM HTTPS – TCP en el puerto 5989³ • Actualizaciones de firmware - TCP en el puerto 6990⁴
Entrada (puertos abiertos en el dispositivo XClarity Integrator)	<ul style="list-style-type: none"> • HTTPS – TCP en el puerto 443 • Actualizaciones de firmware - TCP en el puerto 6990⁴ 	<ul style="list-style-type: none"> • HTTPS – TCP en el puerto 443 • Actualizaciones de firmware - TCP en el puerto 6990⁴

1. XClarity Integrator utiliza este puerto para la configuración del servidor y la actualización de firmware.
2. De forma predeterminada, este puerto está deshabilitado en algunos servidores nuevos. En este caso, no es necesario abrir este puerto y XClarity Integrator utiliza REST sobre HTTPS para la gestión. Solo es necesario abrir este puerto para los servidores gestionados por XClarity Integrator mediante CIM.
3. De forma predeterminada, la gestión se realiza a través de puertos seguros. Los puertos no seguros son opcionales.
4. Este puerto se usa para conectarse al SO BMU para transferir archivos y ejecutar los comandos de actualización.

Firewall

La descarga de las actualizaciones del servidor de gestión y las actualizaciones de firmware requieren acceso a Internet. Configure el firewall (si lo hubiera) en la red para habilitar el servidor de gestión de LXCI a fin de que ejecute estas operaciones. Si el servidor de gestión no puede acceder a Internet, configure LXCI para utilizar un servidor proxy.

Asegúrese de que los siguientes FQDN y puertos estén disponibles en el firewall y permitidos en el proxy.

Tabla 8. Requisitos de conexión a Internet

Nombre DNS	Puertos	Protocolos
datacentersupport.lenovo.com	443	https
download.lenovo.com	443	https
filedownload.lenovo.com	443	https
support.lenovo.com	443	https
supportapi.lenovo.com	443	https

Proxy

Para configurar el proxy en vCenter y utilizar la función vLCM para actualizar el firmware, los usuarios deben permitir la conexión desde vCenter a Lenovo XClarity Integrator (protocolo HTTPS, puerto 443) en la configuración de proxy de la empresa de los usuarios.

El servidor proxy debe cumplir los siguientes requisitos:

- El servidor proxy debe estar configurado para utilizar autenticación básica.
- El servidor proxy debe estar configurado como un proxy no de terminación.
- El servidor proxy debe estar configurado como un proxy de reenvío.
- Los equilibradores de carga deben estar configurados para mantener sesiones con un solo servidor proxy.

Instalación de Lenovo XClarity Integrator para VMware vCenter

En esta sección se describe cómo instalar el dispositivo virtual Lenovo XClarity Integrator para VMware vCenter.

Nota: El dispositivo virtual Lenovo XClarity Integrator para VMware vCenter solo se puede instalar en un entorno basado en VMware ESXi.

Antes de empezar

Antes de realizar la instalación, asegúrese de que:

- El host de ESXi cuente con espacio de disco y memoria libres suficientes como para admitir el dispositivo virtual Lenovo XClarity Integrator para VMware vCenter.
- La red esté configurada para utilizar DHCP o una dirección IP estática.

Procedimiento

Siga los pasos siguientes para instalar el dispositivo virtual Lenovo XClarity Integrator para VMware vCenter en un host ESXi desde el cliente de vSphere.

Paso 1. Inicie sesión en el cliente de vSphere.

Paso 2. Haga clic con el botón derecho en el host ESXi destino y seleccione **Deploy OVF Template** (Desplegar plantilla OVF) Aparece la ventana Deploy OVF Template (Desplegar plantilla OVF).

Paso 3. En la página **Select an OVF template** (Seleccionar una plantilla OVF), seleccione **URL** o **Local file** (Archivo local) como ubicación de origen. Para el archivo local, haga clic en **Choose Files** (Elegir archivos), especifique la ubicación del archivo OVF y haga clic en **NEXT** (Siguiente).

Paso 4. En la página **Select a name and folder** (Seleccionar un nombre y carpeta), introduzca un nombre único y una ubicación de destino para la máquina virtual y, a continuación, haga clic en **NEXT** (Siguiente).

Paso 5. En la página **Select a computer resource** (Seleccionar un recurso informático), seleccione el recurso del equipo de destino y haga clic en **NEXT** (Siguiente).

Paso 6. En la página **Review details** (Revisar detalles), confirme los detalles y haga clic en **NEXT** (Siguiente).

Paso 7. En la página **License agreements** (Contratos de licencia), lea el contrato de licencia, seleccione **I accept all license agreements** (Acepto todos estos contratos de licencia) y haga clic en **NEXT** (Siguiente).

Paso 8. En la página **Select storage** (Seleccionar almacenamiento), seleccione almacenamiento para los archivos de configuración y de disco y luego haga clic en **NEXT** (Siguiente).

Paso 9. En la página **Select networks** (Seleccionar redes), seleccione la red para el servidor virtual de destino y haga clic en **NEXT** (Siguiente).

Nota: Omita los valores que se muestran en la sección **IP Allocation Settings** (Valores de asignación de IP). Los valores de asignación de IP se configurarán en el paso siguiente.

Paso 10. En la página **Customize template** (Personalizar la plantilla), configure las configuraciones de red y luego haga clic en **NEXT** (Siguiente).

Nota: Los usuarios pueden introducir la dirección de vCenter, el nombre de usuario y la contraseña en el área de **vCenter Registration** (Registro de vCenter).

Paso 11. En la página **Ready to complete** (Preparar finalización), revise los detalles y haga clic en **Finish** (Finalizar).

Paso 12. Encienda la máquina virtual. Al encender la máquina virtual, aparece la URL de acceso a la página de administración del dispositivo “Lenovo XClarity Integrator” en la consola de VM.

Por ejemplo, el siguiente diagrama solicita la URL para gestionar el dispositivo:

```
-----  
Lenovo XClarity Integrator - Version x.x.x build xxx  
-----
```

Manage the appliance from: <https://192.0.2.10/admin>

```
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:ffff:ffff:ffff:ffff:ffff:ffff/64  Scope:Global  
        inet6 addr: 2001:db8:56ff:fe80:bea3/64  Scope:Link
```

- Paso 13. Vaya a la página de administración del dispositivo “Lenovo XClarity Integrator”. Por ejemplo:<https://192.0.2.10/admin>
- Paso 14. En la página **Account Configuration** (Configuración de la cuenta), establezca una cuenta de administrador para iniciar sesión en la página de administración del dispositivo “Lenovo XClarity Integrator” y haga clic en **Submit** (Enviar).
- Paso 15. En la página de inicio de sesión de **Lenovo XClarity Integrator Appliance Administration** (Administración de dispositivo Lenovo XClarity Integrator), especifique la cuenta creada en el asistente y haga clic en **Login** (Iniciar sesión). Aparece la página **vCenter Connection** (Conexión a vCenter).
- Paso 16. En la página **vCenter Connection** (Conexión a vCenter), haga clic en **Register** (Registrar) para registrar Lenovo XClarity Integrator en los servidores vCenter. Para obtener más información, consulte [“Configuración de conexiones de vCenter” en la página 53](#).

Habilitar/deshabilitar vSphere Lifecycle Manager

LXCI actúa como gestor de soporte de hardware para vSphere Lifecycle Manager (vLCM) y permite a vLCM gestionar servidores de Lenovo ESXi con una imagen de ancho de clúster que se compone de ESXi, un complemento de controlador de Lenovo y un complemento de firmware.

Antes de empezar

Asegúrese de que el servidor de destino sea compatible. Para obtener más información acerca de los tipos de equipos compatibles, consulte [Tabla 4 “Servidores Lenovo compatibles” en la página 5](#).

Procedimiento

Los usuarios pueden habilitar o deshabilitar LXCI como gestor de soporte de hardware para vLCM.

En la página **vCenter Connection** (Conexión de vCenter), haga clic en **Disable** (Deshabilitar) o **Enable** (Habilitar) en la columna **vSphere Lifecycle Manager** para cambiar el estado de vLCM del servidor requerido.

Para obtener más información sobre la gestión de actualizaciones de firmware a través de vLCM, consulte [“Uso de la función vSphere Lifecycle Manager” en la página 37](#).

Qué debe hacer a continuación

Inicie sesión y configure Lenovo XClarity Integrator para VMware vCenter (consulte [Capítulo 3 “Configuración de Lenovo XClarity Integrator” en la página 15](#)).

Habilitación/deshabilitación de la gestión proactiva del hardware

LXCI actúa como gestor de soporte del hardware para la gestión proactiva del hardware (PHM).

Antes de empezar

Asegúrese de que el servidor de destino sea compatible. Para obtener más información acerca de los tipos de equipos compatibles, consulte [Tabla 4 “Servidores Lenovo compatibles” en la página 5](#).

Procedimiento

Los usuarios pueden habilitar o deshabilitar LXCI como gestor de soporte de hardware para PHM.

En la página **vCenter Connection (Conexión de vCenter)**, haga clic en **Disable (Deshabilitar)** o **Enable (Habilitar)** en la columna **Proactive Hardware Management (Gestión proactiva del hardware)** para cambiar el estado de PHM del servidor requerido.

Para obtener más información sobre la gestión de actualizaciones de firmware a través de PHM, consulte [“Trabajar con la función Gestión proactiva del hardware” en la página 41](#).

Qué debe hacer a continuación

Inicie sesión y configure Lenovo XClarity Integrator para VMware vCenter (consulte [Capítulo 3 “Configuración de Lenovo XClarity Integrator” en la página 15](#)).

Implementación de alta disponibilidad para Lenovo XClarity Integrator

Para implementar la alta disponibilidad de Lenovo XClarity Integrator, utilice la función de alta disponibilidad (HA) de vSphere en el entorno de ESXi. Lenovo XClarity Integrator se reiniciará en el host alternativo cuando se produzca un error de ejecución en el host de ESXi.

Antes de empezar

Asegúrese de que el clúster de HA de vSphere esté disponible. Para obtener más información acerca de la creación del clúster de HA de vSphere, consulte [Creación de un clúster de HA de vSphere](#).

Procedimiento

Lleve a cabo los pasos siguientes para implementar la alta disponibilidad para Lenovo XClarity Integrator:

- Paso 1. Despliegue Lenovo XClarity Integrator en un clúster de Ha de vSphere.
- Paso 2. Seleccione **Restart VMs** (Reiniciar VM) y configure las respuestas ante errores del host basándose en los pasos que se encuentran en [Responder a errores del host](#).
- Paso 3. Active la supervisión de VM de acuerdo con los pasos que se indican en [Activar supervisión de VM](#).

Actualización de Lenovo XClarity Integrator para VMware vCenter

Los usuarios pueden actualizar Lenovo XClarity Integrator para VMware vCenter cuando ya está instalado en entornos basados en VMware ESXi.

Actualización de LXCI para VMware vCenter en entornos con base VMware ESXi

Esta sección describe cómo actualizar el dispositivo virtual Lenovo XClarity Integrator cuando ya está instalada en un entorno con base ESXi.

Antes de empezar

Para realizar la actualización, primero debe obtener el paquete de actualización. Normalmente, el paquete de actualización contiene cuatro archivos:

- **Archivo .chg.** Archivo de historial de cambios
- **Archivo .tgz.** Actualización de carga útil
- **Archivo .txt.** Archivo léame del paquete de actualización específico
- **Archivo .xml.** Metadatos acerca de la actualización

Nota: Para utilizar Lenovo XClarity Integrator v5.0.2 o v5.1.0, aplique el parche de corrección lnvggy_sw_lxci_upload_fixpatch_1.0.0_anyos_noarch antes de aplicar el paquete de actualización. Realice los pasos 2 al 7 en el siguiente procedimiento para aplicar el parche de revisión. Dos de los mensajes se muestran con información sobre el registro de complementos; ignore este mensaje. Los usuarios pueden descargar el parche desde el [Sitio web de Lenovo XClarity Integrator para VMware](#).

Procedimiento

- Paso 1. (Opcional) Cancele el registro de Lenovo XClarity Integrator desde VMware vCenter.
- Paso 2. Desde la interfaz web de Lenovo XClarity Integrator, haga clic en **Version and upgrade** (Versión y actualización) en el panel izquierdo de la página.
- Paso 3. Haga clic en **Import** (Importar). Se muestra el cuadro de diálogo Import (importar).
- Paso 4. Haga clic en **Browse (Examinar)**, seleccione los archivos de destino y haga clic en **Open (Abrir)**. Los archivos seleccionados se enumeran en el diálogo Import (importar).

Nota: Asegúrese de seleccionar los archivos TXT, CHG, XML y TGZ.

- Paso 5. Haga clic en **Import** (Importar) para importar los archivos seleccionados.

Notas:

- El proceso de importación puede tardar varios minutos u horas, en función del tamaño del paquete de actualización y de la red existente. Asegúrese de que la red está conectada y espere hasta que la barra de progreso termine y se cierre el diálogo.
- Si aparece el mensaje de error Invalid session (Sesión no válida), la sesión caducó. Cierre la sesión de la interfaz web de Lenovo XClarity Integrator, vuelva a iniciar sesión y repita la operación de importación. Considere emplazar el paquete de actualización en una red más rápida.

- Paso 6. Después de importar el paquete de actualización, elija el paquete de actualización de la tabla y haga clic en **Perform Update** (Realizar actualización). Se muestra un cuadro de diálogo de solicitud. Lea la información cuidadosamente

Notas:

- Puede que Lenovo XClarity Integrator se reinicie para completar el proceso de actualización. Si se reinicia, se interrumpirán esta conexión de configuración y el resto de los trabajos activos.
- Los usuarios pueden supervisar el progreso de la actualización desde la consola del dispositivo virtual en el cliente de vSphere o el cliente web de vCenter.

- Paso 7. Al abrir la consola del dispositivo, haga clic en **OK (Aceptar)** y la solicitud de actualización se enviará al servidor. El mensaje de progreso de actualización se muestra en la consola. Si se muestra update finished (actualización finalizada) y no se muestran errores en la consola, la actualización se completó correctamente.

```
-----  
Manage the appliance from: https://10.240.197.36/admin
```

```
eth0    Link encap:Ethernet  HWaddr 00:0c:29:4a:d4:5e  
        inet addr:10.240.197.36  Bcast:10.240.199.25  Mask:255.255.255.0  
        inet6 addr: 2002:96b:c2bb:830:20c:29ff:fe34:d34e/64  Scope:Global  
        inet6 addr: fe80:20c:39ff:fe3a:d9/64  Scope:Link
```

```
lxci login: starting to extract update package
```

```
extract update package finished
=====Fri Feb 10 17:32:33 CST 2017=====
start to update...
Preparing... #####
uus          warning: /etc/lighttpd.conf saved as /etc/lighttpd.conf.rpmsave
#####
Stopping uusservd
Starting uusservd
Database record of identificationCode:lnvgy_sw_lxci_upatch1.0.0_anyos_noarch
changed to applied successfully
update finished...
```

Paso 8. (Opcional) Registre Lenovo XClarity Integrator en VMware vCenter.

Desinstalación de Lenovo XClarity Integrator para VMware vCenter

En esta sección se describe cómo desinstalar Lenovo XClarity Integrator para VMware vCenter.

Procedimiento

Siga estos pasos para desinstalar Lenovo XClarity Integrator para VMware vCenter.

1. Inicie sesión en la página **Lenovo XClarity Appliance Administration** (Administración de dispositivo Lenovo XClarity Integrator).
 2. Cree una copia de seguridad del dispositivo.
 3. Cancele el registro del complemento de vCenter. Para obtener más información, consulte [“Configuración de conexiones de vCenter” en la página 53](#).
 4. Apague el dispositivo desde el cliente de vSphere y elimínelo del inventario.
 5. Detenga el servicio del cliente de vSphere.
 6. En el servidor vCenter, quite el directorio `com.lenovo.lxci-*.*` que se encuentra en `/etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity/`.
- Nota:** Según la versión de servidor de vCenter, la ruta `/etc/vmware` puede variar.
7. Inicie el servicio del cliente de vSphere.

Capítulo 3. Configuración de Lenovo XClarity Integrator

Los temas de esta sección proporcionan información acerca de cómo configurar Lenovo XClarity Integrator en el servidor de destino.

Detección y gestión de BMC

Los usuarios pueden utilizar Lenovo XClarity Integrator para detectar el BMC y asociar el BMC al host ESXi, con el fin de habilitar la gestión fuera de banda (OOB) de los servidores de destino en el entorno de vSphere.

Lenovo XClarity Integrator admite dos formas de detectar y gestionar el BMC:

- Detecte y gestione el BMC directamente

Notas: Esto no se puede aplicar a los siguientes servidores:

- Servidores ThinkServer
 - ThinkSystem SR635
 - ThinkSystem SR655
- Detecte y gestione el BMC a través de Lenovo XClarity Administrator

Nota: Para los servidores ThinkSystem, el servicio CIM está deshabilitado de forma predeterminada. En función del nivel de firmware, LXCI podría permitir que el servicio CIM gestione el servidor.

Detección y gestión directa del BMC

Los usuarios pueden detectar y gestionar el BMC directamente proporcionando la credencial y la dirección BMC.

Procedimiento

- Paso 1. En la página web de “vSphere Client”, haga clic en la lista desplegable **Menu (Menú)** y seleccione **Lenovo XClarity Integrator**. Se abre la página de gestión de “Lenovo XClarity Integrator”.
- Paso 2. Haga clic en la sección **Discover servers (Detectar servidores)**. Se muestra la página de detección de servidor.

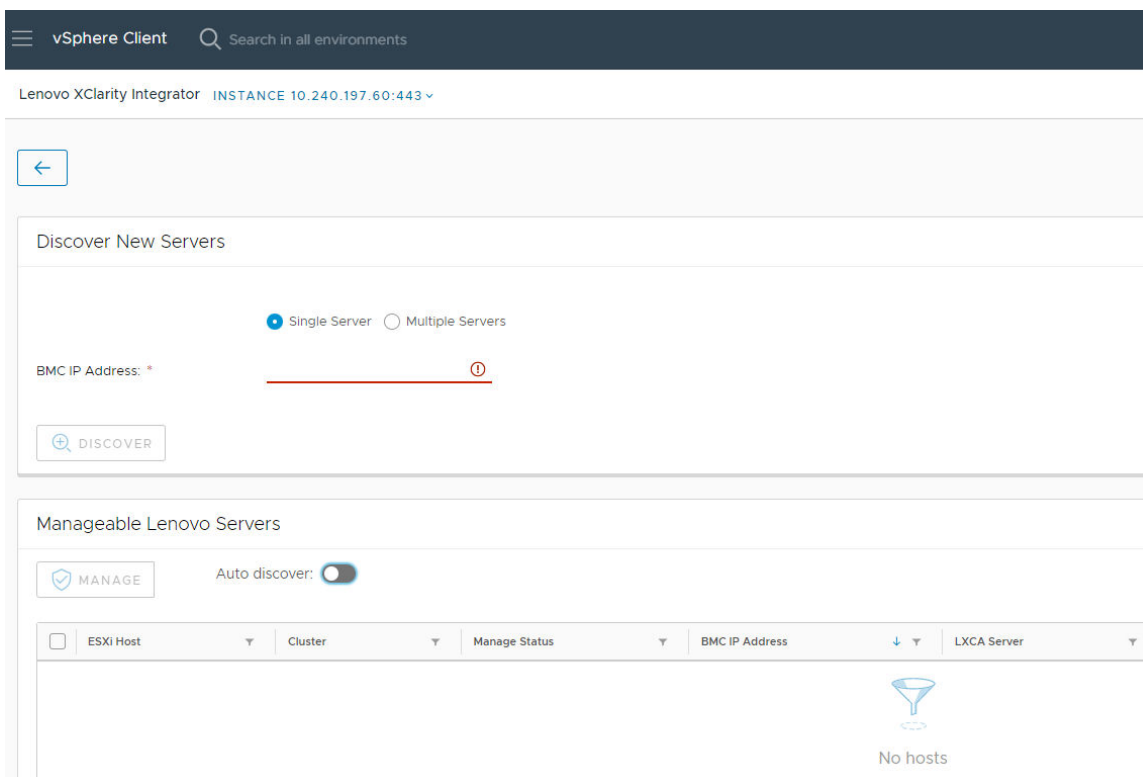


Figura 1. Detección y gestión de BMC

Nota: Todos los hosts ESXi gestionados por vCenter que se pueden gestionar, pero no se han gestionado mediante Lenovo XClarity Integrator se enumeran en la sección **Manageable Lenovo Servers** (Servidores gestionables de Lenovo). Para el host cuyo BMC no se detectó mediante Lenovo XClarity Integrator, el estado de la gestión del host se muestra como "No preparado" en la columna **Manage Status** (Gestionar estado).

- Paso 3. En la sección **Discover New Servers (Detectar nuevos servidores)**, introduzca una sola dirección IP del BMC o un rango de direcciones IP para varios servidores y haga clic en **Discover (Detectar)**.

Notas:

- Se recomienda que un rango de direcciones IP contenga menos de 60 direcciones de IP.
- Si se detecta un BMC y se puede asociar a un host ESXi, se mostrará la dirección IP del BMC en la columna **BMC IP Address (Dirección IP de BMC)** de la tabla **Manageable Lenovo Servers (Servidores Lenovo gestionables)** y el estado de gestión del host de ESXi cambiará a **Ready (Preparado)** en la columna **Manage Status (Estado de gestión)**.

- Paso 4. En el área "Manageable Lenovo Servers (Servidores Lenovo gestionables)", realice uno o más de los siguientes procedimientos:
- Para gestionar los servidores, seleccione uno o varios servidores de destino con estado **Ready (Preparado)** y, a continuación, haga clic en **MANAGE (GESTIONAR)**, introduzca el nombre de usuario y la contraseña del BMC en la ventana emergente y haga clic en **OK (Aceptar)**.

Si el servidor está gestionado correctamente, aparecerá un mensaje de confirmación. El estado de gestión del servidor cambia a **Managing (En gestión)** en la columna **Manage Status (Estado de gestión)** y el servidor se muestra en la sección **Managed Servers (Servidores gestionados)**.

- Para habilitar o deshabilitar la función de detección automática, haga clic en el icono de alternar y haga clic en **YES (Sí)** para iniciar el proceso de inmediato, o bien haga clic en **NO** para iniciar el proceso dentro de las 24 horas siguientes a la habilitación de LXCI.

Nota: El protocolo SSDP debe habilitarse antes de ejecutar el servicio de detección automática. La función de detección automática, si está habilitada, se ejecutará una vez al día.

Detección y gestión de BMC mediante LXCA

Si Lenovo XClarity Administrator está disponible y los servidores ESXi ya se han gestionado mediante Lenovo XClarity Administrator, no es necesario detectar ni gestionar los servidores de Lenovo XClarity Integrator. Basta con registrar el Lenovo XClarity Administrator en Lenovo XClarity Integrator y Lenovo XClarity Integrator detectará y gestionará el BMC automáticamente mediante Lenovo XClarity Administrator. Consulte “[Configuración de Lenovo XClarity Administrator](#)” en la [página 17](#) acerca de cómo registrar Lenovo XClarity Administrator.

Nota: Al registrar LXCA en LXCI, asegúrese de que la cuenta de LXCA tenga permiso para gestionar todos los servidores de destinos gestionados con LXCI. Estos servidores se deben gestionar mediante la **Managed Authentication (Autenticación gestionada)** en lugar de la **Local Authentication (Autenticación local)** en LXCA. Para obtener más información, consulte https://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/aug_product_page.html.

Configuración de Lenovo XClarity Administrator

Lenovo XClarity Integrator proporciona un método integrado para gestionar los servidores de destino junto con Lenovo XClarity Administrator. Después de que Lenovo XClarity Administrator se registre en Lenovo XClarity Integrator, Lenovo XClarity Integrator puede detectar y gestionar servidores automáticamente y los usuarios pueden gestionar servidores de Cliente vSphere utilizando funciones de Lenovo XClarity Administrator, como el mapa de chasis, el patrón de configuración y el despliegue de política de firmware.

Antes de empezar

Antes de registrar Lenovo XClarity Administrator en Lenovo XClarity Integrator, asegúrese de lo siguiente:

- Lenovo XClarity Administrator está funcionando en el entorno actual.
- Los privilegios de *administración de Lenovo XClarity Integrator* están preparados.

Procedimiento

- Paso 1. En la página web de “vSphere Client”, haga clic en el cuadro de la lista desplegable **Menu** (Menú) en la parte superior y seleccione **Lenovo XClarity Integrator**. Se abre la página de gestión de “Lenovo XClarity Integrator”.
- Paso 2. En la sección **Service Status (Estado de servicio)**, haga clic en **ADD LENOVO XCLARITY ADMINISTRATOR (AÑADIR LENOVO XCLARITY ADMINISTRATOR)**. Se muestra la página “Registration Wizard (Asistente de registro)”.

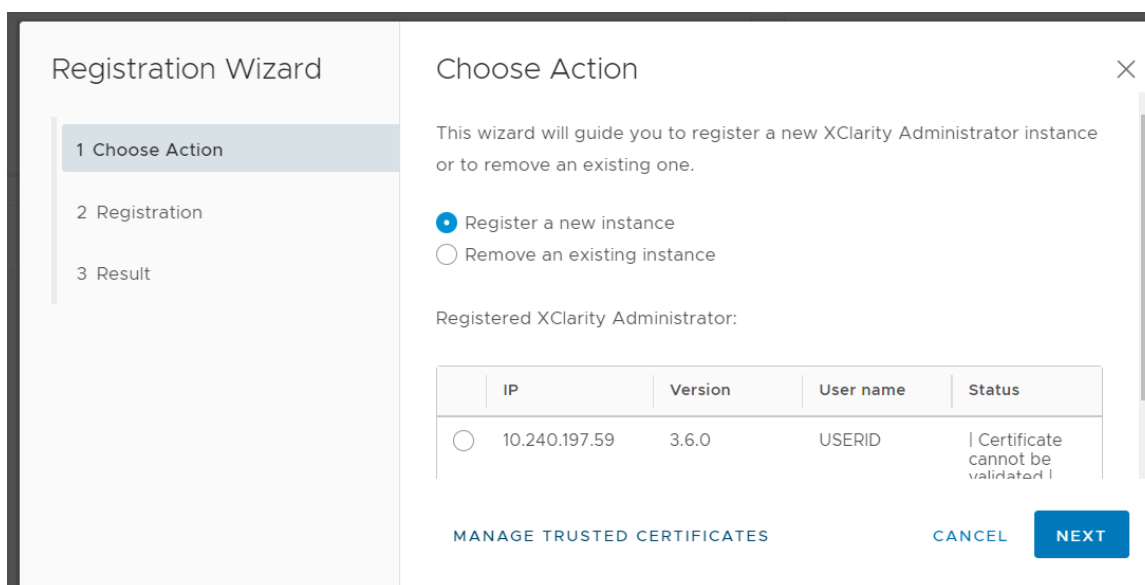


Figura 2. Página Asistente de registro

Paso 3. Realice una de las acciones siguientes:

- Para registrar una nueva instancia:
 1. En la página “Choose Action (Elegir acción)”, seleccione **Register a new instance (Registrar una nueva instancia)** y, a continuación, haga clic en **NEXT (SIGUIENTE)**.
 2. En la página “Registration (Registro)”, lleve a cabo una de las siguientes acciones:
 - Seleccione **Use an existing account (Usar una cuenta existente)**, introduzca el nombre de host o la dirección IP, el nombre de usuario y la contraseña y haga clic en **NEXT (SIGUIENTE)**.

Notas: Asegúrese de que:

- Esta cuenta tiene el grupo de rol “lxc-supervisor” o los grupos de roles “lxc-operator, lxc-fw-admin, lxc-hw-admin y lxc-os-admin” combinados.
 - Si está activado el Control de acceso a recursos en XClarity Administrator, esta cuenta puede tener acceso a los servidores.
 - Seleccione **Create a new account by connecting with this administrative account (Cree una nueva cuenta conectándose con esta cuenta de administrador)**, introduzca el nombre de host o la dirección IP, el nombre de usuario y la contraseña y haga clic en **NEXT (SIGUIENTE)**.
- Notas:**
- Asegúrese de que la cuenta nueva tenga los grupos de roles “lxc-operator, lxc-fw-admin, lxc-hw-admin y lxc-os-admin”.
 - Si está activado el Control de acceso a recursos en XClarity Administrator, asegúrese de que esta cuenta pueda tener acceso a los servidores.
 - Si se utiliza LDAP en XClarity Administrator o se desactiva la cuenta local, no elija esta opción.
3. (Opcional) En la página “View Certificate (Ver certificado)”, haga clic en **NEXT (SIGUIENTE)** para aceptar el certificado.
 4. En la página “Result (Resultado)”, haga clic en **FINISH (FINALIZAR)**.
- Para quitar una instancia existente:
 1. En la página “Choose Action (Elegir acción)”, seleccione **Remove an existing instance (Quitar una instancia existente)**, seleccione la instancia de destino de la tabla y, a continuación, haga clic en **NEXT (SIGUIENTE)**.
 2. En la página “Unregister (Cancelar registro)”, haga clic en **NEXT (SIGUIENTE)**.

3. En la página “Result (Resultado)”, haga clic en **FINISH (FINALIZAR)**.
- Para gestionar certificados de confianza:
 1. En la página “Choose Action (Elegir acción)”, seleccione **MANAGE TRUSTED CERTIFICATES (GESTIONAR CERTIFICADOS DE CONFIANZA)** para ir a la página de VMware vCenter.
 2. Siga los pasos que se indican en [“Gestión de certificados de confianza” en la página 67](#).

Configuración del control de acceso

Lenovo XClarity Integrator es compatible con acceso basado en roles.

Los siguientes cuatro privilegios se definen para controlar el acceso a diversas funciones:

Privilegio	Funciones autorizadas
Lista de sistemas	<ul style="list-style-type: none"> • Vea la información de inventario, los sucesos y la utilización de host • Iniciar la interfaz BMC
Actualización de firmware	Actualización del firmware
Configuración del	Configure los valores del sistema e inicie la KVM
Administración	Acceder a la página de administración de LXCI: <ul style="list-style-type: none"> • Editar la conexión de LXCI/vCenter • Agregar la conexión de LXCA • Detectar y gestionar un servidor • Deshabilitar la gestión de un servidor

De forma predeterminada, el rol de administrador de vCenter tiene todos los privilegios definidos por Lenovo XClarity Integrator. El administrador de vCenter puede otorgar estos privilegios a otros usuarios vCenter si es necesario.

Importación del certificado de Lenovo XClarity Integrator al navegador web

Si el certificado que utiliza Lenovo XClarity Integrator no está firmado por un tercero de confianza, la página de presentación se bloquea cuando se utilizan algunas funciones, como la actualización de firmware, mapa del chasis y valores del sistema. En este caso, los usuarios deben descargar el certificado raíz de Lenovo XClarity Integrator e importarlo a la lista de certificados de confianza de los navegadores web o agregarlo a las excepciones de seguridad, según el navegador que se esté utilizando.

Procedimiento

- Para Internet Explorer y Chrome:
 1. Inicie sesión en la página de Administración de dispositivo Lenovo XClarity Integrator.
 2. Haga clic en **Security Settings** (Valores de seguridad) y luego haga clic en **Certificate Authority** (Autoridad de certificación).
 3. Haga clic en **Download Certification Authority Root Certificate** (Descargar certificado raíz de entidad de certificación) para descargar el certificado.
 4. Haga doble clic en el archivo `downloaded.ca.cer`.
 5. En la pestaña **General**, haga clic en **Install Certificate** (Instalar certificado).
 6. Elija **Local Machine** (Equipo local) y haga clic en **Next** (Siguiendo).
 7. En la página **Certificate Store** (Almacén de certificados), seleccione **Place all certificates in the following store** (Colocar todos los certificados en el siguiente almacén) y, a continuación, haga clic en **Browse...** (Examinar...).
 8. Seleccione **Trusted Root Certificate Authorities** (Entidades de certificación raíz de confianza) y, a continuación, haga clic en **OK** (Aceptar).

9. Haga clic en **Finish** (Finalizar).
 10. Para Internet Explorer, cierre el navegador y vuelva a abrirlo para que los cambios surtan efecto.
- Para Firefox:
 1. Desde un navegador abierto, haga clic en **Firefox → Options (Opciones) → Privacy&Security (Privacidad y seguridad) → Certificates (Certificados) → View Certificates (Ver certificados) → Servers (Servidores) → Add Exception (Añadir excepción)**.
 2. En el campo **Location (Ubicación)**, especifique el nombre de dominio completamente calificado o la dirección IP del host instalado con Lenovo XClarity Integrator.
 3. Haga clic en **Get Certificate** (Obtener certificado).
 4. Haga clic en **Confirm Security Exception (Confirmar excepción de seguridad)** y, a continuación, actualice el navegador.

Capítulo 4. Visualización de un resumen del entorno

Esta sección es una introducción del panel Lenovo XClarity Integrator. El panel Lenovo XClarity Integrator ofrece una visión general de los servidores gestionados, servidores gestionables, el estado de servicio y la información de producto

Procedimiento

Para entrar al panel Lenovo XClarity Integrator, realice los pasos siguientes:

1. Desde la página web de “vSphere Client”, haga clic en el cuadro de la lista desplegable **Menu** (Menú) en la parte superior.
2. Seleccione **Lenovo XClarity Integrator**. Se muestra la página Lenovo XClarity Integrator.

Seleccione una de las secciones siguientes en el panel:

- **Discover Servers** (Detectar servidores). Consulte [“Sección Detectar servidores” en la página 21](#).
- **Managed Servers** (Servidores gestionados). Consulte [“Sección Servidores gestionados” en la página 21](#).
- **Service Status** (Estado de servicio). Consulte [“Sección Estado del servicio” en la página 22](#).
- **Product Information** (Información del producto). Consulte [“Sección Información del producto” en la página 22](#).

Sección Detectar servidores

Esta sección permite a los usuarios ver la cantidad de servidores de Lenovo que pueden gestionarse. Los usuarios pueden hacer clic en **Manageable Lenovo Servers (Servidores Lenovo gestionables)** o en **Discover New Servers (Detectar nuevos servidores)** para acceder al panel de operación detallado para realizar las operaciones, como detectar y gestionar los servidores.

La sección **Manageable Lenovo Servers** (Servidores Lenovo gestionables) proporciona una tabla que enumera los siguientes detalles de los servidores gestionables.

- Host de ESXi
- Clúster
- Estado de gestión
- Dirección IP de BMC
- Servidor LXCA
- Modelo
- Número de serie
- Nombre del producto
- vCenter

Sección Servidores gestionados

Esta sección permite a los usuarios ver la cantidad de servidores gestionados de Lenovo y la cantidad de máquinas virtuales en estos servidores agrupados por estado del servidor. Los usuarios pueden hacer clic en la información de cantidad para acceder al panel de operaciones **Managed Servers (Servidores gestionados)**.

El panel de operaciones **Managed Servers** (Servidores gestionados) proporciona una tabla que enumera los siguientes detalles de los servidores gestionables.

- Host de ESXi
- Clúster
- Estado
- Alimentación
- Dirección IP de BMC
- Servidor LXCA

- Modelo
- Número de serie
- vCenter

Realice una de las acciones siguientes:

- Para actualizar la información de inventario de un servidor gestionado, haga clic en el botón **REFRESH INVENTORY** (Actualizar inventario).
- Para actualizar el nombre de usuario y contraseña de BMC de un servidor gestionado, según sea necesario, haga clic en el botón **EDIT CREDENTIALS (Editar credenciales)**.
- Para deshabilitar la gestión de un servidor gestionado, haga clic en el botón **UNMANAGE** (Cancelar gestión).

Nota: Todas las funciones de Lenovo XClarity Integrator para este servidor se deshabilitarán y este servidor se mostrará en la sección **Manageable Lenovo Servers** (Servidores Lenovo gestionables).

Sección Estado del servicio

Esta sección muestra el estado de servicios que Lenovo XClarity Integrator proporciona.

Existen tres tipos de servicios en esta sección:

- Servicio XClarity Integrator

Muestra la dirección IP y el estado de los servicios de backend de Lenovo XClarity Integrator. Los usuarios pueden hacer clic en **EDIT (EDITAR)** para editar la dirección IP, el nombre de usuario y la contraseña para la conexión a los servicios de Lenovo XClarity Integrator.

- vCenter Server

Muestra los servidores vCenter en los que se registró XClarity Integrator. Los usuarios pueden hacer clic en **EDIT (EDITAR)** para especificar la página web de administrador de Lenovo XClarity Integrator para VMware vCenter. Para obtener más información, consulte [“Configuración de conexiones de vCenter” en la página 53](#).

- XClarity Administrator

Muestra los administradores de XClarity que se han registrado en XClarity Integrator. Los usuarios pueden hacer clic en **EDIT (EDITAR)** o **LAUNCH (INICIAR)** para editar o iniciar los administradores de XClarity.

Sección Información del producto

Esta sección permite a los usuarios ver la información de producto de Lenovo XClarity Integrator.

Los usuarios pueden hacer clic en los siguientes vínculos para obtener información acerca de los productos o enviar comentarios para ayudarnos a mejorar.

- [Ver Acuerdo de licencia de Lenovo](#)
- [Ver licencia de terceros](#)
- [Ver licencia de terceros](#)
- [Documentación en línea](#)
- [Sitio web de producto](#)
- [Visitar foro](#)
- [Enviar idea](#)

Capítulo 5. Gestión de servidores

Lenovo XClarity Integrator proporciona gestión de plataformas para System x, BladeCenter y los servidores Flex. Los temas de esta sección describen cómo utilizar Lenovo XClarity Integrator para gestionar servidores.

Verifique que se hayan completado estos requisitos previos:

- El número de servidores de Lenovo gestionados por vCenters registrados en la misma instancia de LXCI no debe superar los 1.000. De lo contrario, los usuarios deben desplegar varias instancias de LXCI para estos servidores de Lenovo.
- VMware vCenter Server dispone de una conexión de red fuera de banda con el BMC de los servidores ESXi gestionados.
- Los usuarios pueden localizar el BMC y solicitar acceso para el BMC en la página **Cluster Overview (Información general del clúster)**.
- Lenovo XClarity Administrator debe gestionar los siguientes servidores y Lenovo XClarity Administrator debe registrarse en Lenovo XClarity Integrator (consulte [“Configuración de Lenovo XClarity Administrator” en la página 17](#)).
 - Servidores ThinkServer
 - ThinkSystem SR635
 - ThinkSystem SR655

Procedimiento

Paso 1. Seleccione un host del árbol de inventarios de host de vCenter.

Paso 2. Haga clic en la pestaña **Monitor** (Supervisar).

En el panel de navegación izquierdo, seleccione una de las siguientes funciones en **Lenovo XClarity**:

- Información general del sistema
- Sucesos
- Lista de sistemas
- Utilización
- Mapa del chasis
- Topología de hardware

Paso 3. Haga clic en la pestaña **Configure** (Configurar).

En el panel de navegación izquierdo, seleccione una de las siguientes funciones en **Lenovo XClarity**:

- Actualizaciones de firmware
- Política de alimentación
- Configuración del

Paso 4. Haga clic con el botón derecho del mouse en el host del árbol de inventarios de host de vCenter.

En el cuadro de lista desplegable **Actions (Acciones)** que se muestra, mueva el cursor a **Lenovo XClarity**.

Seleccione una de las funciones siguientes:

- Iniciar Consola remota
- Iniciar interfaz BMC

Visualización de la información del sistema

La página System Overview (Información general del sistema) le ofrece una instantánea del sistema actual. Los usuarios pueden ver la información básica del sistema, como el tipo de equipo, el sistema operativo, la versión, la versión de firmware de BMC y la versión de firmware de UEFI. También pueden ver el resumen de sucesos de hardware del sistema y recopilar datos de diagnóstico completos.

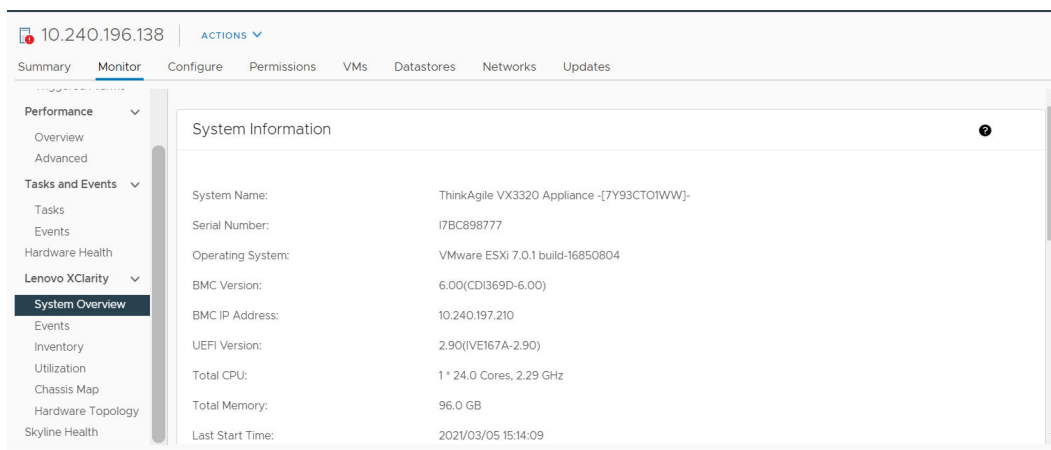


Figura 3. Página System Overview (Información general del sistema)

Inicio de la función de recopilación de diagnóstico del sistema

Procedimiento

Lleve a cabo los pasos siguientes para recopilar los datos de diagnóstico del sistema completo.

Paso 1. Haga clic en **Collect** (Recopilar) ubicado en la sección inferior de la página Información general del sistema.




Nota: Este proceso de recopilación demora hasta cinco minutos. Cuando finaliza, en la página **System Overview** (Información general del sistema) aparece la hora de la última recopilación.

Paso 2. Haga clic en **Download log** (Descargar registro) para descargar los datos más recientes del diagnóstico del sistema.

Visualización de sucesos del servidor

Los usuarios pueden ver los detalles de sucesos de hardware del servidor actual.

Los siguientes iconos indican la gravedad de cada suceso.

-  : crítico
-  : advertencia
-  : informativo

Esta página admite las siguientes operaciones:

- Para filtrar sucesos, haga clic en **Type** (Tipo)
- Para actualizar sucesos, haga clic en **Refresh** (Actualizar)
- Para ordenar los sucesos del sistema, haga clic en el título de la tabla

Visualización del inventario del servidor

La página **Inventory** (Inventario) le ofrece una instantánea del inventario de servidor actual. Los usuarios pueden ver información de la placa del sistema, microprocesadores, memoria, ventilador, sensor, NIC, adaptador de PCI y firmware en esta página.

Utilice **Quick Link (Enlace rápido)** en la parte derecha de la página para acceder a la sección de destino. En una sección específica, haga clic en el símbolo + ver los detalles.

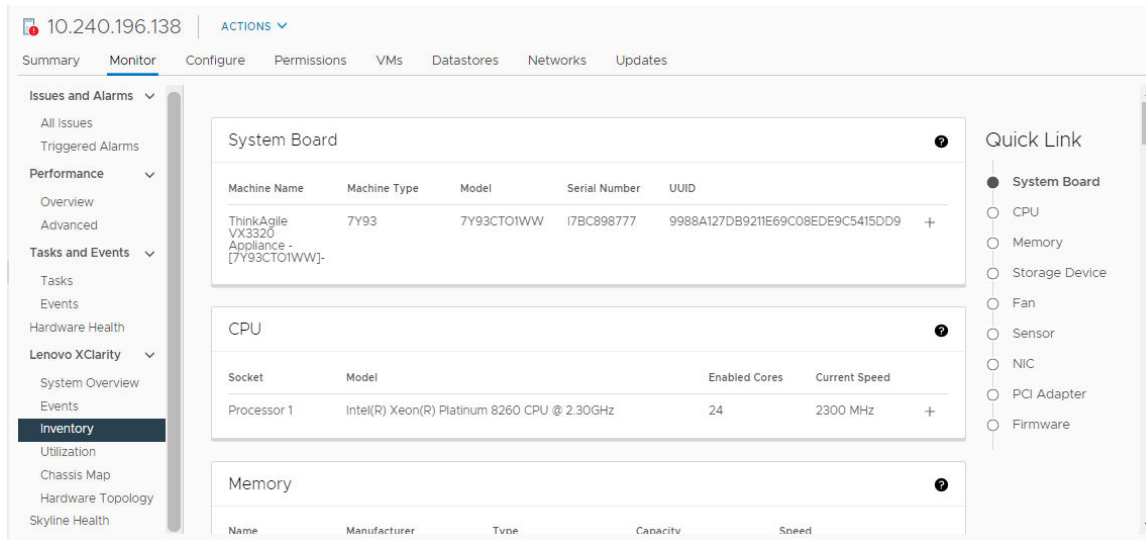


Figura 4. Página "Inventory" (Inventario)

Visualización de utilización del servidor

La página **Utilization (Utilización)** muestra la información de uso histórica y más reciente de temperatura ambiente, entrada de alimentación del sistema, y velocidad del ventilador.

Para mostrar mejor la información, esta página proporciona dos vistas de la información: vista gráfica y vista de tabla.

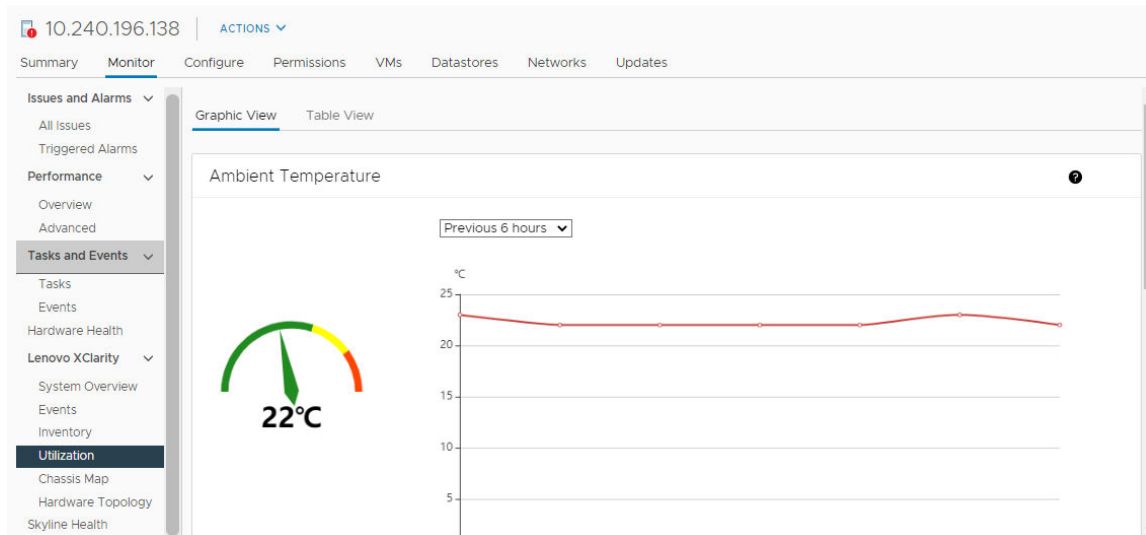


Figura 5. Página "Utilization" (Utilización)

Elemento	Información más reciente	Información histórica
Ambient Temperature (Temperatura ambiente)	Gráfico de termómetro	Gráfico de línea/Lista (6, 12 o 24 horas anteriores)
Power Utilization (Utilización de la alimentación)	Gráfico circular	Gráfico de línea/Lista (1, 6, 12 o 24 horas anteriores)
Fan Speed (Velocidad del ventilador)	Lista	N/A

Nota: Fan Speed (Velocidad del ventilador) solo está disponible en **Table View (Vista de tabla)**.

Trabajo con la topología de hardware

La función de topología de hardware proporciona una vista gráfica integrada para los servidores de dispositivos ThinkAgile VX. Esta interfaz permite ver el diseño del servidor, el inventario de hardware detallado y la información del estado, además de gestionar los discos vSAN.

Topología de hardware del host

La topología de hardware del host ofrece información general sobre los hosts y permite a los usuarios a ejecutar las operaciones en la topología.

Nota: Asegúrese de que vCenter admite el host. En el caso de hosts no compatibles con vCenter, los usuarios pueden comprobar e instalar los paquetes de definición de hardware desde LXCI o desde el navegador siguiendo las instrucciones que se le piden en la página.

Para tener acceso a la página **Hardware Topology (Topología de hardware)**, siga estos pasos:




1. Seleccione un host desde el árbol de inventario del host de vCenter y haga clic en la pestaña **Monitor (Supervisar)** que se encuentra en el panel a la derecha.
2. Haga clic en **Hardware Topology (Topología de hardware)** bajo **Lenovo XClarity**. Se muestra la página Topología de hardware.
3. Realice una de las acciones siguientes:
 - Para ver la información general del host, consulte [“Ver información general del host” en la página 26](#).
 - Para ver la información del disco vSAN, consulte [“Visualización de información de disco vSAN” en la página 27](#).
 - Para ver la información de la fuente de alimentación, consulte [“Visualización del estado de las unidades de fuente de alimentación \(PSU\)” en la página 28](#).
 - Para quitar un disco vSAN, consulte [“Extracción de un disco vSAN” en la página 29](#).
 - Para sustituir un disco vSAN, consulte [“Sustitución de un disco vSAN” en la página 29](#).

Ver información general del host

La página Topología de hardware admite la vista de información general sobre el host.

Información general

En el panel superior de la página **Hardware Topology (Topología de hardware)**, los usuarios pueden ver información general sobre el host:

- **Machine Name (Nombre del equipo)**
- **Machine Type (Tipo de equipo)**
- **Front Panel LED (LED de panel frontal)**
 - : estado de alimentación
 - : estado de LED de ubicación
 - : estado de LED de error.
- **Hardware Health (Estado del hardware)**

- Normal
- Advertencia
- Crítico

Nota: Para ver más información, los usuarios pueden hacer clic en el icono de expandir  que se encuentra en la columna **Hardware Health (Estado del hardware)**.

Acciones

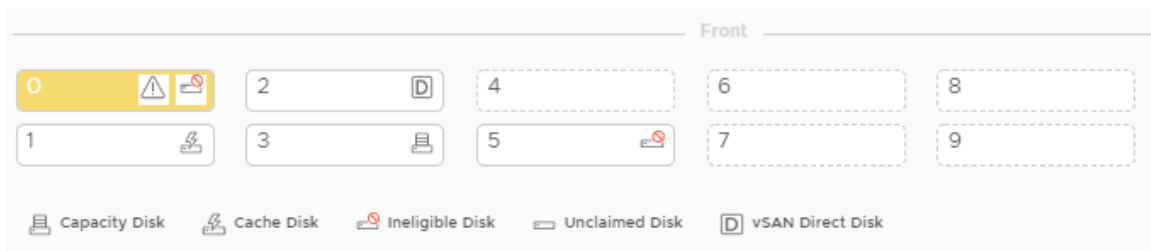
En el lado derecho de este panel, también pueden hacer clic en **VIEW ACTIONS (VER ACCIONES)** y **HOST ACTIONS (ACCIONES DEL HOST)**:

- En **VIEW ACTIONS (Ver acciones)**:
 - **View Detail Inventory (Ver inventario detallado)**: haga clic para acceder a la página **Inventory (Inventario)**.
 - **View Reference Photo (Ver foto de referencia)**: haga clic para acceder a la página de referencia del producto. En esta página se muestran las vistas frontal y posterior de este equipo y se dirige a los usuarios al acceso a la guía del producto en Lenovo Press.
 - **Refresh Hardware Topology (Actualizar topología de hardware)**: haga clic en este para actualizar la información de topología del hardware.
- En **HOST ACTIONS (Acciones del host)**:
 - **Host LED (LED de host)**: haga clic en **Host LED: ON (LED de host: ACTIVADO)**, **Host LED: OFF (LED de host: DESACTIVADO)** o **Host LED: BLINK (LED de host: PARPADEANTE)** para cambiar el estado del LED.
 - **Launch BMC Interface (Iniciar interfaz BMC)**: haga clic en este para tener acceso al sitio web de Lenovo XClarity Controller.
 - **Launch Remote Console (Iniciar Consola remota)**: haga clic en este para tener acceso a la página de la consola remota del sitio web de Lenovo XClarity Controller.

Visualización de información de disco vSAN

La página Topología del hardware proporciona una vista virtual de los discos instalados en las ranuras de servidor.

Figura 6. Topología de hardware



Nota: Para el servidor que tiene placas posteriores traseras, se mostrarán las topologías **Front (Frontal)** y **Rear (Trasera)**.

La topología de hardware ilustra:

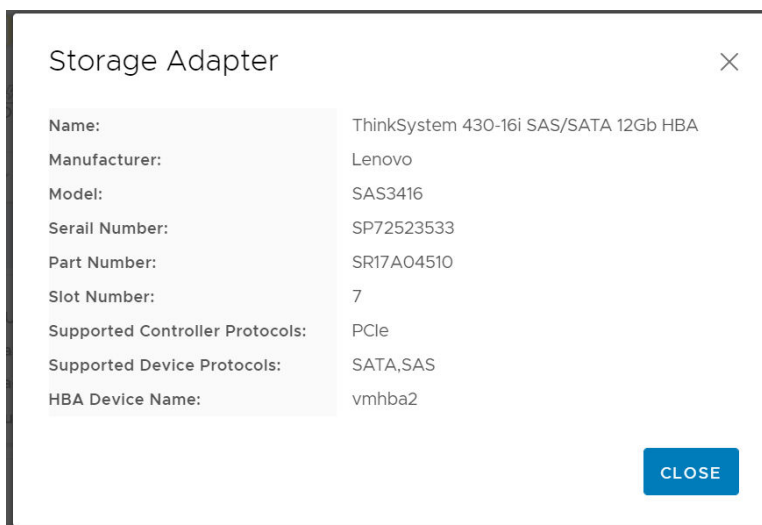
- Ubicación del disco: la ranura sin discos instalados se muestra con líneas punteadas.
- Estado del disco: los distintos colores indican diferentes estados del disco:
 - Blanco: estado normal
 - Amarillo: estado de advertencia
 - Rojo: estado crítico
- Tipo de disco: a la derecha de cada ranura se muestran los iconos de tipo de disco del disco de capacidad, disco caché, disco no disponible, disco no reclamado y disco directo vSAN.

Los usuarios pueden hacer clic en uno de los discos en la topología:

- Si el disco seleccionado pertenece a un grupo vSAN, otros discos en el mismo grupo vSAN se resaltarán con una línea de color negro sólido.
- En **VIEW ACTIONS (Ver acciones)**:
 - **Mostrar leyendas de iconos**: esta opción muestra los iconos utilizados para representar el tipo de disco de los discos en una vista de topología, incluidos el disco caché, el disco de capacidad, el disco no disponible, el disco no reclamado, el disco directo vSAN y la bahía vacía. Para ocultar las leyendas de iconos, vuelva a hacer clic en **Show Icon Legends (Mostrar leyendas de iconos)**.
 - **Mostrar grupos de discos**: esta opción agrega una nueva columna **Disk Group (Grupo de discos)** en la tabla de detalles del disco y muestra el grupo de discos en los discos en la vista de topología. Para ocultar los grupos de discos, vuelva a hacer clic en **Show Disk Groups (Mostrar grupos de discos)**.
- El disco seleccionado se resaltará en la tabla siguiente que indica en detalle la información física y lógica del disco, incluida **Bay (Bahía)**, **Drive Type (Tipo de unidad)**, **Controller (Controlador)**, **Status (Estado)**, **Capacity (Capacidad)** y **Media (Medios)**.
- Si hacen clic en el enlace Grupo de discos en la vista de topología, se resaltarán todos los discos asociados del grupo de discos en la tabla de discos.

Nota: Pueden hacer clic en el nombre del controlador para ver más detalles.

Figura 7. Detalles del controlador



Visualización del estado de las unidades de fuente de alimentación (PSU)

La página Topología de hardware ofrece una vista virtual del estado de las unidades de fuente de alimentación (PSU) instaladas en el servidor.

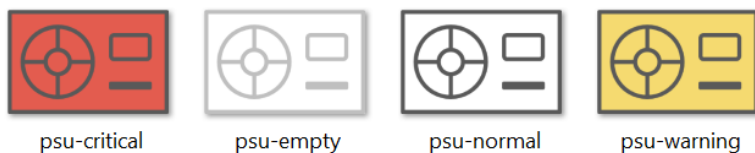


Figura 8. Estado de la PSU

Los diferentes colores indican diferentes estados de la PSU, incluidos:

- Rojo: estado crítico
- Blanco con línea de color gris claro: estado vacío
- Blanco con línea de color gris oscuro: estado normal
- Amarillo: estado de advertencia

Extracción de un disco vSAN

La opción de extracción del disco permite a los usuarios quitar un disco vSAN del grupo de discos y quitarlo físicamente de la bahía de discos.

Notas:

- Antes de quitar el disco caché, recuerde hacer una copia de seguridad de los datos; de lo contrario, puede que se interrumpa la máquina virtual en funcionamiento.
- Si se habilitan la deduplicación y compresión en el host de vSAN, y el disco caché o el último disco de capacidad se elimina del grupo de discos, se eliminará todo el grupo de discos. Si es necesario, los usuarios deben volver a crear el grupo de discos manualmente.
- Después de que el disco físico se extrae de la bahía, el disco se indicará con líneas punteadas y su estado será “vacío”.

Procedimiento

- Paso 1. En la página Topología de hardware, seleccione el disco de destino de la vista de topología.
- Paso 2. En el panel derecho, haga clic en **DISK ACTIONS (Acciones de disco) → Remove Disk (Quitar disco)**. Se muestra el asistente para quitar la unidad.
- Paso 3. En la página Validación, el disco seleccionado está resaltado y se muestra la información relacionada.
- Paso 4. Haga clic en **NEXT (Siguiete)**. Se muestra la página Migrar datos.
- Paso 5. En la lista desplegable **vSAN Data Migration (Migración de datos de vSAN)** que se encuentra en la página Migrar datos, seleccione uno de los siguientes modos deseados para migrar los datos del disco:

Tabla 9. Opciones de migración de datos de vSAN

Opciones	Características admitidas		
	Comprobación previa	Migración de datos a otros discos vSAN en el mismo clúster	Extracción de disco/ grupo de discos
No data migration (Sin migración de datos)	√		√
Ensure accessibility (Garantizar la accesibilidad)	√	√	√
Full data migration (Migración de datos completa)	√	√	√

- Paso 6. Haga clic en **DO IT NOW (Hacerlo ahora)** para quitar el disco del grupo de discos.
- Paso 7. Haga clic en **NEXT (Siguiete)** después de que se ha finalizado el proceso. Se redirigirá a los usuarios a la página Quitar disco.
- Paso 8. En la página Quitar disco, haga clic en **Disk LED (LED de disco)** o **Host LED (LED de host)** para encender/apagar los LED en un disco o en el host, lo que permite al usuario remoto identificar el disco o host correcto.
- Paso 9. Haga clic en **FINISH (Finalizar)** para completar el proceso de extracción del disco.

Sustitución de un disco vSAN

La sustitución de la opción de disco permite a los usuarios reemplazar físicamente el disco seleccionado del grupo de discos por uno nuevo.

Nota: Se reconstruirá todo el grupo de discos si se sustituye el disco caché o el último disco de capacidad. Antes de sustituir el disco caché, recuerde hacer una copia de seguridad de los datos; de lo contrario, puede que se desatienda la máquina virtual en funcionamiento.

Procedimiento

- Paso 1. En la página Topología de hardware, seleccione el disco de destino de la vista de topología.
- Paso 2. En el panel derecho, haga clic en **DISK ACTIONS (Acciones de disco) → Replace Disk (Sustituir el disco)**. Se muestra el asistente para para sustituir unidad.
- Paso 3. En la página Validación, el disco seleccionado está resaltado y se muestra la información relacionada.
- Paso 4. Haga clic en **NEXT (Siguiente)**. Se muestra la página Migrar datos.
- Paso 5. En la lista desplegable **vSAN Data Migration (Migración de datos de vSAN)** que se encuentra en la página Migrar datos, seleccione uno de los siguientes modos deseados para migrar los datos del disco:

Tabla 10. Opciones de migración de datos de vSAN

Opciones	Características admitidas		
	Comprobación previa	Migración de datos a otros discos vSAN en el mismo clúster	Extracción de disco/grupo de discos
No data migration (Sin migración de datos)	√		√
Ensure accessibility (Garantizar la accesibilidad)	√	√	√
Full data migration (Migración de datos completa)	√	√	√

- Paso 6. Haga clic en **DO IT NOW (Hacerlo ahora)** para quitar el disco del grupo de discos.
- Paso 7. Haga clic en **NEXT (Siguiente)** después de que se ha finalizado el proceso. Se redirigirá a los usuarios a la página Quitar disco.
- Paso 8. En la página sustituir disco, haga clic en **DETECT NEW DISK (Detectar nuevo disco)** después de insertar el nuevo disco en la misma bahía. La página mostrará la nueva información del disco.
- Paso 9. Active **Auto Claim New Disk (Reclamación automática de nuevo disco)** para agregar automáticamente el nuevo disco al grupo de discos.
- Paso 10. Haga clic en **FINISH (Finalizar)** para completar el proceso de sustitución del disco.

Topología de hardware del clúster




La topología de hardware del clúster permite ver la topología de todos los hosts de un clúster en una ubicación.

Para tener acceso a la página **Hardware Topology (Topología de hardware)**, siga estos pasos:

1. Seleccione un clúster desde el árbol de inventario del host de vCenter y haga clic en la pestaña **Monitor (Supervisar)** que se encuentra en el panel a la derecha.
2. Haga clic en **Hardware Topology (Topología de hardware)** bajo **Lenovo XClarity**. Se muestra la página Vista de topología de hardware. Los usuarios pueden ver información general sobre el clúster.

Información general

En la página **Hardware Topology (Topología de hardware)**, los usuarios pueden ver la información del estado general del hardware sobre los hosts en la tabla.

- **Total**: Muestra la cantidad de hosts, discos o grupos de discos.
- **Normal** : Muestra la cantidad de hosts, discos o grupos de discos en estado normal.
- **Warning (Advertencia)** : Muestra la cantidad de hosts, discos o grupos de discos en estado de advertencia.
- **Critical (Crítico)** : Muestra la cantidad de hosts, discos o grupos de discos en estado crítico.

Acciones

Se admiten las siguientes operaciones:

- Para buscar un host, introduzca el nombre de este o la dirección IP en el cuadro de búsqueda que se encuentra en la esquina superior derecha y presione **Enter (Intro)**.
- Para ver la información de los hosts en un clúster, haga clic en cualquier número de las columnas **Total/Normal/Warning (Advertencia)/Critical (Crítico)** para expandir la topología de cada host.
- Para ver los detalles de cada host, haga clic en **HOST DETAILS (Detalles del host)** a la derecha de cada topología de host. Se dirigirá a los usuarios a la página Topología de host respectiva.
- Para ver el inventario detallado, consultar la foto o actualizar la topología de hardware, haga clic en **VIEW ACTIONS (Ver acciones)**. Para obtener más información, consulte: [“Acciones” en la página 27](#).
- Para cambiar el estado del LED, iniciar la interfaz de BMC o iniciar el control remoto, haga clic en **HOST ACTIONS (Acciones del host)**. Para obtener más información, consulte: [“Acciones” en la página 27](#).

Inicio de la interfaz web de BMC

Los usuarios pueden iniciar la interfaz web del controlador de gestión de placa base (BMC) para un servidor específico en Lenovo XClarity Integrator.

Procedimiento

Lleve a cabo los pasos siguientes para iniciar la interfaz BMC para un servidor.

- Paso 1. Haga clic con el botón derecho del mouse en un host del árbol de inventarios de host de vCenter. Se muestra el cuadro con la lista desplegable **Actions (Acciones)**.
- Paso 2. Elija **Lenovo XClarity → Launch BMC Interface (Iniciar interfaz BMC)**. Aparecerá un cuadro de diálogo de confirmación.
- Paso 3. Haga clic en **OK (Aceptar)**. Aparece la interfaz web de BMC para el servidor.
- Paso 4. Utilice las credenciales BMC para iniciar sesión en la interfaz BMC.

Inicio de la consola remota

Los usuarios pueden iniciar una sesión de control remoto para un servidor gestionado y realizar operaciones en este servidor como si estuviera en una consola local, como encender o apagar el servidor y para montar lógicamente una unidad local o remota.

Procedimiento

Lleve a cabo los siguientes pasos para iniciar la consola remota para un servidor gestionado.

- Paso 1. Haga clic con el botón derecho del mouse en un host del árbol de inventarios de host de vCenter. Se muestra el cuadro con la lista desplegable **Actions (Acciones)**.
- Paso 2. Elija **Lenovo XClarity → Launch Remote Console (Iniciar Consola remota)**. Aparecerá un cuadro de diálogo de confirmación.

Paso 3. Haga clic en **OK (Aceptar)** y acepte las advertencias de seguridad que se muestran en el navegador web. Se inicia la sesión de control remoto para el servidor.

Uso de la función Actualizaciones de firmware

La función de Actualización de firmware permite obtener y desplegar UpdateXpress System Pack (UXSP) o actualizaciones de firmware individuales en el servidor ESXi que se está ejecutando.

Actualizar un solo servidor ESXi es similar a actualizar los servidores utilizando la función actualización gradual del sistema. La única diferencia es que cuando se está creando una tarea de actualización, se muestra y se puede seleccionar el ESXi actual. Para obtener más información sobre cómo actualizar las preferencias y gestionar tareas de actualización, consulte [“Uso de la función Rolling System Update \(Actualización gradual del sistema\)”](#) en la página 41.

Uso de la función Política de alimentación

La función Política de alimentación permite asignar menos alimentación y refrigeración a un sistema si el firmware admite y habilita la función Política de alimentación. Esta función ayuda a reducir los costes de infraestructura de un centro de datos y, potencialmente, permite introducir más servidores en la infraestructura existente.

El valor de Limitación de alimentación es el valor que definido para un servidor de bastidor o servidor Blade que estará limitado por el firmware. El valor de limitación de la alimentación se mantiene en todos los ciclos de alimentación, tanto en servidores de bastidor como en servidores blade. Si se establece un valor de Limitación de alimentación, el consumo de alimentación del sistema no superará el valor definido.

Si la limitación de alimentación se admite y está habilitada para un servidor, se pueden recuperar los valores mínimos y máximos de limitación de la alimentación del servidor mediante Lenovo XClarity Integrator y se mostrarán como una gama de consumo de alimentación para el servidor. En el siguiente ejemplo, el valor mínimo es 0 y el valor máximo es 750.

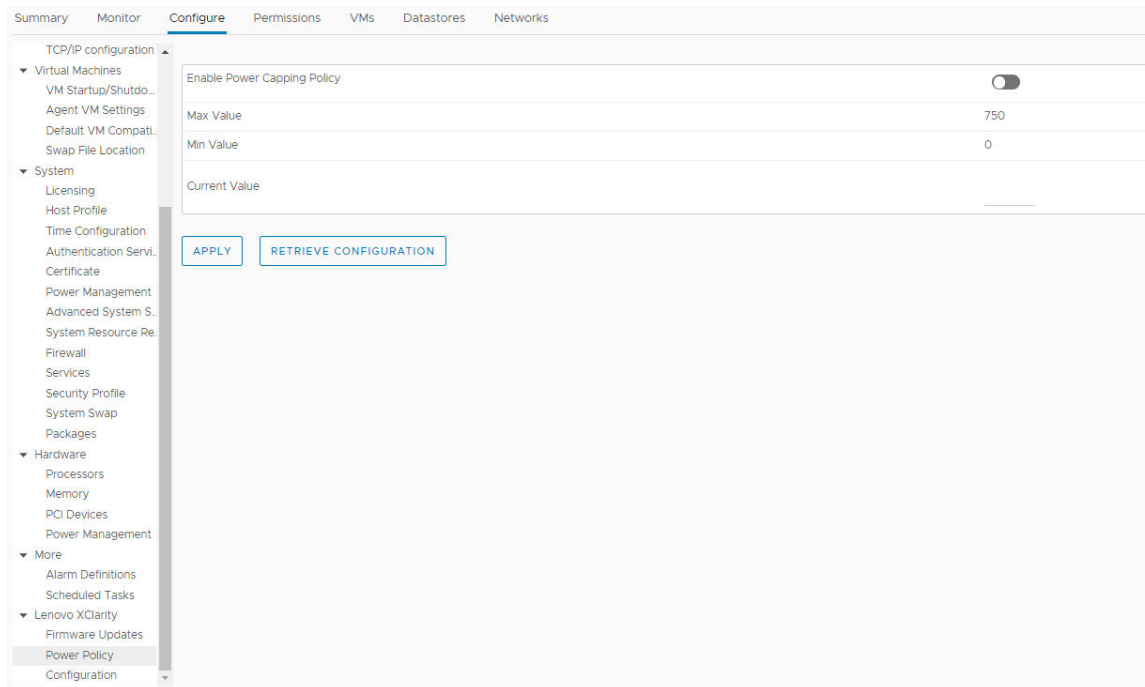


Figura 9. Página de configuración de “Power Policy (Política de alimentación)”

Uso de la función Valores del sistema

La función “System settings (Valores de sistema)” permite gestionar los valores del sistema de un host. Si Lenovo XClarity Administrator gestiona el servidor y Lenovo XClarity Administrator está registrado en este Lenovo XClarity Integrator, los usuarios pueden desplegar un patrón de configuración en el host; de lo contrario, solo pueden ver las opciones de arranque y valores del sistema para el host.

Despliegue de un patrón de configuración en un servidor

Una vez que haya registrado Lenovo XClarity Administrator en Lenovo XClarity Integrator, los usuarios pueden desplegar o desactivar un patrón de configuración en cada uno de los servidores compatibles gestionados por un Lenovo XClarity Administrator. Un patrón de servidor representa una configuración de servidor previa al SO que incluye la configuración del almacenamiento local, el adaptador de E/S, el arranque y otros valores de firmware del BMC y UEFI. Un patrón de servidor se utiliza como patrón general para configurar rápidamente varios servidores de forma simultánea.

Acerca de esta tarea

Si Lenovo XClarity Administrator no tiene ningún patrón predefinido, los usuarios pueden crear patrones de servidores al hacer clic en el vínculo para abrir Lenovo XClarity Administrator. Esta tarea se realiza en la página **Configuration Pattern** (Patrón de configuración).

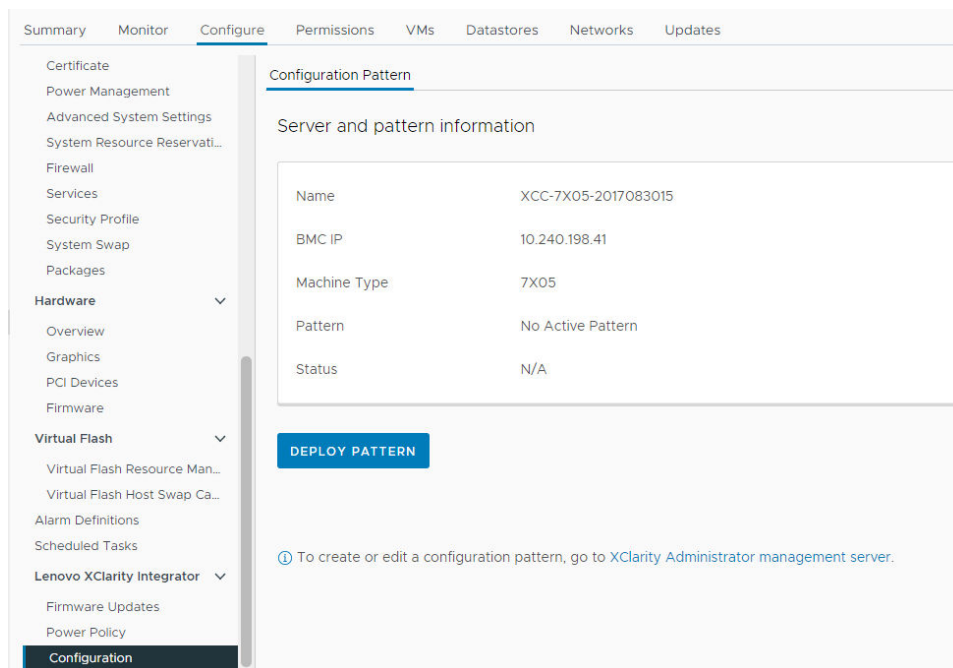


Figura 10. Página Patrón de configuración

Procedimiento

- Paso 1. Seleccione el host de destino y haga clic en **Configure (Configurar) → Lenovo XClarity Integrator → Configuration (Configuración)**.
- Paso 2. En la página **Configuration Pattern (Patrón de configuración)**, seleccione el patrón de configuración.
 - **DEPLOY PATTERN (DESPLEGAR PATRÓN)**. Despliega el patrón seleccionado en los servidores de destino.

- **DEACTIVATE PATTERN (DESACTIVAR PATRÓN)**. Desactiva el patrón seleccionado en los servidores de destino.

Paso 3. En la página **Deploy Pattern (Desplegar patrón)**, seleccione el patrón de destino en la lista desplegable y, a continuación, haga clic en **NEXT (SIGUIENTE)**.

Paso 4. En la página **Confirm Action (Confirmar acción)**, seleccione la hora de activación y, a continuación, haga clic en **DONE (HECHO)**.

Notas:

- **Immediate Activation (Activación inmediata)**. Despliegue el patrón y reinicie el servidor para que los cambios surtan efecto inmediatamente.
- **Delayed Activation (Activación con retardo)**. Despliegue el patrón, pero no reinicie el servidor. Los cambios se aplicarán en el siguiente reinicio.
- Dependiendo de la configuración del servidor, el proceso de despliegue puede tardar unos 30 minutos.
- La contraseña de encendido o protección del sistema detiene el reinicio del servidor. Si la contraseña de encendido o la protección del sistema está habilitada y es necesario reiniciar el servidor de destino durante la actualización, los usuarios deben tomar medidas que sigan el mensaje de la indicación.

Uso de la función Opciones de arranque

En el panel **Boot Options (Opciones de arranque)**, los dispositivos opcionales y el orden de arranque actual se muestran de izquierda a derecha. Para cambiar el orden, suba o baje la opción de orden de arranque o haga clic en los botones de flecha correspondientes que hay entre las dos columnas.

Una indicación de fecha y hora de la última actualización se muestra a la derecha del botón **RETRIEVE CONFIGURATION** (Obtener configuración). Haga clic en **RETRIEVE CONFIGURATION** (Obtener configuración) para obtener los valores de opciones de arranque más recientes. Haga clic en **SAVE (GUARDAR)** para guardar los nuevos valores de opciones de arranque si se han realizado cambios.

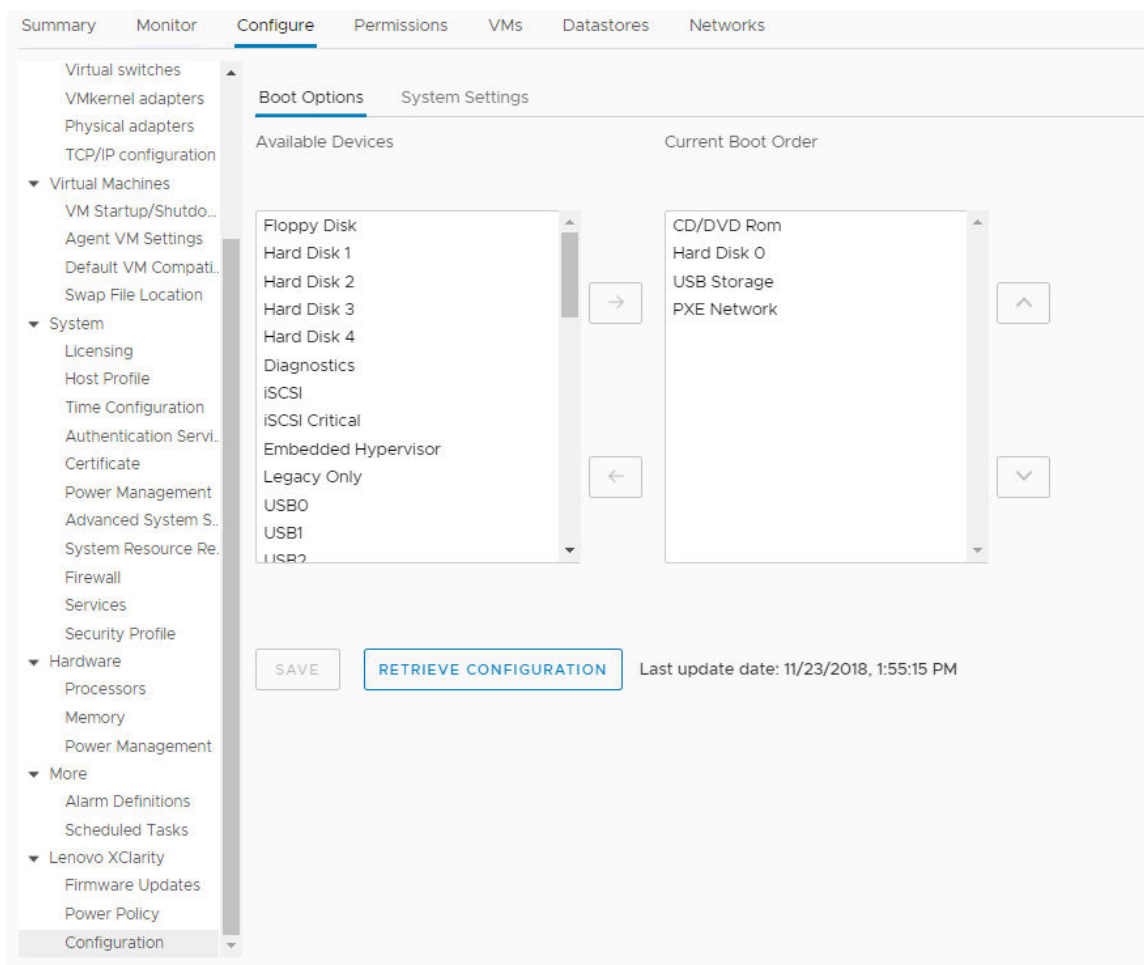


Figura 11. Panel “Boot Options (Opciones de arranque)”

Visualización y exportación de los valores del sistema

Los usuarios pueden ver y exportar los valores del sistema del servidor ThinkSystem, Lenovo System x, BladeCenter o del servidor Flex utilizando el siguiente procedimiento.

Procedimiento

Realice los siguientes pasos para ver y exportar los valores del sistema:

1. En el panel **Configure (Configurar)**, haga clic en **Configuration (Configuración)** en **Lenovo XClarity** y, a continuación, haga clic en la pestaña **System Settings (Valores de sistema)** en el panel derecho.
En el panel **System Settings (Valores de sistema)**, los valores del sistema se enumeran en los botones **EXPORT TO CSV (Exportar a CSV)** y **RETRIEVE CONFIGURATION (Obtener configuración)**. Una indicación de fecha y hora de la última actualización se muestra a la derecha del botón **RETRIEVE CONFIGURATION (Obtener configuración)**.

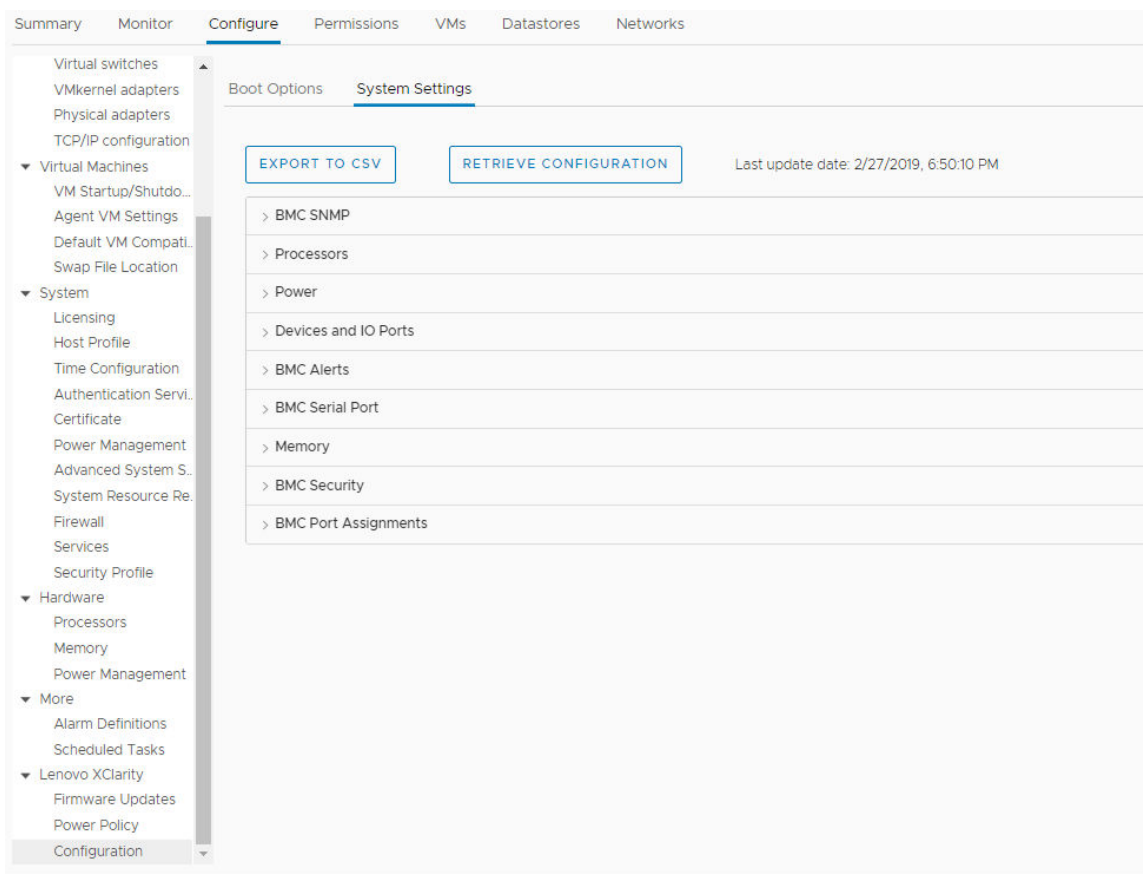


Figura 12. Panel “System Settings” (Valores de sistema)

Paso 2. Realice una de las acciones siguientes:

- Haga clic en **RETRIEVE CONFIGURATION** (Obtener configuración) para obtener los valores de configuración más recientes.
- Para exportar los valores del sistema en un archivo CSV, haga clic en **EXPORT TO CSV** (Exportar a CSV).

Capítulo 6. Gestión de clústeres

Los temas de esta sección describen cómo utilizar Lenovo XClarity Integrator para gestionar clústeres.

Procedimiento

Siga los siguientes pasos para ver las funciones de gestión de clúster de Lenovo XClarity Integrator.

Paso 1. Seleccione un clúster del árbol de inventario de vCenter.

Paso 2. Haga clic en la pestaña **Configure** (Configurar).

En el panel de navegación izquierdo, seleccione una de las siguientes funciones en **Lenovo XClarity**:

- **Rolling Update** (Actualización gradual)
- **Rolling Reboot** (Reinicio gradual)

Uso de la función vSphere Lifecycle Manager

Cuando los usuarios gestionan el clúster utilizando una única imagen, se recomienda utilizar la función vSphere Lifecycle Manager.

Antes de empezar

Asegúrese de que LXCI esté habilitado como el gestor de soporte de hardware para vLCM. Para obtener más información acerca de habilitar vLCM, consulte [“Habilitar/deshabilitar vSphere Lifecycle Manager” en la página 11](#).

Importación de los complementos básicos ESXi y Lenovo

Los usuarios pueden importar las versiones de ESXi y los complementos de Lenovo a vLCM.

Procedimiento

Paso 1. Seleccione **Lifecycle Manager (Gestor de ciclo de vida)** desde la lista del menú desplegable **Menu (Menú)**. Se muestra la página **Lifecycle Manager (Gestor de ciclo de vida)**.

Paso 2. En la página **Lifecycle Manager (Gestor de ciclo de vida)**, seleccione una de las siguientes opciones de la lista desplegable **ACTIONS (ACCIONES)**:

- Seleccione **Sync Updates** (Sincronizar actualizaciones) para descargar automáticamente los complementos estándar ESXi y de personalización de Lenovo del almacén en línea de vSphere Lifecycle Manager.
- Seleccione **Import Updates** (Importar actualizaciones) para importar la imagen de ESXi personalizada de Lenovo en el almacén manualmente. Los usuarios pueden descargar la imagen de ESXi personalizada de Lenovo desde https://vmware.lenovo.com/content/custom_iso.

Nota: En el área **Image Depot (Depósito de imágenes)**, los usuarios también pueden seleccionar la versión de ESXi/complementos del proveedor/componente para ver la información detallada en el panel derecho.

Gestión de paquetes de firmware

Los usuarios pueden gestionar los paquetes de firmware en el cliente de vSphere.

Procedimiento

Paso 1. Seleccione **Lenovo XClarity Integrator** desde la lista del menú desplegable **Menu** (Menú) y haga clic en **Manage Firmware Packages** (Gestionar paquetes de firmware) en el panel izquierdo.

Paso 2. En el panel derecho, lleve a cabo uno o más de los siguientes procedimientos:

- Para actualizar el firmware a una versión anterior, habilite **Permit Downgrade** (Permitir versión anterior).
- Para detener para actualizar el firmware cuya versión instalada en el host es posterior a la versión definida en la imagen de vLCM, deshabilite la opción **Permit Downgrade** (Permitir versión anterior).
- Para ensayar el firmware u omitir el ensayo en operaciones de vLCM, habilite o deshabilite la opción **Stage Firmware (Ensayar firmware)**.

Nota: Esta función solo se admite en los servidores ThinkSystem V3 y ThinkAgile V3.

- Para importar manualmente los paquetes de firmware, haga clic en **IMPORT (Importar)**. Aparece la ventana "Import Firmware Package (Importar el paquete de firmware)".
 1. En la página **Remote repository** (Repositorio remoto), introduzca la URL, el nombre de usuario y la contraseña y, a continuación, haga clic en **NEXT** (Siguiendo).
 2. En la página **Firmware package (Paquete de firmware)**, seleccione el paquete de firmware y haga clic en **FINISH (Finalizar)**.
- Para descargar el paquete de firmware necesario, seleccione el paquete de firmware de destino de la lista y, a continuación, haga clic en **DOWNLOAD (DESCARGAR)**.
- Para copiar el paquete de firmware para personalizarlo, seleccione el paquete de firmware de destino y, a continuación, haga clic en **COPY (COPIAR)**.
- Para personalizar el paquete de firmware, seleccione el paquete de firmware copiado y, a continuación, haga clic en **EDIT (EDITAR)**. Aparece la ventana Editar paquetes de firmware.

Notas:

- Solo se pueden editar los paquetes de firmware copiados.
- Es posible que Lenovo no valide el paquete de firmware sustituido, lo que puede provocar un error de actualización. Por lo tanto, no se recomienda editar el paquete de firmware.
 1. Seleccione el paquete de firmware de destino y haga clic en **REPLACE (SUSTITUIR)**. Aparece la ventana Sustituir firmware.
 2. En la página **Remote repository** (Repositorio remoto), introduzca la URL, el nombre de usuario y la contraseña y, a continuación, haga clic en **NEXT** (Siguiendo).

Nota: La URL debe ser la URL de la carpeta compartida que contiene los archivos de firmware CHG/TXT/UXZ/XML que se van a importar.

3. En la página **Firmware**, seleccione el paquete de firmware que se va a importar y haga clic en **FINISH (FINALIZAR)**. Aparece la página **Edit Firmware Packages (Editar paquetes de firmware)**.
4. En la página **Edit Firmware Packages (Editar paquetes de firmware)**, lleve a cabo uno o más de los siguientes procedimientos:
 - Para completar el proceso de sustitución, haga clic en **APPLY (APLICAR) → CONFIRM (CONFIRMAR)**.
 - Para quitar el paquete de firmware, selecciónelo y, a continuación, haga clic en **REMOVE (QUITAR) → APPLY (APLICAR) → CONFIRM (CONFIRMAR)**.
- Para eliminar el paquete de firmware, seleccione el paquete de firmware de destino y, a continuación, haga clic en **DELETE (ELIMINAR)**.
- Para importar la lista de paquetes de firmware, haga clic en **IMPORT LIST (IMPORTAR LISTA)**, después en la URL para descargar el archivo desde el sitio web de Lenovo, a continuación en **Choose File (Seleccionar archivo)** para importar el archivo y, por último, en **IMPORT (IMPORTAR)**.

Nota: Utilice esta opción cuando LXCI esté desconectado de Internet.

- Para actualizar la lista de paquetes de firmware, haga clic en **REFRESH LIST (ACTUALIZAR LISTA)**.

Nota: Utilice esta opción cuando LXCI acceda a Internet.

Gestión del clúster a través de una imagen

Los usuarios pueden gestionar el clúster a través de una imagen.


Procedimiento

- Paso 1. Seleccione **Hosts and Clusters** (Hosts y clústeres) desde la lista del menú desplegable **Menu** (Menú).
- Paso 2. Seleccione el clúster necesario en el panel izquierdo y haga clic en **Updates (Actualizaciones) → Image (Imagen)** en la página vLCM.

Creación de una imagen de clúster

Los usuarios pueden crear una imagen de clúster para el servidor.

Procedimiento

- Paso 1. En el área **Image** (Imagen), haga clic en **EDIT** (Editar) y lleve a cabo uno o más de los siguientes pasos:
 - En el campo **ESXi Version** (Versión de ESXi), seleccione una versión de ESXi en la lista desplegable.
 - En el campo **Vendor Addon** (Complemento de proveedor), haga clic en **SELECT** (Seleccionar) para seleccionar los complementos de Lenovo para ESXi.
 - En el campo **Firmware and Drivers Addon** (Complemento de firmware y controladores), haga clic en  para seleccionar **Lenovo XClarity Integrator** en la lista desplegable **Select the hardware support manager** (Seleccionar el gestor de soporte de hardware) y luego seleccione un complemento de firmware y controlador en la tabla **Select a firmware and driver addon** (Seleccionar un complemento de firmware y controladores).


Nota: Al configurar el proxy en vCenter, los usuarios deben deshabilitar el proxy o permitir la conexión desde vCenter a Lenovo XClarity Integrator (protocolo HTTPS, puerto 443) en la configuración del proxy. De lo contrario, no se mostrará la lista de firmware ni de complementos de controladores.

- En el campo **Components** (Componentes), haga clic en **Show details** (Mostrar detalles) para añadir componentes.
- Paso 2. Realice una de las siguientes acciones después de editar la imagen:
 - Haga clic en **SAVE** (Guardar) para guardar los cambios.
 - Haga clic en **VALIDATE** (Validar) para comprobar la conformidad de los complementos de Lenovo para ESXi y firmware.
 - Haga clic en **CANCEL** (Cancelar) para eliminar los cambios.

Comprobación de compatibilidad de hardware

Antes de la corrección de firmware, compruebe la compatibilidad del hardware para un clúster de vSAN. Esta función compara el firmware y los controladores que se muestran en la imagen contra el hardware de Lenovo y los controladores compatibles que se encuentran en la lista de compatibilidad de hardware (HCL) de vSAN.

Procedimiento

- Paso 1. En el área **Image (Imagen)**, haga clic en  y seleccione **Check hardware compatibility (Comprobar compatibilidad de hardware)** para comparar el firmware y los controladores de la imagen del clúster con la lista de compatibilidad de hardware (HCL) de vSAN.

Paso 2. Haga clic en **See details (Ver detalles)** para ver los resultados de la comparación en el área de resultados de la **Compatibility check results (Resultados de comprobación de compatibilidad)** y resolver los posibles problemas de compatibilidad de hardware.

Comprobación del cumplimiento del clúster

Los usuarios pueden comprobar el cumplimiento entre los servidores existentes en un clúster y la imagen configurada.

Procedimiento

Paso 1. En el área **Image Compliance (Cumplimiento de imagen)**, haga clic en **CHECK COMPLIANCE (Comprobar cumplimiento)** para comprobar el cumplimiento de las versiones de ESXi, el firmware y los controladores entre los servidores existentes en un clúster y la imagen configurada.

Paso 2. Compruebe los resultados de conformidad en la tabla **Software compliance (Cumplimiento de software)** y la tabla **Firmware compliance (Cumplimiento de firmware)**.

Corrección de servidores no compatibles

El usuario puede corregir las versiones de ESXi, los complementos de Lenovo para ESXi, el firmware y los controladores de los servidores no conformes bajo un clúster.

Procedimiento

Paso 1. Haga clic en **RUN PRE-CHECK (EJECUTAR COMPROBACIÓN PREVIA)** para comprobar el estado de los servidores existentes.

Nota: La contraseña de encendido o protección del sistema detiene el reinicio del servidor. Si la contraseña de encendido o la protección del sistema está habilitada y es necesario reiniciar el servidor de destino durante la actualización, los usuarios deben tomar medidas que sigan el mensaje de la indicación.

Paso 2. Consulte los resultados en la ventana de Comprobación previa completada y resuelva los problemas.

Paso 3. Para corregir las versiones de ESXi, los complementos de Lenovo para ESXi, el firmware y los controladores de uno o de todos los servidores no conformes bajo un clúster, realice lo siguiente:

- Para realizar la corrección de todos los servidores, haga clic en **REMEDIATE ALL (CORREGIR TODO)**
- Para llevar a cabo la corrección de un servidor, seleccione el servidor de destino y, a continuación, haga clic en **Actions (Acciones) → Remediate (Corregir)** en la página del servidor.

Permitir una versión anterior

El usuario puede actualizar el firmware en un clúster cuando la versión del firmware instalado en el host es posterior a la versión definida en la imagen de vLCM.

Procedimiento

Paso 1. Habilite la opción **Permit Downgrade (Permitir versión anterior)** en la página “Manage Firmware Packages (Gestionar paquetes de firmware)”. Consulte [“Gestión de paquetes de firmware” en la página 37](#).

Paso 2. Realice las operaciones de vLCM.

Ensayo del firmware

El usuario puede ensayar el firmware para servidores no conformes en un clúster.

Nota: Esta función solo es compatible con los servidores ThinkSystem V3 y ThinkAgile V3 cuya versión de ESXi es v8.0 o posterior.

Procedimiento

- Paso 1. Habilite la opción **Stage Firmware (Ensayar firmware)** en la página “Manage Firmware Packages (Gestionar paquetes de firmware)”. Consulte [“Gestión de paquetes de firmware” en la página 37](#).
- Paso 2. Haga clic en **STAGE ALL (ENSAYAR TODO)** o en **ACTIONS (ACCIONES) → Stage (Ensayar)** para ensayar el firmware.
- Paso 3. (Opcional) Corrección de servidores no compatibles. Consulte [“Corrección de servidores no compatibles” en la página 40](#).

Trabajar con la función Gestión proactiva del hardware

Introducida en vSphere 8.0u3, la función Gestión proactiva del hardware (PHM) es una función que debe notificarse en una unidad de disco que presenta un error antes de ver problemas de lectura/escritura relacionados con vSAN, por lo que los usuarios tienen recomendaciones de VMware y Lenovo en caso de un problema de estado del disco.

Antes de empezar

- Asegúrese de que LXCI esté habilitado como el gestor de soporte de hardware para PHM. Para obtener más información acerca de habilitar PHM, consulte [“Habilitación/deshabilitación de la gestión proactiva del hardware” en la página 11](#).
- Asegúrese de que el disco esté agregado a un grupo de discos vSAN. PHM solo funciona para los discos del grupo de discos vSAN.

Visualización de información de salud

Cuando LXCI recibe un suceso PHM admitido de XCC, este notifica a vCenter.

Haga lo siguiente para ver la información de estado del clúster de destino:

Procedimiento

- Paso 1. Seleccione el clúster de vSAN, haga clic en **Monitor → vSAN → Skyline Health (Estado de Skyline)**. Se mostrará la página Skyline Health (Estado de Skyline).
- Paso 2. En la página Skyline Health (Estado de Skyline), desplácese hacia abajo para buscar el área **Storage Vendor Reported Drive Health (Estado de la unidad informada del proveedor de almacenamiento)**, haga clic en **TROUBLESHOOT (RESOLUCIÓN DE PROBLEMAS)** y realice uno o más de los siguientes procedimientos:
 - Para comprobar los detalles y la recomendación del suceso, seleccione la pestaña **TROUBLESHOOT (RESOLUCIÓN DE PROBLEMAS)**.
 - Para comprobar el historial del suceso, seleccione la pestaña **HISTORY DETAILS (DETALLES DEL HISTORIAL)**.

Uso de la función Rolling System Update (Actualización gradual del sistema)

La función Actualización gradual del sistema (RSU) ofrece una forma de realizar actualizaciones de firmware sin perturbaciones. RSU gestiona completamente el firmware organizando actualizaciones “graduales” aprovechando el movimiento dinámico de la máquina virtual dentro de un clúster VMware definido y completando todo el proceso de actualización, incluido el reinicio automático del host de ESXi, sin que se produzca ninguna interrupción en los servicios de la aplicación que se ejecutan en el host.

Los usuarios pueden actualizar el firmware utilizando la función Actualización del sistema gradual si no es posible utilizar vSphere Lifecycle Manager en algunos casos. Por ejemplo, el clúster no está gestionado por una sola imagen o los usuarios pretenden actualizar parte del firmware no en los paquetes de firmware para vLCM.

Para obtener más información sobre cómo actualizar el firmware a través de vLCM, consulte [“Uso de la función vSphere Lifecycle Manager” en la página 37](#).

Antes de empezar

- Los siguientes servidores no se admiten:
 - Servidores ThinkServer
 - Servidor ThinkAgile Serie HX
- Asegúrese de que VMware vCenter DRS está habilitado y se está ejecutando en el modo automatizado completo.
- Asegúrese de que el puerto 6990 esté habilitado.

Configuración de las preferencias de Actualización del sistema gradual

Los usuarios pueden configurar el repositorio de actualizaciones y descargar los valores para las actualizaciones de firmware en el panel “Preferences (Preferencias)”.

Especificar la ubicación del repositorio para actualizaciones

Los usuarios pueden configurar el repositorio de actualizaciones donde la función Actualización gradual del sistema comprobará las actualizaciones de firmware al crear una tarea de tipo **Update without Policy (Actualizar sin política)**.

Procedimiento

Paso 1. En el panel de navegación izquierdo, haga clic en **Rolling Update (Actualización gradual)**, en **Lenovo XClarity Integrator**. Luego, haga clic en **Preferences (Preferencias)** en el panel derecho.

Paso 2. En el panel “Preferences (Preferencias)”, seleccione una de las siguientes formas de especificar la ubicación del repositorio de firmware.

- De manera predeterminada, se utiliza un directorio interno del servidor del dispositivo de Lenovo XClarity Integrator como repositorio de firmware y **Download metadata from Lenovo website (Descargar metadatos del sitio web de Lenovo)** está habilitado.
- Para utilizar una carpeta externa como repositorio de firmware, haga clic en **EDIT (EDITAR)** en la parte derecha de la sección **Repository folder (Carpeta de repositorio)**.
 1. En la página **Repository Settings (Configuración del repositorio)**, seleccione **Use Remote Repository (Usar repositorio remoto)**.
 2. Introduzca la URL del repositorio con el formato `\\<IP_address>\<repository_path>` y, si es necesario, introduzca el nombre de usuario y la contraseña.
 3. Haga clic en **OK (ACEPTAR)** para guardar los cambios.

Notas:

- Para la configuración del repositorio en un host que usa direcciones IPv6, especifique la dirección de red utilizando el nombre de dominio completamente calificado (FQDN).
- Se debe conceder el permiso de escritura de la carpeta compartida.
- LXCI admite los siguientes tipos de carpetas externas en la red:
 - Carpeta compartida en un servidor de Windows
 - Carpeta compartida en un servidor de archivos Linux Samba (con el modo de seguridad NTLM)

Paso 3. Haga clic en **EDIT (EDITAR)** en la parte derecha de **Download metadata from the Lenovo website (Descargar metadatos desde el sitio web de Lenovo)** para configurar los valores de descarga del paquete de actualización.

- a. Si el servidor de LXCI no puede acceder a Internet directamente, configure los valores de Internet en la página de administración del dispositivo de “Lenovo XClarity Integrator”. Después de iniciar sesión en la Página Web, haga clic en **Network Settings (Valores de red)** en el panel izquierdo y haga clic en **Internet Settings (Configuración de Internet)** en el panel derecho. Luego, configure los valores del proxy.

- b. Seleccione **Download from website (Descargar desde el sitio web)** y **Periodically download (Descargar periódicamente)** para establecer la frecuencia para descargar de forma automática y periódica los paquetes de actualizaciones.
- c. Haga clic en **OK (Aceptar)**.

Paso 4. (Opcional) Haga clic en **CHECK NOW (BUSCAR AHORA)** en la esquina inferior derecha de la página para descargar el paquete de actualización más reciente desde el sitio web de Lenovo.

Notas:

- **CHECK NOW** (Comprobar ahora) solo está disponible cuando **Download from website (Descargar desde el sitio web)** se seleccionó en el paso anterior.
- La hora de la descarga más reciente se muestra en la esquina inferior izquierda del panel.

Gestión de las tareas de la función Rolling System Update (Actualización gradual del sistema)

La función Actualización del sistema gradual (RSU) permite a los usuarios crear y gestionar tareas de actualización del sistema gradual. Una tarea RSU contiene todos los datos y todas las opciones para efectuar una actualización del sistema gradual.

Procedimiento

- Paso 1. Seleccione el clúster de destino desde el árbol de inventario y haga clic en la pestaña **Configure (Configurar)**.
- Paso 2. En el panel de navegación izquierdo, haga clic en **Rolling Update (Actualización gradual)**, en **Lenovo XClarity Integrator**. La página **Rolling Reboot (Actualización gradual)** se muestra en el panel derecho.

La tabla de tareas proporciona la siguiente información detallada sobre una tarea RSU:

- Nombre de tarea
- Tipo
- Estado
- Hora de creación
- Hora de inicio
- Hora de finalización

Tabla 11. Estados de la tarea **Actualización gradual del sistema**

Destino	Estado	Descripción
Tarea de actualización gradual	Not Started	La tarea no se ha iniciado.
	Running	La tarea se está ejecutando.
	Canceled	La tarea se ha cancelado.
	Failed	Se ha producido un error al descargar el paquete de firmware.
	Finished	La tarea se ha completado.
Host	Not Started	La actualización del host no ha comenzado.
	Migrating	El host está entrando en modo de mantenimiento.
	Maintenance	El host está en modo de mantenimiento.
	Updating	El firmware del host se está actualizando.
	Reboot	El host se está reiniciando tras terminar la actualización.
	Exit Maintenance	El host está saliendo del modo de mantenimiento.

Tabla 11. Estados de la tarea Actualización gradual del sistema (continuación)

Destino	Estado	Descripción
	Success	El firmware se ha actualizado correctamente.
	Failed	Causas de un error en un host: <ul style="list-style-type: none"> No se puede obtener el paquete de actualización. No se puede entrar en el modo de mantenimiento. No se puede actualizar el firmware. No se puede reiniciar el host. No se puede salir del modo de mantenimiento.
Firmware	Not Started	La actualización del firmware no ha comenzado.
	Running	La actualización del firmware se está ejecutando.
	Success	El firmware se ha actualizado correctamente.
	Failed	Error al actualizar el firmware.

Paso 3. Realice uno de los pasos siguientes.

Tabla 12. Funciones de tareas de actualización continua del sistema

Función de la tarea	Descripción
CREAR	Crear una nueva tarea de RSU.
COPIAR	Crear una nueva tarea de RSU desde una tarea existente de RSU.
EDITAR	Editar una tarea RSU que no se ha iniciado.
QUITAR	Eliminar una tarea de RSU de la lista de tareas.
CANCELAR	Detener una tarea RSU en ejecución.
ACTUALIZAR	Actualizar la lista de RSU.

Creación de una tarea RSU

Utilice la opción **CREATE (CREAR)** para crear una nueva tarea de Actualización del sistema gradual (RSU) y programar la actualización de firmware del host en un periodo planificado.

Procedimiento

- Paso 1. Seleccione **Configure (Configurar) → Lenovo XClarity Integrator → Rolling Update (Actualización gradual)** y haga clic en la pestaña **Rolling Update (Actualización gradual)** en la parte superior.
- Paso 2. En la página **Rolling Update (Actualización gradual)**, haga clic en **CREATE (CREAR)** para iniciar el asistente de creación de tareas.
- Paso 3. En la página **Create Task (Crear tarea)**, introduzca el nombre de la tarea, seleccione uno de los siguientes tipos de tareas y, a continuación, haga clic en **NEXT (SIGUIENTE)**.
 - **Update with a policy from XClarity Administrator (Actualizar con una política de XClarity Administrator)**: seleccione esta opción para asegurarse de que el firmware del servidor esté en cumplimiento. Antes de realizar la actualización, asegúrese de que:
 - Los servidores que están ejecutando ESXi estén agregados y gestionados por Lenovo XClarity Administrator.
 - Se crean políticas de cumplimiento de firmware en Lenovo XClarity Administrator.
 - El firmware se descarga desde Lenovo XClarity Administrator
 - Lenovo XClarity Administrator se registra en Lenovo XClarity Integrator.
 - Si el firmware de un servidor se actualiza de otras maneras en lugar de Lenovo XClarity Administrator, antes de crear la tarea de actualización continua (con una política) en vCenter,

se recomienda actualizar la información de inventario de este servidor en Lenovo XClarity Administrator.

- **Update without a policy (Actualizar sin política):** si Lenovo XClarity Administrator no está disponible, seleccione las actualizaciones de firmware individuales o UXSP para cada servidor. Antes de realizar la actualización, asegúrese de que:
 - Se concede acceso a BMC.
 - Se configura el repositorio de actualización y se descarga el firmware (consulte [“Configuración de las preferencias de Actualización del sistema gradual” en la página 42](#)).

Notas:

- Asegúrese de que el tipo de tarea de destino cumpla los requisitos antes de la actualización.
- No se pueden usar caracteres ascii en el nombre de tarea.

Paso 4. En la página **Select Version (Seleccionar versión)**, seleccione el tipo de equipo, el host y la política y, a continuación, haga clic en **NEXT (SIGUIENTE)**.

Paso 5. En la página **Task Options (Opciones de tarea)**, seleccione o alterne una o más de las opciones siguientes y, a continuación, haga clic en **NEXT (SIGUIENTE)**.

- **Reboot after Update (Reiniciar después de una actualización):** especifica si debe reiniciar el sistema operativo después de actualizar el firmware. Esta opción es obligatoria si está seleccionada la opción **Update without a policy (Actualizar sin política)**.
- **Number of nodes to be updated in parallel (Número de nodos que se van a actualizar en paralelo):** especifica el número de hosts que se van a actualizar al mismo tiempo. Para actualizar con una política mediante LXCA, el número máximo es 16; para actualizar sin un método de política, el número máximo es ocho. Una instancia de LXCI admite actualizar el firmware en paralelo para 32 hosts como máximo.
- **Allow updating to a firmware version lower than the current version (Permitir actualizar a una versión de firmware inferior a la versión actual):** especifique si la versión del firmware debe ser anterior a la versión actual.
- **Run Memory Test (Ejecutar prueba de memoria):** ejecute una prueba de memoria una vez que la actualización de firmware se haya completado después de reiniciar el servidor. Esta opción es compatible con todos los servidores ThinkSystem, excepto los servidores ThinkSystem SR635, SR645, SR655 y SR665. Los usuarios pueden comprobar los resultados de la prueba de memoria en la vista de sucesos de LXCI o comprobar el estado del trabajo en LXCA.
- **Perform VM Evacuation (Realizar evacuación de VM):** Especifica si se han de migrar las máquinas virtuales antes de actualizar el host.
- **Stop the overall task if any node fails (Detener la tarea general si se produce un error en un nodo):** especifica si se debe detener la tarea de actualización completa cuando se produce un error de actualización para un host en el clúster.
- **Perform the update (Realizar la actualización):** seleccione la hora a la que debe realizarse la actualización. Seleccione **Now (Ahora)** para realizar la actualización ahora mismo o establezca el valor en **Schedule Time (Programar hora)** para realizar la actualización a la hora programada.

Nota: La contraseña de encendido o protección del sistema detiene el reinicio del servidor. Si la contraseña de encendido o la protección del sistema está habilitada y es necesario reiniciar el servidor de destino durante la actualización, los usuarios deben tomar medidas que sigan el mensaje de la indicación.

Paso 6. En la página **Confirm (Confirmar)**, confirme la información y, a continuación, haga clic en **FINISH (FINALIZAR)**.

Clonación de una tarea RSU completada

Utilice la opción **COPY (COPIAR)** para clonar una nueva tarea de Actualización del sistema gradual (RSU) utilizando una tarea cuyo estado sea finalizada, con fallos o cancelada.

Procedimiento

- Paso 1. Seleccione **Configure (Configurar) → Lenovo XClarity Integrator → Rolling Update (Actualización gradual)** y haga clic en la pestaña **Rolling Update (Actualización gradual)** en la parte superior.
- Paso 2. En la página **Rolling Update (Actualización gradual)**, seleccione una tarea de RSU finalizada, con fallos o cancelada de la lista.
- Paso 3. Haga clic en **COPY (COPIAR)** para iniciar el Asistente para copiar tareas.
- Paso 4. Edite la selección original y, a continuación, haga clic en **FINISH (FINALIZAR)** para guardar la nueva tarea.

Edición de una tarea RSU no iniciada

Utilice la opción **EDIT (EDITAR)** para editar una tarea de Actualización del sistema gradual (RSU) no iniciada.

Procedimiento

- Paso 1. Seleccione **Configure (Configurar) → Lenovo XClarity Integrator → Rolling Update (Actualización gradual)**.
- Paso 2. Seleccione una tarea de RSU no iniciada en la lista y, a continuación, haga clic en **EDIT (EDITAR)** para iniciar el asistente para crear tareas.
- Paso 3. Edite la tarea y, a continuación, haga clic en **FINISH (FINALIZAR)** para guardar los cambios.

Eliminación de una tarea de RSU

Utilice la opción **REMOVE (QUITAR)** para quitar una tarea de Actualización del sistema gradual (RSU) de la lista de tareas si no se está ejecutando actualmente. Todas las tareas de RSU que no se están ejecutando actualmente se pueden quitar.

Procedimiento

- Paso 1. Seleccione **Configure (Configurar) → Lenovo XClarity Integrator → Rolling Update (Actualización gradual)**.
- Paso 2. En la lista, seleccione una o más tareas de RSU que no se estén ejecutando.
- Paso 3. Haga clic en **REMOVE (QUITAR)**. Las tareas seleccionadas se quitan de la lista de tareas.

Cancelación de una tarea RSU en ejecución

Utilice la opción **CANCEL (CANCELAR)** para cancelar una tarea de Actualización del sistema gradual (RSU) que está en ejecución. Al cancelar una tarea, el estado de esta cambia a Canceling (Cancelando).

Procedimiento

- Paso 1. Seleccione **Configure (Configurar) → Lenovo XClarity Integrator → Rolling Update (Actualización gradual)**.
- Paso 2. En la lista, seleccione una tarea RSU que se encuentre en ejecución.
- Paso 3. Haga clic en **CANCEL (CANCELAR)**. La tarea RSU completa la actualización del host que se ha iniciado y solo cancela las otras. Esta operación puede tardar varios minutos en completarse.

Actualización de la lista de tareas de RSU

Utilice la opción **REFRESH (ACTUALIZAR)** para actualizar la lista de tareas de Actualización del sistema gradual (RSU).

Procedimiento

- Paso 1. Seleccione **Configure (Configurar) → Lenovo XClarity Integrator → Rolling Update (Actualización gradual)**.

Paso 2. Haga clic en **REFRESH (ACTUALIZAR)** para actualizar la lista de tareas de RSU.

Uso de la función Reinicio gradual del sistema

La función Reinicio gradual del sistema (RSR) reinicia un servidor mientras el sistema continúa ejecutándose sin interrupción en los servicios de aplicación mediante la migración dinámica de VM.

Antes de empezar

Para poder utilizar la función Reinicio gradual del sistema, deben cumplirse los siguientes requisitos previos:

- Los siguientes servidores no se admiten:
 - Servidor ThinkAgile Serie HX
- Se necesita VMware vCenter Enterprise o Enterprise Plus Edition con DRS.
- DRS está habilitado y se está ejecutando en el modo automatizado completo.

Gestión de las tareas Reinicio gradual del sistema

La función Reinicio del sistema gradual (RSR) permite crear y gestionar las tareas de reinicio gradual. Una tarea RSR contiene todos los datos y todas las opciones para efectuar un re arranque continuo.

Procedimiento

Paso 1. Seleccione el clúster de destino desde el árbol de inventario y haga clic en la pestaña **Configure (Configurar)**.

Paso 2. En el panel de navegación izquierdo, haga clic en **Rolling Reboot (Reinicio gradual)** en **Lenovo XClarity Integrator**. La página **Rolling Reboot (Reinicio gradual)** se muestra en el panel derecho.

La tabla de tareas proporciona la siguiente información detallada sobre una tarea RSR:

- Nombre de tarea
- Estado
- Progreso
- Hora de inicio
- Hora de finalización

Paso 3. Realice uno de los pasos siguientes.

Tabla 13. Funciones de tareas de reinicio gradual del sistema

Función de la tarea	Descripción
CREAR	Crea una nueva tarea de RSR.
EDITAR	Editar una tarea RSR que no se ha iniciado.
COPIAR	Crear una nueva tarea de RSR desde una tarea existente de RSR.
ELIMINAR	Eliminar una tarea de RSR de la lista de tareas.
CANCELAR	Detener una tarea RSR en ejecución.

Creación de una tarea RSR

Utilice la opción **CREATE (CREAR)** para crear una nueva tarea de reinicio del sistema gradual (RSR). Cada clúster solo puede tener una tarea RSR activa.

Procedimiento

Paso 1. Seleccione **Configure (Configurar)** → **Lenovo XClarity Integrator** → **Rolling Reboot (Reinicio gradual)**.

Paso 2. Haga clic en **CREATE (CREAR)** para iniciar el Asistente para crear tareas.

Nota: El botón **CREATE (CREAR)** solo está habilitado si una tarea se muestra con el estado **Finished (Finalizada)**, **Canceled (Cancelada)** o **Failed (Ha fallado)** en la lista de tareas.

- Paso 3. En la página **Select hosts (Seleccionar hosts)**, introduzca el nombre de la tarea, seleccione uno o varios hosts de destino y, a continuación, haga clic en **NEXT (SIGUIENTE)**.
- Paso 4. En **Reboot options (Opciones de re arranque)**, seleccione o alterne una o más de las opciones siguientes y, a continuación, haga clic en **NEXT (SIGUIENTE)**.
- **Parallelization (Paralelización):** especifica el número de hosts que pueden reiniciarse al mismo tiempo. Para reiniciar varios hosts simultáneamente se necesitan más recursos del sistema. Se recomienda establecer el valor de acuerdo con los recursos del sistema disponibles actuales del clúster, por ejemplo, la CPU y la memoria en el servidor vCenter. El valor predeterminado es 1 y el valor máximo es 4.
 - **Stop On Error (Detener en caso de error):** especifica si se debe continuar con la actualización si un host ha fallado.
 - **Recommission Mode (Modo de reactivación):** esta opción solo está visible en el clúster de vSAN. Los usuarios pueden especificar el modo de reactivación al migrar máquinas virtuales.
 - **Schedule (Programar):** especifica el momento el que debe iniciarse la tarea.

Nota: La contraseña de encendido o protección del sistema detiene el reinicio del servidor. Si la contraseña de encendido o la protección del sistema está habilitada y es necesario reiniciar el servidor de destino durante la actualización, los usuarios deben tomar medidas que sigan el mensaje de la indicación.

- Paso 5. En la página **Summary (Resumen)**, confirme la información y, a continuación, haga clic en **FINISH (FINALIZAR)**. La función RSU iniciará la tarea de acuerdo con la programación.

Edición de una tarea RSR no iniciada

Utilice la opción **EDIT (EDITAR)** para editar una tarea de Reinicio del sistema gradual (RSR) no iniciada.

Procedimiento

- Paso 1. Seleccione **Configure (Configurar) → Lenovo XClarity Integrator → Rolling Reboot (Reinicio gradual)**.
- Paso 2. Seleccione una tarea de RSR no iniciada en la lista y, a continuación, haga clic en **EDIT (EDITAR)** para iniciar el asistente para crear tareas.
- Paso 3. Edite la tarea y, a continuación, haga clic en **FINISH (FINALIZAR)** para guardar los cambios.

Clonación de una tarea RSR completada

Utilice la opción **COPY (COPIAR)** para clonar una nueva tarea de Reinicio del sistema gradual (RSR) utilizando una tarea cuyo estado sea finalizada, con fallos o cancelada.

Procedimiento

- Paso 1. Seleccione **Configure (Configurar) → Lenovo XClarity Integrator → Rolling Reboot (Reinicio gradual)**.
- Paso 2. Seleccione una tarea RSR finalizada, fallida o cancelada de la lista.
- Paso 3. Haga clic en **COPY (COPIAR)** para iniciar el Asistente para copiar tareas.
- Paso 4. Edite la selección original y, a continuación, haga clic en **FINISH (FINALIZAR)** para guardar la nueva tarea.

Eliminación de una tarea RSR

Utilice la opción **DELETE (ELIMINAR)** para eliminar una tarea de Reinicio del sistema gradual (RSR) de la lista de tareas si no se está ejecutando. Todas las tareas de RSR que no se están ejecutando actualmente se pueden eliminar.

Procedimiento

- Paso 1. Seleccione **Configure (Configurar) → Lenovo XClarity Integrator → Rolling Reboot (Reinicio gradual)**.
- Paso 2. En la lista, seleccione una o más tareas de RSR que no se estén ejecutando.
- Paso 3. Haga clic en **DELETE (ELIMINAR)**. Las tareas seleccionadas se quitan de la lista de tareas.

Cancelación de una tarea RSR en ejecución

Utilice la opción **CANCEL (CANCELAR)** para cancelar una tarea de Reinicio del sistema gradual (RSR) mientras está en funcionamiento. Al cancelar una tarea, el estado de esta cambia a Canceling (Cancelando).

Procedimiento

- Paso 1. Seleccione **Configure (Configurar) → Lenovo XClarity Integrator → Rolling Reboot (Reinicio gradual)**.
- Paso 2. En la lista, seleccione una tarea RSR que se encuentre en ejecución.
- Paso 3. Haga clic en **CANCEL (CANCELAR)**. La tarea RSR completa la actualización del host que se ha iniciado y solo cancela las otras. Esta operación puede tardar varios minutos en completarse.

Visualización de informe de la tarea de RSR

La vista del informe de reinicio gradual del sistema proporciona información de estado detallada de la tarea.

Procedimiento

Seleccione **Configure (Configurar) → Lenovo XClarity → Rolling Reboot (Reinicio gradual)** y haga clic en un enlace de estado en la columna **Status (Estado)** para abrir la vista de Informe de reinicio de sistema gradual. La tabla siguiente muestra los estados de las tareas y de los hosts. Para obtener información detallada acerca de las tareas Reinicio gradual del sistema, consulte [“Uso de la función Reinicio gradual del sistema” en la página 47](#).

Tabla 14. Estado de la tarea Reinicio gradual del sistema

Destino	Estado	Descripción
Tarea Reinicio gradual	Not Started	La tarea no se ha iniciado.
	Running	La tarea se está ejecutando.
	Canceled	La tarea se ha cancelado.
	Failed	Causas de un error en una tarea: <ul style="list-style-type: none">• Se ha producido un error al descargar el paquete de firmware.• Se produjo un error al reiniciar el host de ESXi.• Se ha producido un error en la migración de la VM.• Se ha producido un error en la actualización del firmware
	Finished	La tarea se ha completado.
Host	Not Started	La actualización del host no ha comenzado.
	Migrating	El host está entrando en modo de mantenimiento.
	Maintenance	El host está en modo de mantenimiento.
	Reboot	El host se está reiniciando tras terminar la actualización.
	Exit Maintenance	El host está saliendo del modo de mantenimiento.
	Success	El firmware se ha actualizado correctamente.

Tabla 14. Estado de la tarea Reinicio gradual del sistema (continuación)

Destino	Estado	Descripción
	Failed	Causas de un error en un host: <ul style="list-style-type: none"> • No se puede entrar en el modo de mantenimiento. • No se puede reiniciar el host. • No se puede salir del modo de mantenimiento.

Trabajo con alta disponibilidad proactiva

VMware vSphere v6.5 añade la nueva característica HA preventiva, que es una optimización de la función de alta disponibilidad (HA) original. Lenovo XClarity Integrator para VMware vCenter admite la característica HA preventiva al registrar un proveedor de Lenovo HA preventiva para VMware vCenter.

Antes de empezar

- Asegúrese de que VMware vSphere v6.5 o posterior está instalado.
- Asegúrese de que Lenovo XClarity Integrator esté registrado correctamente en VMware vCenter.

Habilitación de VMware vCenter HA preventiva con el proveedor de HA preventiva de Lenovo para un clúster

Antes de empezar

Si el clúster no está vacío, asegúrese de solicitar acceso a BMC para cada host del clúster. De lo contrario, es posible que el proveedor de alta disponibilidad proactiva de Lenovo no se muestre correctamente.

Si el mismo host con acceso al BMC se ha eliminado y se ha vuelto a agregar, los usuarios deben volver a solicitar acceso a BMC, incluso si la interfaz de usuario indica que el host puede acceder a BMC. De lo contrario, es posible que el proveedor de alta disponibilidad proactiva de Lenovo no se muestre correctamente.

Procedimiento

- Paso 1. En el cliente de vSphere, haga clic en el clúster que se va a configurar.
- Paso 2. Seleccione **Configure (Configurar)** → **vSphere Availability (Disponibilidad de vSphere)** y, a continuación, haga clic en **Edit (Editar)** en el lado derecho de la página. Aparece un cuadro de diálogo de configuración.
- Paso 3. En **vSphere DRS**, seleccione **Turn ON vSphere DRS (Activar vSphere DRS)**.
- Paso 4. En **vSphere Availability (Disponibilidad de vSphere)**, seleccione **Turn ON Proactive HA (Activar HA preventiva)**.
- Paso 5. En **Proactive HA Failures and Responses (Fallas y respuestas de HA preventiva)**, establezca **Automation Level (Nivel de automatización)** en **Automated** y establezca **Remediation (Remediación)** en **Mixed Mode** o **Maintenance Mode**.
- Paso 6. En la lista de proveedores de HA preventiva, seleccione el proveedor **com.lenovo.HealthUpdateProvider_ver100**.
- Paso 7. Opcional: Seleccione ignorar ciertas condiciones de error para los hosts específicos o en todo el clúster haciendo clic en **Edit (Editar)** en el lado derecho del cuadro de diálogo. Aparece otro cuadro de diálogo en el que los usuarios pueden seleccionar los sucesos y hosts para ignorar las condiciones de error. Para obtener más información, consulte la guía de usuario de VMware vSphere.

Nota: Los usuarios pueden utilizar otros valores del nivel y corrección automatización según VMware, pero existen algunas limitaciones. Por ejemplo, si utilizan los modos “manual” y

“cuarentena”, el host debe tener al menos 1 VM; de lo contrario, los sucesos de condición no se recibirán.

Agregar un host en un clúster con HA preventiva habilitada (con un proveedor de Lenovo)

Procedimiento

- Paso 1. Agregue el host en un DataCenter o cualquier clúster con HA preventiva deshabilitada.
- Paso 2. Solicitud de acceso BMC del host (consulte [“Detección y gestión de BMC” en la página 15](#)).
- Paso 3. Mueva el host al clúster con HA preventiva habilitada.

Nota: Si el mismo host con acceso al BMC se ha eliminado y se ha vuelto a agregar, los usuarios deben volver a solicitar acceso a BMC, incluso si la interfaz de usuario indica que el host puede acceder a BMC; de lo contrario, no se podrá quitar el host del clúster habilitado para alta disponibilidad proactiva.

Reutilizar el proveedor de HA preventiva de Lenovo

El proveedor de alta disponibilidad proactiva de Lenovo se registra automáticamente en VMware vCenter al registrar Lenovo XClarity Integrator en VMware vCenter, en la página del asistente o de administración. Cuando los usuarios cancelan el registro de Lenovo XClarity Integrator en VMware vCenter, se mostrará una ventana en la que se le consultará si desea cancelar también el registro de proveedor de alta disponibilidad proactiva. Normalmente, los usuarios pueden mantener el proveedor de VMware vCenter para que se pueda reutilizar la próxima vez que registre Lenovo XClarity Integrator en VMware vCenter y se mantiene el proveedor de configuración de VMware vCenter.

Pulsación de alta disponibilidad proactiva

Lenovo XClarity Integrator requiere la pulsación con VMware vCenter para asegurarse de que la HA preventiva funcione correctamente. Si se muestra el mensaje “Provider com.lenovo.HealthUpdateProvider_ver101 has not posted an update in 300 seconds” (El proveedor com.lenovo.HealthUpdateProvider_ver101 no ha publicado una actualización en 300 segundos) en la lista de sucesos del clúster habilitado con alta disponibilidad proactiva, la pulsación puede estar inactiva por algún motivo. Compruebe la red para comprobar si Lenovo XClarity Integrator correctamente puede comunicarse con VMware vCenter y si el dispositivo de Lenovo XClarity Integrator está disponible. Si el problema persiste, reinicie Lenovo XClarity Integrator.

Gestión de sucesos del hardware

Los sucesos de hardware y las alarmas están integradas en vCenter. Lenovo XClarity Integrator para VMware vCenter carga sucesos de los nodos fuera de banda (OOB) de BMC en el servidor vCenter, lo que permite que los administradores los vean y gestionen desde vSphere Client. De esta forma, también obtienen una sola visión global heterogénea de todos los sucesos del sistema del host dentro del entorno gestionado.

Qué debe hacer a continuación

Seleccione la pestaña **Events (Sucesos)** en vSphere Client para ver los sucesos de hardware de Lenovo.

Alarmas

Cuando un suceso de Lenovo se envía a VMware vCenter Server, el estado general del host cambia basándose en la gravedad del suceso en cuestión. Si los cambios efectuados en el estado del host cumplen los criterios asignados por el administrador, se activa una alarma.

Cuando se produce una alarma, en la parte derecha de la ventana de Cliente vSphere aparece un icono a lo largo de la barra de herramientas situada encima de las pestañas del Cliente vSphere o en el icono del host del árbol del inventario.

Para ver una lista de todas las alarmas contenidas en la pestaña **Alarms** (Alarmas), haga clic en el icono de alarmas.

Capítulo 7. Administración de Lenovo XClarity Integrator

Este capítulo proporciona información sobre cómo utilizar la página web de administrador de Lenovo XClarity Integrator para VMware vCenter para recopilar datos del servicio, registrar la extensión y crear copias de seguridad y restaurar las configuraciones del dispositivo.

Configuración de conexiones de vCenter

Cuando Lenovo XClarity Integrator para VMware vCenter se despliega inicialmente, se registra en un servidor vCenter. Los usuarios pueden registrar Lenovo XClarity Integrator para VMware vCenter en servidores vCenter adicionales. También pueden cancelar el registro de Lenovo XClarity Integrator para VMware vCenter de un servidor vCenter.

Registro de Lenovo XClarity Integrator en un servidor vCenter

En el modo asociado, los usuarios pueden registrar Lenovo XClarity Integrator en un servidor vCenter o en varios servidores vCenter.

Antes de empezar

Prepare un nombre de usuario y una contraseña de vCenter para registrar Lenovo XClarity Integrator en el servidor vCenter. El usuario de vCenter puede ser un administrador de vCenter o un usuario de servicio dedicado con bajo privilegio de seguridad. Si se utiliza un usuario con servicio dedicado, se requieren los siguientes privilegios:

- Alarms.Create
- Datacenter.Create
- Extension.Register
- Extension.Unregister
- Extension.Update
- Global.LogEvent
- HealthUpdateProvider.Register
- HealthUpdateProvider.Unregister
- HealthUpdateProvider.Update
- Host.Config.Maintenance
- Host.Inventory.ModifyCluster
- Resource.ColdMigrate
- Resource.HotMigrate
- Sessions.ValidateSession

Nota: Estos privilegios se pueden otorgar de forma manual o automática al usuario de vCenter en el registro.

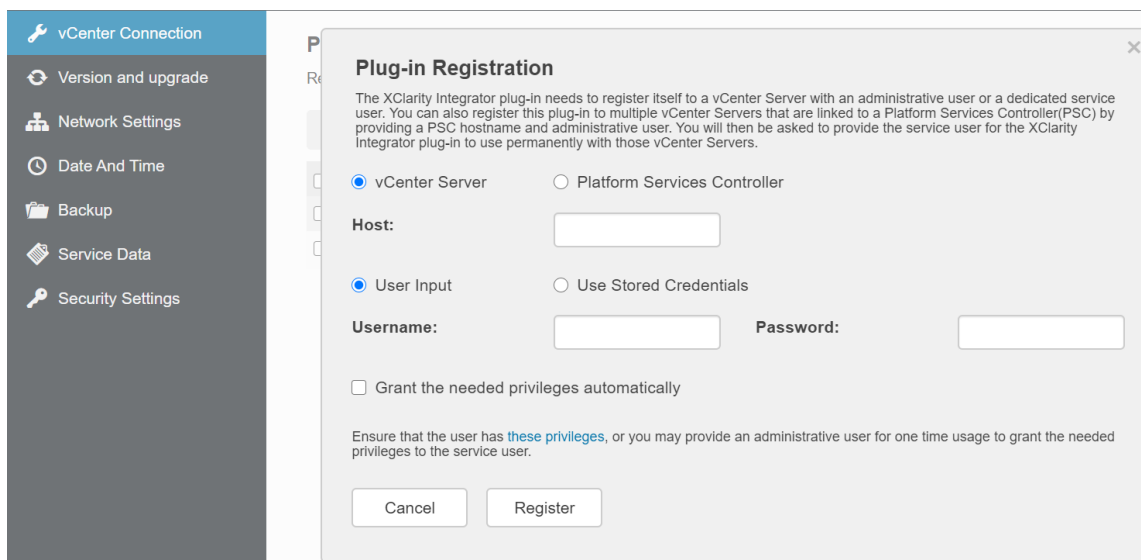
Registrar LXCI en un servidor vCenter

Los usuarios pueden registrar Lenovo XClarity Integrator en un servidor vCenter o en varios servidores vCenter por separado.

Procedimiento

Lleve a cabo los pasos siguientes para registrar Lenovo XClarity Integrator en un servidor vCenter:

Paso 1. En la página **vCenter Connection** (Conexión a vCenter), haga clic en **Register** (Registrar). Se abre la página **Plug-in Registration (Registro de complemento)**.



Paso 2. Seleccione **vCenter Server** (Servidor vCenter). En el campo **Host**, especifique el nombre de dominio completamente calificado (FQDN) o la dirección IP del servidor vCenter.

Nota: Si el vCenter está configurado con el FQDN, se recomienda que especifique el FQDN vCenter en lugar de la dirección IP. En tanto, asegúrese de que DNS está configurado en el panel **Network Settings** (Valores de red).

Paso 3. Realice una de las acciones siguientes:

- Para registrar manualmente, seleccione **User Input** (Entrada del usuario) e ingrese el nombre de usuario de vCenter en el campo **Username** (Nombre de usuario) y la contraseña en el campo **Password** (Contraseña).
- Para registrarse a través de las credenciales, seleccione **Use Stored Credentials (Utilizar credenciales almacenadas) → Manage (Gestionar) → Create (Crear)**. En la ventana Create new stored credentials (Crear nuevas credenciales almacenadas), introduzca el nombre de usuario de vCenter en el campo **User name (Nombre de usuario)** y la contraseña en el campo **Password (Contraseña)** y el campo **Confirm Password (Confirmar contraseña)**, haga clic en **Save (Guardar) → Create (Cerrar)** y seleccione las credenciales en la lista desplegable.

Nota: Si el usuario de vCenter no tiene los privilegios requeridos por Lenovo XClarity Integrator, seleccione la casilla de verificación **Otorgar los privilegios necesarios automáticamente**, especifique una cuenta de usuario administrativo en el campo **Usuario administrativo** y especifique la contraseña en el campo **Contraseña**. Lenovo XClarity Integrator otorgará automáticamente los privilegios al usuario de vCenter a través de la cuenta de usuario administrativo. Sin embargo, Lenovo XClarity Integrator no guardará la información de la cuenta administrativa.

Paso 4. Haga clic en **Register** (Registrar).

Registrar LXCI en varios servidores vCenter en modo asociado

Los usuarios pueden registrar Lenovo XClarity Integrator en varios servidores vCenter conectados al Controlador de servicios de plataforma (PSC) en modo vinculado mediante un nombre de host PSC.

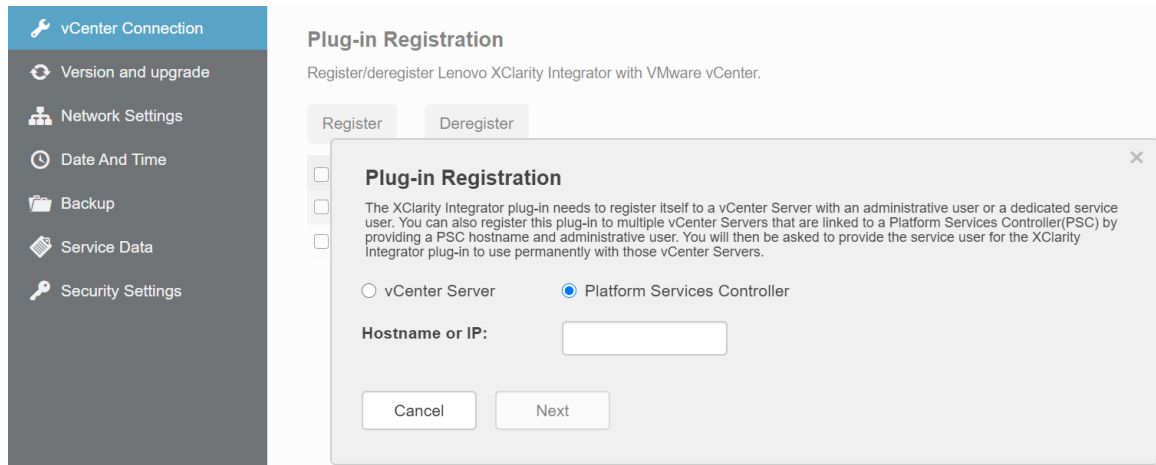
Nota: El número máximo de servidores vCenter que puede gestionar una instancia de plug-in de LXCI es de 1000. Si el número total de servidores vCenter para un modo vinculado supera los 1000, los usuarios deben desplegar varias instancias de plug-in de LXCI y registrar cada instancia en un vCenter.

Procedimiento

Lleve a cabo los pasos siguientes para registrar Lenovo XClarity Integrator en varios servidores vCenter en modo asociado:

- Paso 1. En la página **vCenter Connection** (Conexión a vCenter), haga clic en **Register** (Registrar). Se abre la página **Plug-in Registration (Registro de complemento)**.
- Paso 2. Seleccione **Platform Services Controller** (Controlador de servicios de plataforma), especifique el nombre de dominio completamente calificado (FQDN) o la dirección IP de PSC en el campo **Hostname or IP** (Nombre de host o IP) y haga clic en **Next** (Siguiente).

Nota: Si se introduce el FQDN, asegúrese de que DNS está configurado en la página “Network Settings (Valores de red)”.



- Paso 3. En la lista de **Host**, seleccione los servidores vCenter de destino y, a continuación, haga clic en **Next (Siguiente)**.
- Paso 4. Realice una de las acciones siguientes:
 - Para registrar manualmente, seleccione **User Input** (Entrada del usuario) e ingrese el nombre de usuario de vCenter en el campo **Username** (Nombre de usuario) y la contraseña en el campo **Password** (Contraseña).
 - Para registrarse a través de las credenciales, seleccione **Use Stored Credentials (Utilizar credenciales almacenadas)** → **Manage (Gestionar)** → **Create (Crear)**. En la ventana **Create new stored credentials (Crear nuevas credenciales almacenadas)**, introduzca el nombre de usuario de vCenter en el campo **User name (Nombre de usuario)** y la contraseña en el campo **Password (Contraseña)** y el campo **Confirm Password (Confirmar contraseña)**, haga clic en **Save (Guardar)** → **Create (Cerrar)** y seleccione las credenciales en la lista desplegable.

Notas:

- El usuario de vCenter debe tener acceso a todos los servidores vCenter de destino.
- Si el usuario de vCenter no tiene los privilegios requeridos por Lenovo XClarity Integrator, seleccione la casilla de verificación **Otorgar los privilegios necesarios automáticamente**, especifique una cuenta de usuario administrativo en el campo **Usuario administrativo** y especifique la contraseña en el campo **Contraseña**. Lenovo XClarity Integrator otorgará automáticamente los privilegios al usuario de vCenter a través de la cuenta de usuario administrativo. Sin embargo, Lenovo XClarity Integrator no guardará la información de la cuenta administrativa.

- Paso 5. Haga clic en **Register** (Registrar).

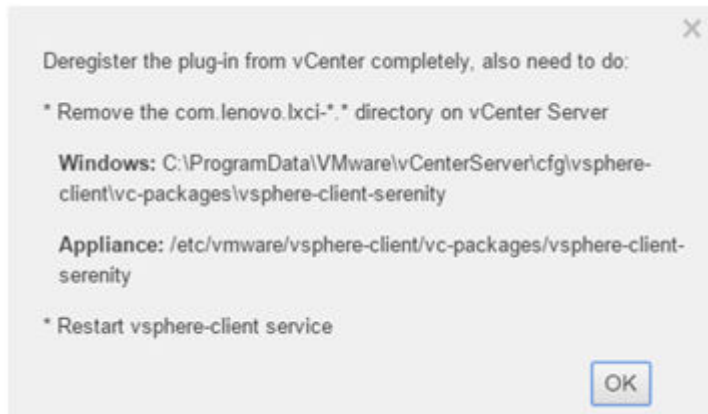
Eliminar el registro de Lenovo XClarity Integrator de un servidor vCenter

Los usuarios pueden cancelar el registro de Lenovo XClarity Integrator en el servidor vCenter.

Procedimiento

- Paso 1. Seleccione uno o más servidores vCenter y haga clic en **Deregister** (Cancelar registro). Aparecerá un cuadro de diálogo de confirmación.
- Paso 2. Haga clic en **Yes (Sí)** para confirmar que desea cancelar el registro de Lenovo XClarity Integrator.
- Paso 3. Haga clic en **Yes (Sí)** de nuevo para finalizar el proceso de cancelación de registro.

De completarse el proceso correctamente, aparecerá una ventana similar a la que se muestra en la figura siguiente.



- Paso 4. En el servidor vCenter, quite el directorio `com.lenovo.lxci-*. *`.
- Paso 5. Reinicie el servicio "vsphere-client".

Edición de las credenciales del servidor

Los usuarios pueden editar las credenciales del servidor.

Procedimiento

- Paso 1. Seleccione el servidor vCenter de destino y haga clic en **Edit Credential (Editar credencial)**.
- Paso 2. En la ventana "Edit selected credential (Editar credencial seleccionada)", introduzca el nombre de usuario y la contraseña y, a continuación, haga clic en **Save (Guardar)**.

Actualización del software de servidor de gestión

En esta página Configuración, los usuarios pueden descargar los paquetes de actualización más recientes desde el sitio web de LXCI y actualizar el software del servidor de gestión a la versión más reciente.

Procedimiento

- Paso 1. Haga clic en **Version and upgrade (Versión y actualización)** en el panel de navegación izquierdo. Aparece la página **Update Management Server (Actualizar servidor de gestión)**.
- Paso 2. En la página **Update Management Server (Actualizar servidor de gestión)**, haga clic en **Check for Updates (Buscar actualizaciones)** para comprobar nuevos paquetes de actualización aplicables al servidor LXCI actual.

Nota: Si la instancia de LXCI está conectada a Internet, comprobará automáticamente las actualizaciones y le notificará al usuario una vez a la semana.

- Paso 3. Seleccione el paquete necesario de la lista y haga clic en **Download (Descargar)**.
- Paso 4. Seleccione el paquete necesario de la lista y haga clic en **Perform Update (Realizar actualización)**.

Configuración del acceso de red

En esta página de valores, los usuarios pueden configurar el nombre de host, el nombre de dominio y los valores de DNS y de IP para las interfaces Eth0 y Eth1.

Antes de empezar

Cuando Lenovo XClarity Integrator se despliega inicialmente, la interfaz Eth0 está habilitado para conectar VMware vCenter y la red del controlador de gestión de placa base (BMC). Los usuarios pueden habilitar opcionalmente la interfaz Eth1 para la conexión de red de BMC. Después de habilitar la interfaz Eth1, la interfaz Eth0 deja de estar disponible para las conexiones de BMC.

No se recomienda cambiar los valores de red establecidos en el asistente. Si es necesario modificar los valores de red, siga estos pasos para reconfigurar el dispositivo virtual.

Atención: Los cambios incorrectos en los valores pueden provocar la desconexión del dispositivo virtual.

1. Vuelva a generar el certificado de servidor (consulte [“Trabajo con certificados de seguridad” en la página 64](#)).
2. Cancele el registro de vCenter y vuelva a registrarlo (consulte [“Configuración de conexiones de vCenter” en la página 53](#)).
3. Borre Lenovo XClarity Integrator del servidor vCenter (consulte [“Desinstalación de Lenovo XClarity Integrator para VMware vCenter” en la página 14](#)).
4. En los siguientes casos, deshabilite la gestión sobre todos los hosts que están gestionados por Lenovo XClarity Integrator y luego vuelva a gestionar los hosts.
 - Se cambió Eth0 y Eth1 está deshabilitado.
 - Hay cambios en Eth1.

Configuración del nombre de host, el nombre de dominio y DNS

Los usuarios pueden configurar el nombre de host, el nombre de dominio y DNS desde la página Valores de red.

Procedimiento

- Paso 1. Haga clic en **Network Settings (Valores de red)** en el panel de navegación izquierdo y, a continuación, haga clic en la pestaña **IP and DNS Settings (Valores de IP y DNS)** en el panel derecho.
- Paso 2. En el área **Host Name, Domain Name and DNS for virtual appliance (Nombre de host, nombre de dominio y DNS para dispositivo virtual)**, cambie el nombre de host, el DNS y el nombre de dominio.

Notas:

- El nombre de dominio es opcional. Para configurar el nombre de host y el nombre de dominio, se define un nombre de dominio completamente calificado (FQDN). En este caso, este FQDN se utiliza para el registro de vCenter y la generación de certificado del servidor. Asegúrese de que DNS esté especificado correctamente en vCenter.
- Para utilizar el nombre de host para conectarse a vCenter y a los hosts de ESXi gestionados por vCenter, configure un DNS para Lenovo XClarity Integrator para que Lenovo XClarity Integrator pueda acceder a vCenter y a los hosts de ESXi a través del nombre de host.

- Paso 3. Haga clic en **Save (Guardar)**.

Configuración de los valores IP de Eth0

Los usuarios pueden cambiar los valores de la dirección IP de Eth0 y de la puerta de enlace en la página Valores de red.

Acerca de esta tarea

Al cambiar los valores IP de la interfaz de Eth0, se perderá la conexión a la interfaz web de Lenovo XClarity Integrator. Revise la consola de máquina virtual para la nueva dirección IP Eth0 y vuelva a abrir la interfaz web de Lenovo XClarity Integrator para continuar la configuración.

Procedimiento

- Paso 1. Haga clic en **Network Settings (Valores de red)** en el panel de navegación izquierdo y, a continuación, haga clic en la pestaña **IP and DNS Settings (Valores de IP y DNS)** en el panel derecho.
- Paso 2. En el área **IP Settings (Valores IP)**, especifique la dirección IPv4, la dirección IPv6 o ambas para la interfaz Eth0.

Para IPv4, los usuarios pueden usar una dirección IP asignada de forma estática, obtener una dirección IP desde un servidor DHCP o deshabilitar IPv4.

Para IPv6, pueden asignar una dirección IPv6 a la interfaz utilizando uno de los siguientes métodos de asignación:

- Use una dirección IP asignada estáticamente
- Usar una configuración de dirección con estado (DHCPv6)
- Usar una configuración automática de dirección sin estado

- Paso 3. Especifique la puerta de enlace predeterminada.

Notas:

- Dado que Eth1 se utiliza intencionadamente para conectarse con la red de BMC, que generalmente se encuentra dentro de la subred Eth1, los usuarios pueden configurar la puerta de enlace predeterminada para Eth0 específicamente.
- Si especifican una puerta de enlace predeterminada, debe ser una dirección IP válida y debe utilizar la misma máscara de red (la misma subred) que la dirección IP de Eth0.
- Si Eth0 usa DHCP para obtener una dirección IP, la puerta de enlace predeterminada también debe utilizar DHCP y no se puede cambiar.

- Paso 4. Haga clic en **Save (Guardar)**.

Configuración de los valores IP de Eth1

Los usuarios pueden habilitar la interfaz Eth1 para la red del controlador de gestión de placa base (BMC) y cambiar los valores de la dirección IP de Eth1 y de la puerta de enlace en la página **Network Settings (Valores de red)**.

Acerca de esta tarea

De forma predeterminada, Eth0 y Eth1 están conectados a la misma red de VM con la etiqueta “red de VM”. Los usuarios pueden configurar Eth1 para que se conecte a otra red distinta siguiendo estos pasos:

1. Edite los valores de Lenovo XClarity Integrator
2. Seleccione **Network adapter 2 (Adaptador de red 2)** y seleccione la red de VM de destino.
3. Guarde los valores.

Procedimiento

- Paso 1. Haga clic en **Network Settings (Valores de red)** en el panel de navegación izquierdo y, a continuación, haga clic en la pestaña **IP and DNS Settings (Valores de IP y DNS)** en el panel derecho.
- Paso 2. En el área **IP Settings (Valores IP)**, seleccione **Enable Eth1 (Habilitar Eth1)** para habilitar Eth1. Se mostrarán los campos de configuración de IP.

Paso 3. Especifique la dirección IPv4, la dirección IPv6 o ambas para la interfaz Eth1.

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

Para IPv4, los usuarios pueden usar una dirección IP asignada de forma estática, obtener una dirección IP desde un servidor DHCP o deshabilitar IPv4.

Para IPv6, pueden asignar una dirección IPv6 a la interfaz utilizando uno de los siguientes métodos de asignación:

- Use una dirección IP asignada estáticamente
- Usar una configuración de dirección con estado (DHCPv6)
- Usar una configuración automática de dirección sin estado

Paso 4. Haga clic en **Save** (Guardar).

Configuración de proxy

Los usuarios pueden establecer el proxy de LXCI para conectarse a Internet en la página **Advanced Routing (Valores de red)**.

Nota: Solo se admite el protocolo HTTP.

Procedimiento

Paso 1. Haga clic en **Network Settings (Valores de red)** en el panel de navegación izquierdo y, a continuación, haga clic en la pestaña **Internet Settings (Configuración de Internet)** en el panel derecho.

Paso 2. En el área **Proxy settings (Configuración de proxy)**, seleccione **Use HTTP proxy (Usar proxy HTTP)** e introduzca el proxy, el puerto, el nombre de usuario y la contraseña.

Notas:

- El proxy debe ser una dirección IPv4/IPv6 o un FQDN.
- El puerto proxy debe ser un entero entre 0 y 65535.

Paso 3. Haga clic en **Save (Guardar)**.

Configuración del enrutamiento avanzado

Los usuarios pueden agregar, editar y quitar la ruta en la página **Network Settings (Valores de red)**.

Procedimiento

Paso 1. Haga clic en **Network Settings (Valores de red)** en el panel de navegación izquierdo y, a continuación, haga clic en la pestaña **Advanced Routing (Enrutamiento avanzado)** en el panel derecho.

Paso 2. Realice una de las acciones siguientes:

- Para añadir la ruta:

1. Haga clic en **Add (Añadir)**. Se muestra la ventana Valores de ruta avanzados.
2. En la ventana Valores de ruta avanzados, seleccione la interfaz y el tipo de ruta en la lista desplegable e introduzca el destino, la máscara de red y la puerta de enlace.
3. Haga clic en **Save (Guardar)**.

- Para editar la ruta:

1. Seleccione la ruta de destino y haga clic en **Edit (Editar)**. Se muestra la ventana Valores de ruta avanzados.

2. En la ventana Valores de ruta avanzados, seleccione la interfaz y el tipo de ruta en la lista desplegable y edite el destino, la máscara de red y la puerta de enlace.
 3. Haga clic en **Save (Guardar)**.
- Para quitar la ruta, seleccione la ruta de destino y haga clic en **Remove (Quitar)**.

Prueba de la conexión de red

Los usuarios pueden probar la conexión de red en la página **Network Settings (Valores de red)**.

Procedimiento

- Paso 1. Haga clic en **Network Settings (Valores de red)** en el panel de navegación izquierdo y, a continuación, haga clic en la pestaña **Test Connection (Probar conexión)** en el panel derecho.
- Paso 2. Seleccione el método para probar la conexión en la lista desplegable e introduzca el nombre de host, el número de puerto, el recuento, los sondeos y el tiempo de espera.
- Paso 3. Haga clic en **Test Connection (Probar conexión)**. El resultado de la prueba se mostrará en el área de **Result (Resultado)**.

Establecimiento de la fecha y la hora

Los usuarios pueden cambiar la fecha y hora desde la página **Date And Time (Fecha y hora)**.

Procedimiento

- Paso 1. Haga clic en **Date And Time (Fecha y hora)** en el panel de navegación izquierdo.
- Paso 2. Especifique la región y zona horaria.
- Paso 3. Especifique la fecha y hora. Los usuarios pueden establecer la fecha u hora manualmente o permitir que Lenovo XClarity Integrator se sincronice con un servidor NTP.

Notas:

- Lenovo XClarity Integrator solo admite NTP versión 4.
- Utilice la coma (,) para separar si se agregan varias direcciones de servidor NTP.

- Paso 4. Haga clic en **Save (Guardar)**.

Gestión de la capacidad del disco

Los usuarios pueden administrar la capacidad del disco desde la página **System Monitor (Supervisión del sistema)**.

Procedimiento

- Paso 1. Haga clic en **System Monitor (Supervisión del sistema)** en el panel de navegación izquierdo.
- Paso 2. Lleve a cabo uno o más de los procedimientos siguientes:
 - Vea el uso del disco de cada elemento en la página Disk Usage (Uso del disco) en el panel derecho.
 - Para limpiar el repositorio de vLCM, haga clic en **Clean Up (Limpiar)** y siga los pasos que aparecen en la ventana **Notice (Aviso)** para quitar el repositorio.
 - Para limpiar el repositorio de actualización de firmware, haga clic en **Clean Up (Limpiar) → Yes (Si)**.

Recopilación de datos de servicio

Los usuarios pueden recopilar los registros de Lenovo XClarity Integrator y enviarlos al servicio de Lenovo para obtener soporte.

Procedimiento

- Paso 1. Haga clic en **Service Data (Datos de servicio)** en el panel de navegación izquierdo.
- Paso 2. (Opcional) Habilite **Send LXCI audit logs to vCenter (Enviar registros de auditoría de LXCI a vCenter)**.
- Paso 3. En la página **Collect Log (Recopilar registro)**, seleccione el nivel de registro de la lista desplegable.

Nota: Si es necesario, los usuarios pueden seleccionar **Debug (Depurar)**. Asegúrese de restaurar el nivel del registro a Información después de resolver el problema.

- Paso 4. Haga clic en **Collect log** (Recopilar registro). Aparece la página **Download Log** (Descargar registro).
- Paso 5. Haga clic en el vínculo **Download Log** (Descargar registro) para descargar el registro.

Gestión de autenticación y autorización

Lenovo XClarity Integrator para VMware vCenter proporciona mecanismos de seguridad para verificar las credenciales de los usuarios y controlar el acceso a los recursos y las tareas.

Configuración de un servidor de autenticación LDAP externo

Los usuarios pueden usar un servidor de autenticación LDAP externo en lugar del servidor de autenticación de LXCI para VMware vCenter local en el nodo de gestión.

Antes de empezar

- Es preciso llevar a cabo la configuración inicial de LXCI para VMware vCenter antes de configurar el servidor de autenticación externo.
- Se admiten los siguientes servidores de autenticación externos:
 - Microsoft Active Directory. Debe residir en un Microsoft Windows Server externo capaz de comunicarse con el dispositivo LXCI para VMware vCenter.
- LXCI para VMware vCenter realiza un control de conectividad cada 10 minutos para mantener la conectividad en los servidores LDAP externos. Los entornos con muchos servidores LDAP podrían experimentar un alto uso de la CPU durante esta comprobación de conectividad. Para lograr el mejor rendimiento, especifique solo los servidores LDAP conocidos y accesibles al configurar el cliente LDAP.
- Asegúrese de que los usuarios de LDAP que pueden iniciar sesión en esta interfaz web de XClarity Integrator sean miembros del grupo LDAP en el servidor LDAP.

Cree el grupo y agregue los usuarios al servidor LDAP antes de configurar este cliente LDAP:

1. Desde el servidor de autenticación externo, cree una cuenta de usuario. Para obtener instrucciones, consulte la documentación del servidor LDAP.
2. Cree un grupo en el servidor LDAP. El nombre de grupo LDAP puede ser el nombre predeterminado **LXCI-SUPERVISOR** u otros nombres definidos por el usuario. El grupo debe existir en el contexto del nombre distinguido raíz definido en el cliente LDAP.
3. Añada el usuario como miembro del grupo creado anteriormente.

Procedimiento

Para configurar LXCI para VMware vCenter para que use un servidor de autenticación externo, lleve a cabo los pasos siguientes.

- Paso 1. Configure el método de autenticación de usuarios para Microsoft Active Directory siguiendo uno de estos procedimientos:
 - Para usar una autenticación no segura, no se requiere ninguna configuración adicional. Los controladores de dominio de Windows Active Directory usan la autenticación LDAP no segura de forma predeterminada.
 - Para utilizar la autenticación LDAP segura:

1. Configure los controladores de dominio para permitir la autenticación LDAP segura. Para obtener más información sobre la configuración de la autenticación LDAP segura en Active Directory, consulte <https://social.technet.microsoft.com/wiki/contents/articles/2980.ldap-over-ssl-ldaps-certificate.aspx>.
2. Compruebe que los controladores de dominio de Active Directory están configurados para usar la autenticación LDAP segura:
 - Busque el suceso LDAP sobre Secure Sockets layer (SSL) ya está disponible en la ventana Visor de sucesos de los controladores del dominio.
 - Use la herramienta ldp.exe de Windows para comprobar que la conexión LDAP con los controladores de dominio sea segura.
3. Importe el certificado del servidor LDAP, los certificados intermedios (si los hay) y el certificado raíz de la entidad de certificación que firma el certificado de servidor.
 - a. En el panel de navegación izquierdo del menú LXCI para VMware vCenter, haga clic en **Security Settings (Valores de seguridad)**.
 - b. Haga clic en **Trusted Certificates (Certificados de confianza)** en la sección Gestión de certificados.
 - c. Haga clic en **Add (Añadir)**.
 - d. En la ventana Añadir, haga clic en **Choose File (Seleccionar archivo)** para cargar el certificado de destino.
 - e. Haga clic en **Upload Certificate (Cargar certificado)**.

Paso 2. Configure el cliente LDAP de LXCI para VMware vCenter:

- a. En el panel de navegación izquierdo del menú LXCI para VMware vCenter, haga clic en **Security Settings (Valores de seguridad) → LDAP Client (Cliente LDAP)**.
 - b. Elija uno de los siguientes métodos de autenticación de usuario:
 - **Allow logons from local users (Permitir inicios de sesión de usuarios locales)**. La autenticación se realiza mediante la autenticación local. Cuando se selecciona esta opción, los usuarios solo pueden iniciar sesión en LXCI con la cuenta local.
 - **Allow LDAP users first, then local users (Permitir usuarios de LDAP primero, luego usuarios locales)**. Un servidor LDAP externo realiza la autenticación primero. Si falla, el servidor de autenticación local realiza la autenticación.
- Si se selecciona este método, haga lo siguiente:
1. Introduzca una o varias direcciones de servidor y puertos.
 2. Ingrese el nombre del grupo LDAP.

Notas:

- De manera predeterminada, el nombre del grupo LDAP es **LXCI-SUPERVISOR**. Los usuarios también pueden introducir otros nombres.
 - Seleccione **Use nested group search (Usar la búsqueda de grupos anidados) → OK (Aceptar)**, LXCI puede buscar el grupo y su grupo primario para el usuario objetivo. Esta característica solo se aplica a Active Directory.
3. Elija uno de los siguientes métodos de vinculación:
 - **Configured Credentials (Credenciales configuradas)**. Use este método de vinculación para utilizar el nombre y la contraseña de cliente que se deberán utilizar para vincular LXCI para VMware vCenter con el servidor de autenticación externo. Si la vinculación falla, también fallará el proceso de autenticación

El nombre de cliente puede ser cualquier nombre que el servidor LDAP admita, incluido un nombre distinguido, sAMAccountName, nombre de NetBIOS o UserPrincipalName. El nombre de usuario de cliente debe ser una cuenta de usuario con el dominio que tenga al menos privilegios de solo lectura. Por ejemplo:

```
cn=administrator,cn=users,dc=example,dc=com
example\administrator
administrator@example.com
```


Atención: Para cambiar la contraseña del cliente en el servidor de autenticación externo, asegúrese de actualizar también la nueva contraseña en LXCI para VMware vCenter. Si se cambia la contraseña del cliente en el servidor LDAP externo, los usuarios pueden iniciar sesión en Integrator mediante una cuenta local para actualizar la nueva contraseña.

- **Login Credentials (Credenciales de inicio de sesión).** Use este método de vinculación para utilizar el nombre de usuario y la contraseña de LDAP para vincular LXCI para VMware vCenter con el servidor de autenticación externo.

El ID usuario y la contraseña que especifica se usan solo para probar la conexión con el servidor de autenticación. Si es correcta, los valores del cliente LDAP se guardarán, pero la credencial de inicio de sesión de prueba especificada no se guardará. Todas las vinculaciones futuras utilizarán el nombre de usuario y la contraseña que haya usado para iniciar sesión en LXCI para VMware vCenter.

Notas:

- Los usuarios deben iniciar sesión en LXCI para VMware vCenter utilizando un ID de usuario completamente calificado (por ejemplo, administrator@domain.com o DOMAIN\admin).
 - Los usuarios deben utilizar un nombre de cliente de prueba completamente calificado para el método de vinculación.
4. En el campo **Root DN (DN raíz)**, especifique la entrada de nivel superior en el árbol del directorio LDAP. En este caso, las búsquedas se inician utilizando el nombre distinguido raíz especificado como la base de búsqueda.
 5. En el campo **User Search Attribute (Atributo de búsqueda de usuarios)**, especifique el atributo que debe usarse para buscar el nombre de usuario.

Cuando el método de vinculación está configurado como **Configured Credentials (Credenciales configuradas)**, una solicitud de búsqueda sigue la vinculación inicial al servidor LDAP al recuperar la información específica acerca del usuario, incluyendo el DN de usuario y la membresía de grupo. Esta solicitud de búsqueda debe especificar el nombre del atributo que representa los ID de usuario en ese servidor. Este nombre del atributo se configura en este campo.

6. En el campo **Group Search Attribute (Atributo de búsqueda de grupos)**, especifique el nombre del atributo que se utilizará para identificar los grupos a los que un usuario pertenece.
7. En el campo **Group Name Attribute (Atributo de nombre de grupo)**, especifique el nombre del atributo que se utilizará para identificar el nombre de grupo que está configurado por el servidor LDAP.

- c. Haga clic en **Save (Guardar)**.

LXCI para VMware vCenter intenta probar la configuración para detectar errores comunes. Si la prueba falla, se muestran mensajes de error que indican el origen de los errores. Para el método de vinculación **Configured Credentials (Credenciales configuradas)**, si la prueba se realiza correctamente y las conexiones a los servidores especificados finalizan correctamente, la autenticación del usuario podría seguir fallando si:

- Hay una configuración errónea o cambios en el servidor LDAP, los usuarios pueden iniciar sesión utilizando la cuenta local. Se recomienda conservar un registro de la cuenta y contraseña local.
- El nombre distinguido raíz no es correcto.
- El usuario no es miembro del grupo LDAP en el servidor LDAP.

- d. Haga clic en **OK (Aceptar)**.

Resultados

LXCI para VMware vCenter valida la conexión al servidor LDAP. Si la validación se realiza correctamente, la autenticación del usuario en el servidor de autenticación externo se lleva a cabo al iniciar sesión en LXCI para VMware vCenter.

Si la validación falla, el modo de autenticación se revierte automáticamente a la opción **Allow logons from local users (Permitir inicios de sesión de usuarios locales)** y se muestra un mensaje en el que se explica la causa del error.

Nota: Se deben configurar los grupos de roles correctos en LXCI para VMware vCenter y las cuentas de usuarios deben estar definidas como miembros del grupo LDAP en el servidor LDAP. De lo contrario, la autenticación de usuario fallará.

Trabajo con certificados de seguridad

Lenovo XClarity Integrator y su software asociado (Lenovo XClarity Administrator y VMware vCenter) utilizan los certificados SSL para establecer conexiones seguras entre sí. De forma predeterminada, Lenovo XClarity Integrator utiliza certificados generados por Lenovo XClarity Integrator que están autofirmados y que fueron emitidos por una entidad de certificación (CA) interna.

Generación de un certificado de servidor firmado externamente y personalizado

Al instalar un certificado de servidor personalizado en Lenovo XClarity Integrator, los usuarios deben indicar el conjunto de certificados que contiene toda la cadena de firma de la CA.

Acerca de esta tarea

Si el nuevo certificado de servidor no lo ha firmado un tercero de confianza internacional (como VeriSign), la próxima vez que se conecte a Lenovo XClarity Integrator, se mostrará un mensaje de seguridad que pedirá a los usuarios que acepten el nuevo certificado en el navegador como una excepción. Para evitar los mensajes de seguridad, los usuarios pueden importar una cadena de firma de CA del certificado de servidor en la lista de certificados de confianza del navegador web.

Para obtener más información sobre cómo importar certificados, consulte [“Importación del certificado de Lenovo XClarity Integrator al navegador web” en la página 19.](#)

Procedimiento

Lleve a cabo los pasos siguientes para generar un certificado de servidor personalizado.

Paso 1. Genere una solicitud de firma de certificado (CSR) para Lenovo XClarity Integrator.

- a. En el panel de navegación izquierda, haga clic en **Security Settings** (Valores de seguridad).
- b. Haga clic en **Server certificate** (Certificado de servidor) para mostrar la página **Server Certificate** (Certificado de servidor).
- c. Haga clic en la pestaña **Generate Certificate Signing Request (CSR)** (Generar solicitud de firma de certificado (CSR)).
- d. Rellene los campos de la página Generar solicitud de firma de certificado (CSR):
 - País
 - Estado o provincia
 - Ciudad o localidad
 - Organización
 - Unidad organizativa (opcional)
 - Nombre común
 - Nombres alternativos

Atención: Seleccione un nombre común que coincida con la dirección IP o el nombre de host del dispositivo virtual Lenovo XClarity Integrator. Si no selecciona el valor correcto, se podrían producir conexiones no fiables. Los usuarios pueden permitir que Lenovo XClarity Integrator genere el nombre común automáticamente al especificar “Generado por LXCI”.

Nota: Para crear una CSR que se va a firmar con una CA que admita el Certificado de nombre alternativo del sujeto, los usuarios pueden añadir nombres alternativos. Haga clic **+** en el campo **Alternative Names** (Nombres alternativos). En la ventana Add Alternative Names (Añadir nombres alternativos), haga clic en **+** después de la dirección predeterminada para añadir la dirección IP/DNS y haga clic en **Submit** (Enviar).

e. Haga clic en **Generate CSR File** (Generar archivo CSR) para descargar el archivo generado.

Paso 2. Envíe todas las CSR a su CA de confianza para que las firmen. La CA de confianza devuelve un conjunto de certificados para cada CSR. El conjunto de certificados contiene el certificado firmado y la cadena de confianza completa de la entidad de certificación (CA).

Paso 3. Cargue el certificado de servidor firmado externamente en Lenovo XClarity Integrator.

Nota: El certificado que se está cargando se debe haber creado a partir de la solicitud de firma de certificado creada más recientemente con el botón **Generate CSR File** (Generar archivo CSR). El archivo cargado debe contener la cadena de certificado completa, incluido el certificado raíz y todos los certificados intermedios. El orden de los certificados en el archivo deben ser certificado del servidor, certificados intermedios y después certificado raíz.

1. En el panel de navegación izquierda, haga clic en **Security Settings** (Valores de seguridad).
2. Haga clic en **Server Certificate** (Certificado de servidor) en la página de valores.
3. Haga clic en la pestaña **Upload Certificate** (Cargar certificado).
4. Haga clic en el botón **Choose File** (Elegir archivo) para cargar el archivo de certificado (.der, .pem o .cer).
5. Haga clic en el botón **Upload Certificate** (Cargar certificado). Se carga el archivo del certificado.

Una vez cargado el certificado de servidor, se reinicia Lenovo XClarity Integrator y finaliza la conexión del navegador a la interfaz web de Lenovo XClarity Integrator. Para continuar con la tarea, vuelva a iniciar sesión en la interfaz web de Lenovo XClarity Integrator.

Nota: Se cargará el registro de VMware vCenter después de cargar el nuevo certificado de servidor.

Restauración del certificado de servidor generado por Lenovo XClarity Integrator

Los usuarios pueden generar un nuevo certificado de servidor para reinstalar un certificado generado por Lenovo XClarity Integrator en el caso de que Lenovo XClarity Integrator esté utilizando un certificado de servidor personalizado. El certificado del servidor personalizado luego se sustituye y el nuevo certificado de servidor autofirmado se utiliza en Lenovo XClarity Integrator.

Procedimiento

Siga estos pasos para generar un nuevo certificado de servidor y firmarlo con el certificado raíz de la CA recién generado:

Paso 1. En el panel de navegación izquierda, haga clic en **Security Settings** (Valores de seguridad).

Paso 2. Haga clic en **Server Certificate** (Certificado de servidor) en la página de valores.

Paso 3. Haga clic en la pestaña **Regenerate Server Certificate** (Volver a generar certificado de servidor).

Paso 4. Rellene los campos de la página **Regenerate Server Certificate** (Volver a generar certificado de servidor):

- País
- Estado o provincia
- Ciudad o localidad
- Organización
- Unidad de organización
- Nombre común

Nota: Seleccione un nombre común que coincida con la dirección IP o el nombre de host del dispositivo virtual Lenovo XClarity Integrator. Si no selecciona el valor correcto, se podrían producir conexiones no fiables. Los usuarios pueden permitir que Lenovo XClarity Integrator genere el nombre común automáticamente al especificar “Generado por LXCI”.

Paso 5. Haga clic en **Regenerate Certificate** (Volver a generar certificado)

Cuando se vuelve a generar un nuevo certificado de servidor, Lenovo XClarity Integrator se reinicia y la conexión del navegador web con la interfaz web de Lenovo XClarity Integrator finaliza. Para continuar con el trabajo, vuelva a iniciar sesión en la interfaz web de Lenovo XClarity Integrator.

Nota: Se cargará VMWare vCenter después de volver a generar el certificado de servidor.

Regeneración del certificado raíz de la Entidad de certificación (CA)

Los usuarios pueden volver a generar el certificado raíz de la entidad de certificación (CA).

Procedimiento

Paso 1. En el panel de navegación izquierda, haga clic en **Security Settings** (Valores de seguridad).

Paso 2. Haga clic en **Certificate Authority** (Entidad de certificación) en la página de valores.

Paso 3. Haga clic en **Regenerate Certificate Authority Root Certificate** (Volver a generar certificado raíz de entidad de certificación).

Notas:

1. Después de volver a generar el certificado raíz de la CA, deberán volver a generar el certificado de servidor. Consulte [“Restauración del certificado de servidor generado por Lenovo XClarity Integrator” en la página 65.](#)
2. Después de volver a generar el certificado raíz de la CA, deben volver a establecer los valores de confianza de la CA en todos los equipos cliente. Consulte [“Importación del certificado de Lenovo XClarity Integrator al navegador web” en la página 19.](#)

Descarga e instalación de un certificado raíz de la entidad de certificación (CA)

Los usuarios pueden descargar e instalar el certificado raíz de la entidad de certificación (CA).

Procedimiento

Paso 1. En el panel de navegación izquierda, haga clic en **Security Settings** (Valores de seguridad).

Paso 2. Haga clic en **Certificate Authority** (Entidad de certificación) en la página de valores.

Paso 3. Pulse **Download Certificate Authority Root Certificate** (Descargar certificado raíz de entidad de certificación).

Paso 4. Haga doble clic en el archivo ca.der.

Paso 5. Haga clic en la pestaña **General** y en **Install Certificate** (Instalar certificado).

Paso 6. Haga clic en **Next** (Siguiente).

- Paso 7. En la página Certificate Store (Almacén de certificados), seleccione **Place all certificates in the following store** (Colocar todos los certificados en el siguiente almacén) y, a continuación, haga clic en **Browse** (Examinar).
- Paso 8. Seleccione **Trusted Root Certificate Authorities** (Entidades de certificación raíz de confianza) y, a continuación, haga clic en **OK** (Aceptar).
- Paso 9. Haga clic en **Finish** (Finalizar).

Nota: Si el navegador es Firefox, se mostrará un diálogo en el paso 3. Este cuadro de diálogo pregunta si confía en el certificado. Marque **Trust this CA to identify websites** (Confiar en este CA para identificar sitios web), haga clic en **OK** (Aceptar) y omita los pasos 4 al 9.

Descarga del certificado de servidor

Los usuarios pueden descargar el certificado de servidor.

Procedimiento

- Paso 1. En el panel de navegación izquierda, haga clic en **Security Settings** (Valores de seguridad).
- Paso 2. Haga clic en **Server Certificate** (Certificado de servidor) en la página de valores.
- Paso 3. Haga clic en la pestaña **Download Certificate** (Descargar certificado).
- Paso 4. Haga clic en **Download Certificate** (Descargar certificado).

Gestión de certificados de confianza

Los usuarios pueden agregar, descargar o quitar los certificados de confianza.

Procedimiento

- Paso 1. En el panel de navegación izquierda, haga clic en **Security Settings** (Valores de seguridad).
- Paso 2. Haga clic en **Trusted Certificates (Certificados de confianza)** en la página de valores.
- Paso 3. Realice una de las acciones siguientes:
- Para agregar un certificado de confianza:
 1. Haga clic en **Add (Añadir)**.
 2. En la ventana Añadir, haga clic en **Choose File (Seleccionar archivo)** para cargar el certificado de destino.
 3. Haga clic en **Upload Certificate (Cargar certificado)**.
 - Para descargar un certificado de confianza:
 1. Seleccione el certificado de destino.
 2. Haga clic en **Save (Guardar)**. El certificado se guardará de forma local.
 - Para quitar un certificado de confianza:
 1. Seleccione el certificado de destino.
 2. Haga clic en **Remove** (Quitar). Se mostrará un cuadro de diálogo emergente para que los usuarios confirmen si desean quitar el certificado.
 3. Haga clic en **Yes** (Sí).

Apagado o reinicio de Lenovo XClarity Integrator

Los usuarios pueden apagar o reiniciar Lenovo XClarity Integrator. Sin embargo, Lenovo XClarity Integrator se desconecta después de que se apague o reinicie, por lo que se debe volver a conectar después de este proceso.

Antes de empezar

Asegúrese de que no se esté ejecutando ninguna tarea. Se pueden cancelar todos los trabajos en ejecución durante el apagado o reinicio de Lenovo XClarity Integrator.

Procedimiento

Lleve a cabo los siguientes pasos para apagar o reiniciar Lenovo XClarity Integrator Administration.

- Paso 1. En la página **Lenovo XClarity Integrator for VMware vCenter**, haga clic en **Power Control** (Control de alimentación) en la esquina superior derecha. Se mostrará un cuadro de diálogo de confirmación con una lista de los trabajos que están en ejecución.
- Paso 2. Pulse **Shut down** (Apagar) o **Restart** (Reiniciar). Lenovo XClarity Integrator se apagará o reiniciará y todos los trabajos en ejecución se cancelarán.

Apéndice A. Sucesos de gestión proactiva de hardware compatibles

LE-FQXSPSD0002G : Falla prevista en [StorageVolumeElementName] para la matriz [ComputerSystemElementName].

Falla prevista en [StorageVolumeElementName] para la matriz [ComputerSystemElementName].

Este mensaje se utiliza cuando una implementación ha detectado que se ha previsto una falla de la matriz.

Internal Event

No

Gravedad

Advertencia

Categoría de las alertas

Sistema - Falla prevista

Acción del usuario

Lleve a cabo los siguientes pasos hasta que se solucione el problema:

1. Compruebe si hay algún error de unidad.
2. De ser así, sustituya la unidad con error.
3. Si el problema persiste, recopile el registro de datos del servicio desde WebGUI de XCC y póngase en contacto con el Soporte técnico de Lenovo.

Reviewed

LE-FQXSPSD0003G : Se pronostica un error en la unidad [arg1] en el alojamiento/chasis (MTM-SN: [arg2]).

Se pronostica un error en la unidad [arg1] en el alojamiento/chasis (MTM-SN: [arg2]).

Este mensaje se utiliza cuando una implementación ha detectado que se ha previsto una falla de la matriz.

Internal Event

No

Gravedad

Advertencia

Categoría de las alertas

Sistema - Falla prevista

Acción del usuario

Lleve a cabo los siguientes pasos hasta que se solucione el problema:

1. Compruebe si hay algún error de unidad.
2. De ser así, sustituya la unidad con error.
3. Si el problema persiste, recopile el registro de datos del servicio desde WebGUI de XCC y póngase en contacto con el Soporte técnico de Lenovo.

Reviewed

Apéndice B. Resolución de problemas

Utilice esta sección para solucionar y resolver problemas con Lenovo XClarity Integrator para VMware vCenter.

Los servidores no se pueden administrar automáticamente cuando se agrega LXCA a LXCI

Si los usuarios seleccionan **Create a new account by connecting with this administrative account** (Cree una nueva cuenta conectándose con esta cuenta de administrador) al agregar LXCA a LXCI, los grupos de roles predeterminados asignados a la nueva cuenta deben ser **lxc-operator**, **lxc-fw-admin**, **lxc-hw-admin** y **lxc-os-admin**. Sin embargo, el grupo de roles predeterminado de servidores es **lxc-supervisor** cuando el **Resource Access Control (Control de acceso a recursos)** está habilitado.

Procedimiento

Realice los siguientes pasos para solucionar el problema:

- Paso 1. Inicie sesión en la página web de LXCA.
- Paso 2. Haga clic en **Administration (Administración) → Security (Seguridad) → Access Control (Control de acceso) → Resource View (Vista de recursos)**.
- Paso 3. Realice una de las acciones siguientes:
 - Deshabilite **Resource Access Control** (Control de acceso a recursos).
 - Añada uno o más grupos a los servidores: **lxc-operator**, **lxc-fw-admin**, **lxc-hw-admin** y **lxc-os-admin**.

Aparece el mensaje “No healthy upstream” (No hay flujo ascendente en buen estado) en la página de LXCI en vCenter

En vCenter 8.0u3 y versiones posteriores, es posible que aparezca **No healthy upstream** (No hay flujo ascendente en buen estado) en la página de LXCI. Esto puede deberse a que el certificado LXCI ha caducado. En este caso, LXCI no se puede conectar mediante vCenter, y los usuarios deben volver a generar o cargar el nuevo certificado en LXCI y volver a registrar LXCI en vCenter.

Procedimiento

Realice los siguientes pasos para solucionar el problema:

- Paso 1. Inicie sesión en la página de administración de LXCI:
`https://<LXCI IP>/admin`
- Paso 2. Haga clic en **Security Settings (Valores de seguridad) → Server Certificate (Certificado de servidor) → Download Certificate (Descargar certificado) → Download (Descargar)**.
- Paso 3. Abra el certificado descargado y compruebe si ha caducado.
- Paso 4. Si el certificado ha caducado, vuelva a generar uno o cargue uno nuevo.
- Paso 5. Anule el registro de LXCI con vCenter y vuelva a registrarlo en vCenter.

No se muestra la lista de firmware ni de complementos de controladores

Al crear una imagen para un clúster utilizando vSphere Lifecycle Manager, si **Lenovo XClarity Integrator** está seleccionado como gestor de compatibilidad de hardware y el proxy está habilitado en vCenter pero no está configurado para permitir la conexión desde vCenter a LXCI (protocolo HTTPS, puerto 443), puede que no se muestre la lista de firmware ni de complementos de controladores.

Procedimiento

Realice los siguientes pasos para solucionar el problema:

Paso 1. Reproduzca el problema.

Paso 2. Inicie sesión en la consola de shell de vCenter.

Paso 3. En el shell, ejecute el siguiente comando:

```
vi /storage/log/vmware/vmware-updatemgr/vum-server/hsm-service.log
```

Paso 4. Si aparece el siguiente mensaje de error u otro similar, significa que el proxy prohíbe la solicitud HTTPS de vCenter a XClarity Integrator. Los usuarios deben deshabilitar el proxy o permitir la conexión desde vCenter a Lenovo XClarity Integrator (protocolo HTTPS, puerto 443) en la configuración del proxy.

```
HTTPSConnectionPool(host='<XClarity Integrator IP or FQDN', port=443): Max retries exceeded with url: /hsm/vsphere-lcm/hw-support/v1/packages (Caused by ProxyError('Cannot connect to proxy.', OSError('XXX failed or timeout: '))).
```

Error en la función Exploración de BMC

Si la lista de detección de BMC no se muestra correctamente, significa que se ha producido un error en el proceso de detección de BMC.

Acerca de esta tarea

Si la lista de detección no se muestra después de pulsar en **Discovery** (Detección), realice los siguientes pasos:

Procedimiento

Paso 1. Asegúrese de que la conexión de red entre vCenter y el host esté funcionando.

Paso 2. Vuelva a intentar ejecutar el proceso de detección haciendo clic en **Discovery** (Detección).

No se muestra la página de mapa de chasis, actualización de firmware o patrón de configuración

Es posible que no se muestre la página de mapa de chasis, actualización de firmware o patrón de configuración.

Procedimiento

Realice los siguientes pasos para solucionar el problema:

Paso 1. Asegúrese de haber instalado el certificado de Lenovo XClarity Integrator siguiendo las instrucciones indicadas en [“Importación del certificado de Lenovo XClarity Integrator al navegador web” en la página 19](#).

Paso 2. Si se ha utilizado el FQDN de vCenter al registrar Lenovo XClarity Integrator en el cliente de vCenter, utilice el FQDN de vCenter para abrir el cliente de vSphere.

Lenovo XClarity Integrator no se muestra en el cliente de vSphere después de la instalación

Después de instalar Lenovo XClarity Integrator y registrarlo en vCenter correctamente, Cliente vSphere puede presentar un error para descargar e implementar el complemento Lenovo XClarity Integrator. En este caso, Lenovo XClarity Integrator no se mostrará en el Cliente vSphere.

Procedimiento

Compruebe el archivo `vsphere_client_virgo.log` para ver si hay el siguiente mensaje de error:
Error downloading https://[*****LXCI IP*****]:443/IVPUI.zip. Make sure that the URL is reachable;
then logout/login to force another download. java.net.ConnectionException: Network is unreachable.

Nota: El archivo de registro se encuentra en el directorio `C:\ProgramData\VMware\vCenterServer\logs\vsphere-client\logs` o `/storage/log/vmware/vsphere-client/logs`, dependiendo de la versión de vCenter.

Si el mensaje de error está presente en el archivo de registro, siga uno de los siguientes pasos:

- Para Windows vCenter, abra el navegador web en VMware vCenter Server y acceda a la URL que aparece en el mensaje de error (por ejemplo, `https://[*****LXCI IP*****]:443/IVPUI.zip`). Si esto no funciona, verifique que el servidor Lenovo XClarity Integrator se esté ejecutando.
- Para un dispositivo virtual vCenter ejecute el comando `curl <URL>` en VMware vCenter Server, donde `<URL>` es la URL que aparece en el mensaje de error (por ejemplo, `https://[*****LXCI IP*****]:443/IVPUI.zip`).

Si aparecen mensajes de error semejantes a “SSL certificate problem, verify that the CA cert is OK” (Problema de certificado SSL, verifique que el certificado CA esté correcto) o “Certificate verify failed” (Error al verificar el certificado), importe el certificado de Lenovo XClarity Integrator al dispositivo VMware vCenter Server al realizar los siguientes pasos:

1. Abra la página web de gestión del dispositivo Lenovo XClarity Integrator y luego inicie sesión en la página web.
2. Haga clic en **Security Settings (Valores de seguridad)** en el panel izquierdo y luego haga clic en **Certificate Authority (Entidad de certificación)**.
3. Pulse **Download Certificate Authority Root Certificate** (Descargar certificado raíz de entidad de certificación).
4. Importe el certificado de Lenovo XClarity Integrator en VMware vCenter Server como un Certificado raíz de confianza.

Los datos que se muestran en Lenovo XClarity Integrator no están actualizados cuando Lenovo XClarity Integrator se abre en Internet Explorer 11 o versiones posteriores

El mecanismo de memoria caché de Internet Explorer puede afectar el uso de Lenovo XClarity Integrator. Los usuarios deben configurar las opciones de Internet cada vez que utilizan Internet Explorer 11 o versiones posteriores para visitar la página web de Lenovo XClarity Integrator.

Procedimiento

- Paso 1. Abra el navegador Internet Explorer y haga clic en **Tools (Herramientas) → Internet options (Opciones de Internet)**. Se muestra la ventana Internet Options (Opciones de Internet).
- Paso 2. Haga clic en la pestaña **General** y en **Settings (Valores)**. Se muestra la ventana Website Data Settings (Valores de datos del sitio web).
- Paso 3. Seleccione **Every time I visit the webpage** (Cada vez que visito el sitio web) y haga clic en **OK** (Aceptar).

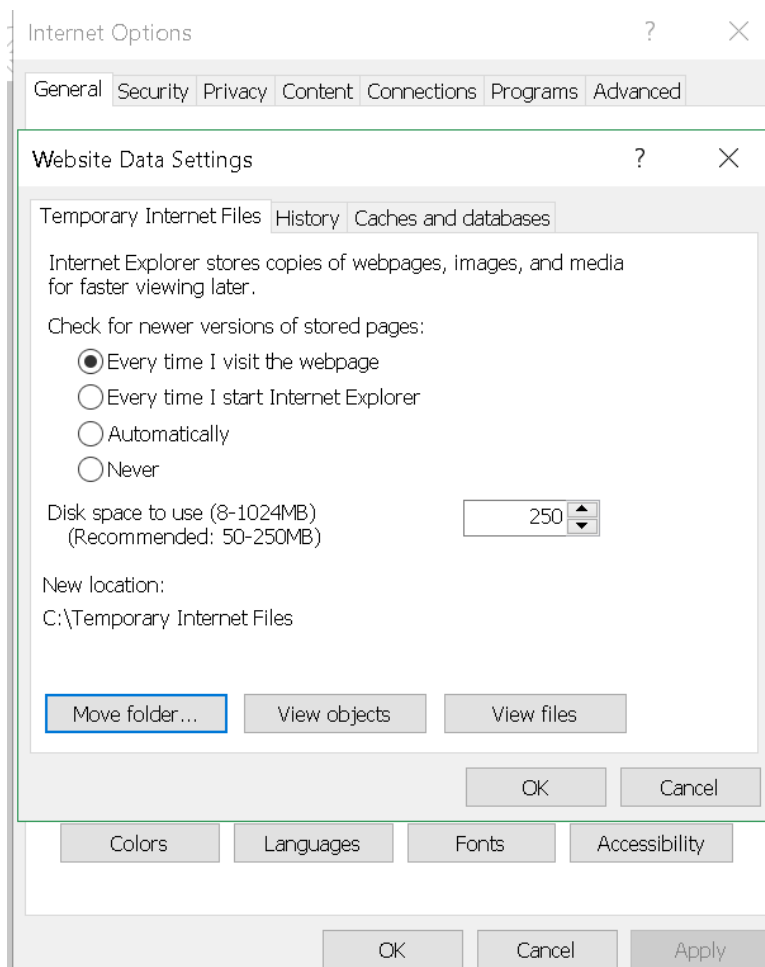


Figura 13. Valores de Internet Explorer

Paso 4. Haga clic en **OK** (Aceptar) en la ventana Internet Options (Opciones de Internet).

Los sucesos de hardware de un host se pierden cuando este host se gestiona mediante dos clientes de vCenter

Un host puede ser gestionado por un solo cliente de vCenter. Si se agrega un host en un cliente vCenter nuevo sin extracción desde el vCenter original, los sucesos de hardware del host no se recibirán en el Lenovo XCI en el cliente de vCenter original.

Los usuarios deben quitar el host del vCenter original.

Apéndice C. Funciones de accesibilidad

Las funciones de accesibilidad ayudan a los usuarios que tienen alguna discapacidad física, como una movilidad limitada o una visión reducida, para que puedan utilizar correctamente los productos de tecnología de la información.

En Lenovo nos esforzamos para ofrecer productos que puedan ser utilizados por todos los usuarios, sea cual sea su edad o sus capacidades.

El documento *Instalación y Guía del usuario de Lenovo XClarity Integrator para VMware vCenter* admite las funciones de accesibilidad del software de gestión del sistema en el que están integradas. Consulte la documentación del software de gestión del sistema para obtener información específica acerca de las funciones de accesibilidad y del desplazamiento con el teclado.

La colección de temas de VMware vCenter y sus publicaciones relacionadas tienen habilitadas las funciones de accesibilidad para la tecnología de lectura de pantalla. Los usuarios pueden utilizar todas las funciones utilizando el teclado en lugar del mouse.

Pueden ver las publicaciones para Lenovo XClarity Integrator para VMware vCenter en formato Portable Document Format (PDF) de Adobe usando Adobe Acrobat Reader. Las publicaciones están disponibles para descarga desde el [Sitio web de Lenovo XClarity Integrator para VMware](#).

Lenovo y las funciones de accesibilidad

Visite el [Sitio web de accesibilidad de Lenovo](#) para obtener más información acerca del compromiso que Lenovo ha adquirido en lo que se refiere a la accesibilidad.

Apéndice D. Avisos

Puede que Lenovo no comercialice en todos los países los productos, servicios o características a los que se hace referencia en este documento. Póngase en contacto con su representante local de Lenovo para obtener información acerca de los productos y servicios disponibles actualmente en su zona.

Las referencias a productos, programas o servicios de Lenovo no pretenden afirmar ni implicar que solo puedan utilizarse esos productos, programas o servicios de Lenovo. En su lugar, puede utilizarse cualquier producto, programa o servicio funcionalmente equivalente que no infrinja ninguno de los derechos de propiedad intelectual de Lenovo. Sin embargo, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier otro producto, programa o servicio.

Lenovo puede tener patentes o solicitudes de patentes pendientes que aborden temas descritos en este documento. No obstante, la posesión de este no le otorga ninguna licencia sobre dichas patentes. Puede enviar consultas sobre licencias, por escrito, a:

*Lenovo (United States), Inc.
8001 Development Drive
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing*

LENOVO PROPORCIONA ESTA PUBLICACIÓN “TAL CUAL” SIN GARANTÍA DE NINGUNA CLASE, NI EXPLÍCITA NI IMPLÍCITA, INCLUIDAS, PERO SIN LIMITARSE A, LAS GARANTÍAS IMPLÍCITAS DE NO VULNERACIÓN DE DERECHOS, COMERCIALIZACIÓN O IDONEIDAD PARA UNA FINALIDAD DETERMINADA. Algunas legislaciones no contemplan la exclusión de garantías, ni implícitas ni explícitas, por lo que puede haber usuarios a los que no afecte dicha norma.

Esta información podría incluir inexactitudes técnicas o errores tipográficos. La información aquí contenida está sometida a modificaciones periódicas, las cuales se incorporarán en nuevas ediciones de la publicación. Lenovo se reserva el derecho a realizar, si lo considera oportuno, cualquier modificación o mejora en los productos o programas que se describen en esta publicación.

Los productos descritos en este documento no están previstos para su utilización en implantes ni otras aplicaciones de reanimación en las que el funcionamiento incorrecto podría provocar lesiones o la muerte a personas. La información contenida en este documento no cambia ni afecta a las especificaciones o garantías del producto de Lenovo. Ninguna parte de este documento deberá regir como licencia explícita o implícita o indemnización bajo los derechos de propiedad intelectual de Lenovo o de terceros. Toda la información contenida en este documento se ha obtenido en entornos específicos y se presenta a título ilustrativo. Los resultados obtenidos en otros entornos operativos pueden variar.

Lenovo puede utilizar o distribuir la información que le suministre el cliente de la forma que crea oportuna, sin incurrir con ello en ninguna obligación con el cliente.

Las referencias realizadas en esta publicación a sitios web que no son de Lenovo se proporcionan únicamente en aras de la comodidad del usuario y de ningún modo pretenden constituir un respaldo de los mismos. La información de esos sitios web no forma parte de la información para este producto de Lenovo, por lo que la utilización de dichos sitios web es responsabilidad del usuario.

Los datos de rendimiento incluidos en este documento se han obtenido en un entorno controlado. Así pues, los resultados obtenidos en otros entornos operativos pueden variar de forma significativa. Es posible que algunas mediciones se hayan realizado en sistemas en desarrollo, por lo que no existen garantías de que estas sean las mismas en los sistemas de disponibilidad general. Además, es posible que la estimación de

algunas mediciones se haya realizado mediante extrapolación. Los resultados reales pueden variar. Los usuarios de la presente publicación deben verificar los datos pertinentes en su entorno de trabajo específico.

Marcas registradas

LENOVO, FLEX SYSTEM, SYSTEM X y NEXTSCALE SYSTEM son marcas registradas de Lenovo. Intel y Xeon son marcas registradas de Intel Corporation en Estados Unidos y/o en otros países. Internet Explorer, Microsoft y Windows son marcas registradas del grupo de empresas Microsoft. Linux es una marca registrada de Linus Torvalds. El resto de las marcas registradas son propiedad de sus propietarios respectivos. © 2024 Lenovo.

Avisos importantes

La velocidad del procesador indica la velocidad del reloj interno del microprocesador; también hay otros factores que afectan al rendimiento de la aplicación.

Cuando se hace referencia al almacenamiento del procesador, al almacenamiento real y virtual o al volumen del canal, KB representa 1.024 bytes, MB representa 1.048.576 bytes y GB representa 1.073.741.824 bytes.

Cuando se hace referencia a la capacidad de la unidad de disco duro o al volumen de comunicaciones, MB representa 1 000 000 bytes y GB representa 1 000 000 000 bytes. La capacidad total a la que puede acceder el usuario puede variar en función de los entornos operativos.

Lenovo no ofrece declaraciones ni garantía de ningún tipo respecto a productos que no sean de Lenovo. El soporte (si existe) para productos que no sean de Lenovo lo proporcionan terceros y no Lenovo.

Es posible que parte del software difiera de su versión minorista (si está disponible) y que no incluya manuales de usuario o todas las funciones del programa.

Lenovo